

Official Journal of the European Union

L 231



English edition

Legislation

Volume 66

20 September 2023

Contents

I *Legislative acts*

DIRECTIVES

- ★ **Directive (EU) 2023/1791 of the European Parliament and of the Council of 13 September 2023 on energy efficiency and amending Regulation (EU) 2023/955 (recast) ⁽¹⁾** 1

II *Non-legislative acts*

REGULATIONS

- ★ **Commission Implementing Regulation (EU) 2023/1792 of 13 September 2023 approving Union amendment to the specification for a Protected Designation of Origin or a Protected Geographical Indication ('Ribera del Guadiana' (PDO))** 112

DECISIONS

- ★ **Decision (EU) 2023/1793 of the Representatives of the Governments of the Member States of 15 September 2023 appointing two Judges to the General Court** 114
- ★ **Council Decision (EU) 2023/1794 of 18 September 2023 establishing the position to be taken on behalf of the European Union within the Committee on Government Procurement on the adoption of its rules of procedure for the selection of the Chairperson ⁽¹⁾** 115
- ★ **Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (notified under document C(2023)4745) ⁽¹⁾** 118

⁽¹⁾ Text with EEA relevance.

EN

Acts whose titles are printed in light type are those relating to day-to-day management of agricultural matters, and are generally valid for a limited period.

The titles of all other acts are printed in bold type and preceded by an asterisk.

I

(Legislative acts)

DIRECTIVES

DIRECTIVE (EU) 2023/1791 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 13 September 2023
on energy efficiency and amending Regulation (EU) 2023/955 (recast)
(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 194(2) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national Parliaments,

Having regard to the opinion of the European Economic and Social Committee ⁽¹⁾,

Having regard to the opinion of the Committee of the Regions ⁽²⁾,

Acting in accordance with the ordinary legislative procedure ⁽³⁾,

Whereas:

- (1) Directive 2012/27/EU of the European Parliament and of the Council ⁽⁴⁾ has been substantially amended several times ⁽⁵⁾. Since further amendments are to be made, that Directive should be recast in the interests of clarity.
- (2) In its communication of 17 September 2020 on ‘Stepping up Europe’s 2030 climate ambition – Investing in a climate-neutral future for the benefit of our people’ (the ‘Climate Target Plan’), the Commission proposed to raise the Union’s climate ambition by increasing the greenhouse gas (GHG) emissions target to at least 55 % below 1990 levels by 2030. That is a substantial increase compared to the existing 40 % reduction target. The proposal delivered on the commitment made in the communication of the Commission of 11 December 2019 on ‘The European Green Deal’ (the ‘European Green Deal’) to put forward a comprehensive plan to increase the Union’s target for 2030 towards 55 % in a responsible way. It is also in accordance with the objectives of the Paris Agreement adopted on 12 December 2015 under the United Nations Framework Convention on Climate Change (the ‘Paris Agreement’) to keep the global temperature increase to well below 2 °C and pursue efforts to keep it to 1,5 °C.

⁽¹⁾ OJ C 152, 6.4.2022, p. 134.

⁽²⁾ OJ C 301, 5.8.2022, p. 139.

⁽³⁾ Position of the European Parliament of 11 July 2023 (not yet published in the Official Journal) and decision of the Council of 25 July 2023.

⁽⁴⁾ Directive 2012/27/EU of the European Parliament and of the Council of 25 October 2012 on energy efficiency, amending Directives 2009/125/EC and 2010/30/EU and repealing Directives 2004/8/EC and 2006/32/EC (OJ L 315, 14.11.2012, p. 1).

⁽⁵⁾ See Part A of Annex XVI.

- (3) The conclusions of the European Council of 10-11 December 2020 endorsed the Union's binding domestic reduction target for net GHG emissions of at least 55 % by 2030 compared to 1990. The European Council concluded that the climate ambition needed to be raised in a manner that would spur sustainable economic growth, create jobs, deliver health and environmental benefits for Union citizens, and contribute to the long-term global competitiveness of the Union's economy by promoting innovation in green technologies.
- (4) To implement those objectives, the Commission, in its communication of 19 October 2020 on 'Commission Work Programme 2021 – A Union of vitality in a world of fragility', announced a legislative package to reduce GHG emissions by at least 55 % by 2030 (the 'Fit for 55 package'), and to achieve a climate-neutral European Union by 2050. That package covers a range of policy areas including energy efficiency, renewable energy, land use, land change and forestry, energy taxation, effort sharing and emissions trading.
- (5) The purpose of the Fit for 55 package is to safeguard and create jobs in the Union and to enable the Union to become a world leader in the development and uptake of clean technologies in the global energy transition, including energy efficiency solutions.
- (6) Projections indicate that, with the full implementation of current policies, GHG emission reductions by 2030 would be around 45 % compared to 1990 levels, when excluding land use emissions and absorptions, and around 47 %, when including them. The Climate Target Plan therefore provides for a set of required actions across all sectors of the economy and revisions of the key legislative instruments to reach that increased climate ambition.
- (7) In its communication of 28 November 2018 on 'A Clean Planet for all – A European strategic long-term vision for a prosperous, modern, competitive and climate neutral economy', the Commission stated that energy efficiency is a key area of action, without which the full decarbonisation of the Union's economy cannot be achieved. The need to capture the cost-effective energy saving opportunities has led to the Union's current energy efficiency policy. In December 2018, a new 2030 Union headline energy efficiency target of at least 32,5 %, compared to projected energy use in 2030, was included as part of the Clean Energy for All Europeans package, which aimed at putting energy efficiency first, achieving global leadership in renewable energies and providing a fair deal for consumers.
- (8) The impact assessment accompanying the Climate Target Plan demonstrated that, to achieve the increased climate ambition, energy efficiency improvements will need to be significantly raised from the current level of 32,5 %.
- (9) An increase in the Union's 2030 energy efficiency target can reduce energy prices and be crucial in reducing GHG emissions, accompanied by an increase and uptake of electrification, hydrogen, e-fuels and other relevant technologies necessary for the green transition, including in the transport sector. Even with the rapid growth of renewable electricity generation, energy efficiency can reduce the need of new power generation capacity and the costs relating to storage, transmission and distribution. Increased energy efficiency is also particularly important for the security of the energy supply of the Union, by lowering the Union's dependence on the import of fuels from third countries. Energy efficiency is one of the cleanest and most cost-efficient measures by which to address that dependence.
- (10) The sum of national contributions communicated by Member States in their national energy and climate plans falls short of the Union's target of 32,5 %. The contributions would collectively lead to a reduction of 29,7 % for primary energy consumption and 29,4 % for final energy consumption compared to the projections from the Commission's 2007 EU Reference Scenario for 2030. That would translate in a collective gap of 2,8 percentage points for primary energy consumption and 3,1 percentage points for final energy consumption for the EU-27.

- (11) A number of Member States presented ambitious national energy and climate plans, which were assessed by the Commission as 'sufficient', and which contained measures that allow those Member States to contribute to reaching the collective targets for energy efficiency with a ratio larger than the Union average. In addition, a number of Member States have documented 'early efforts' in achieving energy savings, namely energy savings above the Union average trajectories in the last years. Both cases are significant efforts that should be recognised and should be included in the Union's future modelling projections and that can serve as good examples of how all Member States can work on their energy efficiency potential to deliver significant benefits to their economies and societies.
- (12) In some cases, the assumptions used by the Commission in its 2020 EU Reference Scenario and the assumptions used by some Member States for their reference scenarios underpinning their national energy and climate plans are different. This may lead to divergences as regards the calculation of primary energy consumption but both approaches are valid with regard to primary energy consumption.
- (13) While the energy savings potential remains large in all sectors, there is a particular challenge relating to transport, as it is responsible for more than 30 % of final energy consumption, and to buildings, since 75 % of the Union's building stock has a poor energy performance. Another increasingly important sector is the information and communications technology (ICT) sector, which is responsible for 5 to 9 % of the world's total electricity use and more than 2 % of global emissions. In 2018, data centres accounted for 2,7 % of the electricity demand in the EU-28. In that context, the Commission, in its communication of 19 February 2020 on 'Shaping Europe's digital future' (the 'Union's Digital Strategy'), highlighted the need for highly energy-efficient and sustainable data centres and transparency measures for telecoms operators as regards their environmental footprint. Furthermore, the possible increase in industry's energy demand that may result from its decarbonisation, particularly for energy intensive processes, should also be taken into account.
- (14) The higher level of ambition requires a stronger promotion of cost-effective energy efficiency measures in all areas of the energy system and in all relevant sectors where activity affects energy demand, such as the transport, water and agriculture sectors. Improving energy efficiency throughout the full energy chain, including energy generation, transmission, distribution and end-use, will benefit the environment, improve air quality and public health, reduce GHG emissions, improve energy security by decreasing the need for energy imports, in particular of fossil fuels, cut energy costs for households and companies, help alleviate energy poverty, and lead to increased competitiveness, more jobs and increased economic activity throughout the economy. Improving energy efficiency would thus improve citizens' quality of life, while contributing to the transformation of the Union's energy relations with third-country partners towards achieving climate neutrality. That complies with the Union commitments made in the framework of the Energy Union and global climate agenda established by the Paris Agreement. Improving the energy performance of various sectors has the potential of fostering urban regeneration, including improvement of buildings, and changes in mobility and accessibility patterns, while promoting more efficient, sustainable and affordable options.
- (15) This Directive takes a step forward towards climate neutrality by 2050, under which energy efficiency is to be treated as an energy source in its own right. The energy efficiency first principle is an overarching principle that should be taken into account across all sectors, going beyond the energy system, at all levels, including in the financial sector. Energy efficiency solutions should be considered as the first option in policy, planning and investment decisions when setting new rules for the supply side and other policy areas. While the energy efficiency first principle should be applied without prejudice to other legal obligations, objectives and principles, such obligations, objectives and principles should not hamper its application or lead to exemptions from applying the principle. The Commission should ensure that energy efficiency and demand response can compete on equal terms with generation capacity. Energy efficiency improvements need to be made whenever they are more cost-effective than equivalent supply-side solutions. That should help exploit the multiple benefits of energy efficiency for the Union, in particular for citizens and businesses. Implementing energy efficiency improvement measures should also be a priority in alleviating energy poverty.

- (16) Energy efficiency should be recognised as a crucial element and a priority consideration in future investment decisions on the Union's energy infrastructure. The energy efficiency first principle should be applied taking into consideration primarily the system efficiency approach and societal and health perspective, and paying attention to security of supply, energy system integration and the transition to climate neutrality. Consequently, the energy efficiency first principle should help increase the efficiency of individual end-use sectors and of the whole energy system. The application of the principle should also support investments in energy-efficient solutions contributing to the environmental objectives of Regulation (EU) 2020/852 of the European Parliament and of the Council ⁽⁶⁾.
- (17) The energy efficiency first principle is provided for in Regulation (EU) 2018/1999 of the European Parliament and of the Council ⁽⁷⁾ and is at the core of the EU Strategy for Energy System Integration established in the Commission's communication of 8 July 2022. While the principle is based on cost-effectiveness, its application has wider implications from the societal perspective. Those implications can vary depending on the circumstances and should be carefully evaluated through robust cost-benefit analysis methodologies that take into account the multiple benefits of energy efficiency. The Commission has prepared dedicated guidelines for the operation and application of the principle, by proposing specific tools and examples of application in various sectors. The Commission has also issued a recommendation to Member States that builds on the requirements laid down in this Directive and calls for specific actions in relation to the application of the principle. Member States should take the utmost account of that recommendation and be guided by it in implementing the energy efficiency principle in practice.
- (18) The energy efficiency first principle implies adopting a holistic approach, which takes into account the overall efficiency of the integrated energy system, security of supply and cost effectiveness and promotes the most efficient solutions for climate neutrality across the whole value chain, from energy production, network transport to final energy consumption, so that efficiencies are achieved in both primary energy consumption and final energy consumption. That approach should look at the system performance and dynamic use of energy, where demand-side resources and system flexibility are considered to be energy efficiency solutions.
- (19) In order to have an impact, the energy efficiency first principle needs to be consistently applied by national, regional, local and sectoral decision makers in all relevant scenarios and policy, planning and major investment decisions – that is to say large-scale investments with a value of more than EUR 100 000 000 each or EUR 175 000 000 for transport infrastructure projects – affecting energy consumption or supply. The proper application of the principle requires using the right cost-benefit analysis methodology, setting enabling conditions for energy efficient solutions and proper monitoring. Cost-benefit analyses should be systematically developed and carried out, should be based on the most up-to-date information on energy prices and should include scenarios for rising prices, such as due to decreasing Union's emission trading system (EU ETS) allowances pursuant to Directive 2003/87/EC of the European Parliament and of the Council ⁽⁸⁾, in order to provide an incentive to apply energy efficiency measures. Priority should be given to demand-side solutions where they are more cost-effective than investments in energy supply infrastructure in meeting policy objectives. Demand-side flexibility can bring wider economic, environmental and societal benefits to consumers and to society at large, including local communities, and can increase the efficiency of the energy system and decrease the energy costs, for example by reducing system operation costs resulting in lower tariffs for all consumers. Member States should take into account potential benefits from demand-side flexibility in applying the energy efficiency first principle and where relevant consider demand response at both centralised and decentralised level, energy storage, and smart solutions as part of their efforts to increase efficiency of the integrated energy system.

⁽⁶⁾ Regulation (EU) 2020/852 of the European Parliament and of the Council of 18 June 2020 on the establishment of a framework to facilitate sustainable investment, and amending Regulation (EU) 2019/2088 (OJ L 198, 22.6.2020, p. 13).

⁽⁷⁾ Regulation (EU) 2018/1999 of the European Parliament and of the Council of 11 December 2018 on the Governance of the Energy Union and Climate Action, amending Regulations (EC) No 663/2009 and (EC) No 715/2009 of the European Parliament and of the Council, Directives 94/22/EC, 98/70/EC, 2009/31/EC, 2009/73/EC, 2010/31/EU, 2012/27/EU and 2013/30/EU of the European Parliament and of the Council, Council Directives 2009/119/EC and (EU) 2015/652 and repealing Regulation (EU) No 525/2013 of the European Parliament and of the Council (OJ L 328, 21.12.2018, p. 1).

⁽⁸⁾ Directive 2003/87/EC of the European Parliament and of the Council of 13 October 2003 establishing a system for greenhouse gas emission allowance trading within the Union and amending Council Directive 96/61/EC (OJ L 275, 25.10.2003, p. 32).

- (20) When assessing the values of projects for the purpose of the application of the energy efficiency first principle, the Commission, in its report to the European Parliament and to the Council, should assess, in particular, whether and in what manner the thresholds are effectively applied in each Member State.
- (21) The energy efficiency first principle should always be applied in a proportional way and the requirements laid down in this Directive should not entail overlapping or conflicting obligations on Member States, where the application of the principle is ensured directly by other legislation. This might be the case for the projects of common interest included in the Union list pursuant to Article 3 of Regulation (EU) 2022/869 of the European Parliament and of the Council ⁽⁹⁾, which introduces the requirements to consider the energy efficiency first principle in the development and assessment for those projects.
- (22) A fair transition towards a climate-neutral Union by 2050 is central to the European Green Deal. Energy poverty is a key concept in the Clean Energy for All Europeans package and designed to facilitate a just energy transition. Pursuant to Regulation (EU) 2018/1999 and Directive (EU) 2019/944 of the European Parliament and of the Council ⁽¹⁰⁾, the Commission, in its Recommendation (EU) 2020/1563 on energy poverty ⁽¹¹⁾, provided indicative guidance on appropriate indicators for measuring energy poverty and defining a 'significant number of households in energy poverty'. Directive 2009/73/EC of the European Parliament and of the Council ⁽¹²⁾ and Directive (EU) 2019/944 require Member States to take appropriate measures to address energy poverty wherever it is identified, including measures addressing the broader context of poverty. This is particularly relevant in a context of rising energy prices and inflationary pressure, where both short and long-term measures should be implemented to address systemic challenges to the Union's energy system.
- (23) People facing or risking energy poverty, vulnerable customers, including final users, low- and medium-income households, and people living in social housing should benefit from the application of the energy efficiency first principle. Energy efficiency measures should be implemented as a priority to improve the situations of those individuals and households and to alleviate energy poverty, and should not encourage any disproportionate increase in housing, mobility or energy costs. A holistic approach in policy making and in implementing policies and measures requires Member States to ensure that other policies and measures have no adverse effect on those individuals and households.
- (24) This Directive is part of a broader policy framework of energy efficiency policies addressing energy efficiency potentials in specific policy areas, including buildings (Directive 2010/31/EU of the European Parliament and of the Council ⁽¹³⁾), products (Directive 2009/125/EC of the European Parliament and of the Council ⁽¹⁴⁾ and Regulations (EU) 2017/1369 ⁽¹⁵⁾ and (EU) 2020/740 ⁽¹⁶⁾ of the European Parliament and of the Council), and governance (Regulation (EU) 2018/1999). Those policies play a very important role in delivering energy savings when products are replaced or buildings constructed or renovated.

⁽⁹⁾ Regulation (EU) 2022/869 of the European Parliament and of the Council of 30 May 2022 on guidelines for trans-European energy infrastructure, amending Regulations (EC) No 715/2009, (EU) 2019/942 and (EU) 2019/943 and Directives 2009/73/EC and (EU) 2019/944, and repealing Regulation (EU) No 347/2013 (OJ L 152, 3.6.2022, p. 45).

⁽¹⁰⁾ Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p. 125).

⁽¹¹⁾ Commission Recommendation (EU) 2020/1563 of 14 October 2020 on energy poverty (OJ L 357, 27.10.2020, p. 35).

⁽¹²⁾ Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211, 14.8.2009, p. 94).

⁽¹³⁾ Directive 2010/31/EU of the European Parliament and of the Council of 19 May 2010 on the energy performance of buildings (OJ L 153, 18.6.2010, p. 13).

⁽¹⁴⁾ Directive 2009/125/EC of the European Parliament and of the Council of 21 October 2009 establishing a framework for the setting of ecodesign requirements for energy-related products (OJ L 285, 31.10.2009, p. 10).

⁽¹⁵⁾ Regulation (EU) 2017/1369 of the European Parliament and of the Council of 4 July 2017 setting a framework for energy labelling and repealing Directive 2010/30/EU (OJ L 198, 28.7.2017, p. 1).

⁽¹⁶⁾ Regulation (EU) 2020/740 of the European Parliament and of the Council of 25 May 2020 on the labelling of tyres with respect to fuel efficiency and other parameters, amending Regulation (EU) 2017/1369 and repealing Regulation (EC) No 1222/2009 (OJ L 177, 5.6.2020, p. 1).

- (25) Reaching an ambitious energy efficiency target requires barriers to be removed in order to facilitate investment in energy efficiency measures. The Clean Energy Transition sub-programme of the Union's LIFE Programme, established by Regulation (EU) 2021/783 of the European Parliament and of the Council ⁽¹⁷⁾, will dedicate funding to support development of Union best practices in energy efficiency policy implementation, addressing behavioural, market, and regulatory barriers to energy efficiency.
- (26) The European Council, in its conclusion of 23 and 24 October 2014, supported a 27 % energy efficiency target for 2030 at Union level, to be reviewed by 2020 having in mind a Union-level target of 30 %. In its resolution of 15 December 2015 entitled 'Towards a European Energy Union', the European Parliament called on the Commission to assess, in addition, the viability of a 40 % energy efficiency target for the same timeframe.
- (27) In its communication of 28 November 2018 on 'A Clean Planet for all – A European strategic long-term vision for a prosperous, modern, competitive and climate neutral economy', the Commission projects that the 32,5 % Union's energy efficiency target for 2030 and the other policy instruments of the existing framework would lead to a reduction in GHG emissions of about 45 % by 2030. For an increased climate ambition of a 55 % decrease of GHG emissions by 2030, the impact assessment of the Climate Target Plan assessed what level of efforts would be needed in the different policy areas. It concluded that, in relation to the baseline, achieving the GHG emissions target in a cost-optimal way meant that primary energy consumption and final energy consumption are to decrease by at least 39 to 41 % and 36 to 37 % respectively.
- (28) The Union's energy efficiency target was initially set and calculated using the 2007 EU Reference Scenario projections for 2030 as a baseline. The change in the Eurostat energy balance calculation methodology and improvements in subsequent modelling projections call for a change of the baseline. Thus, using the same approach to define the target, namely by comparing it to the future baseline projections, the ambition of the Union's 2030 energy efficiency target is set compared to the 2020 EU Reference Scenario projections for 2030 reflecting national contributions from the national energy and climate plans. With that updated baseline, the Union will need to further increase its energy efficiency ambition by at least 11,7 % in 2030 compared to the level of efforts under the 2020 EU Reference Scenario. The new way of expressing the level of ambition for the Union's targets does not affect the actual level of efforts needed and corresponds to a reduction of 40,5 % for primary energy consumption and 38 % for final energy consumption when compared to the 2007 EU Reference Scenario projections for 2030.
- (29) The methodology for calculation of primary energy consumption and final energy consumption is aligned with the new Eurostat methodology, but the indicators used for the purpose of this Directive have a different scope, in that they exclude ambient energy and include energy consumption in international aviation for the targets in primary energy consumption and final energy consumption. The use of new indicators also implies that any changes in energy consumption of blast furnaces are now only reflected in primary energy consumption.
- (30) The need for the Union to improve its energy efficiency should be expressed in primary energy consumption and final energy consumption, to be achieved in 2030, indicating an additional level of efforts required when compared to the measures in place or planned measures in the national energy and climate plans. The 2020 EU Reference Scenario projects 864 Mtoe of final energy consumption and 1 124 Mtoe of primary energy consumption to be reached in 2030 (excluding ambient energy and including international aviation). An additional reduction of 11,7 % results in 763 Mtoe and 992,5 Mtoe in 2030. Compared to 2005 levels, it means that final energy consumption in the Union should be reduced by approximately 25 % and primary energy consumption should be reduced by approximately 34 %. There are no binding targets at Member State level in the 2020 and 2030 perspectives, and Member States should establish their contributions to the achievement of the Union's energy efficiency target taking

⁽¹⁷⁾ Regulation (EU) 2021/783 of the European Parliament and of the Council of 29 April 2021 establishing a Programme for the Environment and Climate Action (LIFE), and repealing Regulation (EU) No 1293/2013 (OJ L 172, 17.5.2021, p. 53).

into account the formula provided for in this Directive. Member States should be free to set their national objectives based either on primary energy consumption or final energy consumption or primary energy savings or final energy savings, or on energy intensity. This Directive amends the way in which Member States should express their national contributions to the Union's target. Member States' contributions to the Union's target should be expressed in primary energy consumption and final energy consumption to ensure consistency and monitoring of progress. A regular evaluation of progress towards the achievement of the Union's 2030 targets is necessary and is provided for in Regulation (EU) 2018/1999.

- (31) By 30 November 2023, the Commission should update the 2020 EU Reference Scenario based on the latest Eurostat data. Member States wishing to use the updated reference scenario should notify their updated national contributions by 1 February 2024, as part of the iterative process provided for in Regulation (EU) 2018/1999.
- (32) It would be preferable for the energy efficiency targets to be achieved as a result of the cumulative implementation of specific Union and national measures promoting energy efficiency in different fields. Member States should be required to set national energy efficiency policies and measures. Those policies and measures and the individual efforts of each Member State should be evaluated by the Commission, alongside data on the progress made, to assess the likelihood of achieving the overall Union target and the extent to which the individual efforts are sufficient to meet the common goal.
- (33) The public sector is responsible for approximately 5 % to 10 % of the Union's total final energy consumption. Public authorities spend approximately EUR 1 800 000 000 000 every year. This represents around 14 % of the Union's gross domestic product. For that reason the public sector constitutes an important driver to stimulate market transformation towards more efficient products, buildings and services, as well as to trigger behavioural changes in energy consumption by citizens and enterprises. Furthermore, decreasing energy consumption through energy efficiency improvement measures can free up public resources for other purposes. Public bodies at national, regional and local level should fulfil an exemplary role as regards energy efficiency.
- (34) To lead by example, the public sector should set its own decarbonisation and energy efficiency goals. Energy efficiency improvements in the public sector should reflect the efforts required at Union level. To comply with the final energy consumption target, the Union should decrease its final energy consumption by 19 % by 2030 as compared to the average energy consumption in years 2017, 2018 and 2019. An obligation to achieve an annual reduction of the energy consumption in the public sector by at least 1,9 % should ensure that the public sector fulfils its exemplary role. Member States retain full flexibility regarding the choice of energy efficiency improvement measures to achieve a reduction of the final energy consumption. Requiring an annual reduction of final energy consumption has a lower administrative burden than establishing measurement methods for energy savings.
- (35) To fulfil their obligation, Member States should target the final energy consumption of all public services and installations of public bodies. To determine the scope of addressees, Member States should apply the definition of 'public bodies' provided for in this Directive, where 'directly financed by those authorities' means that those entities are mostly funded by public funds and 'administered by those authorities' means that a national, regional or local authority has a majority with regard to the choice of the entity's management. The obligation can be fulfilled by the reduction of final energy consumption in any area of the public sector, including transport, public buildings, healthcare, spatial planning, water management and wastewater treatment, sewage and water purification, waste management, district heating and cooling, energy distribution, supply and storage, public lighting, infrastructure planning, education and social services. Member States may also include other types of services when transposing this Directive. To lower the administrative burden for public bodies, Member States should establish digital platforms or tools to collect the aggregated consumption data from public bodies, make them publicly available, and report the data to the Commission. Member States should provide planning and annual reporting on the consumption of public bodies in an aggregated form per sector.

- (36) Member States should promote energy efficient means of mobility, including in their public procurement practices, such as rail, cycling, walking or shared mobility, by renewing and decarbonising fleets, encouraging a modal shift and including those modes in urban mobility planning.
- (37) Member States should exercise an exemplary role by ensuring that all energy performance contracts, energy audits and energy management systems are carried out in the public sector in line with European or international standards, or that energy audits are used to a large extent in energy-intensive parts of the public sector. Member States should provide guidance and should provide for procedures for the use of those instruments.
- (38) Public authorities are encouraged to obtain support from entities such as sustainable energy agencies established at regional or local level, where applicable. The organisation of those agencies usually reflects the individual needs of public authorities in a certain region or operating in a certain area of the public sector. Centralised agencies can serve the needs better and work more effectively in other respects, for example, in smaller or centralised Member States or regarding complex or cross-regional aspects such as district heating and cooling. Sustainable energy agencies can serve as one-stop shops. Those agencies are often responsible for developing local or regional decarbonisation plans, which may also include other decarbonisation measures, such as the exchange of fossil fuel boilers, and for supporting public authorities in the implementation of energy-related policies. Sustainable energy agencies or other entities to assist regional and local authorities may have clear competences, objectives and resources in the field of sustainable energy. Sustainable energy agencies could be encouraged to consider initiatives taken in the framework of the Covenant of Mayors, which brings together local governments voluntarily committed to implementing the Union's climate and energy objectives, and other existing initiatives for that purpose. The decarbonisation plans should be linked to territorial development plans and take into account the comprehensive assessment which the Member States should carry out.
- (39) Member States should support public bodies in planning and the uptake of energy efficiency improvement measures, including at regional and local level, by providing guidelines promoting competence-building and training opportunities and encouraging cooperation amongst public bodies including amongst agencies. For that purpose, Member States could set up national competence centres on complex issues, such as advising local or regional energy agencies on district heating or cooling. The requirement to transform buildings into nearly zero-energy buildings does not exclude or prohibit a differentiation between nearly zero-energy building levels for new or renovated buildings. Nearly zero-energy buildings, including the cost-optimal level, are defined in Directive 2010/31/EU.
- (40) Until the end of 2026, Member States that renovate more than 3 % of the total floor area of their buildings in any given year should be given the possibility to count the surplus towards the annual renovation rate of any of the three following years. A Member State that renovates more than 3 % of the total floor area of its buildings from 1 January 2027 should be able to count the surplus towards the annual renovation rate of the following two years. That possibility should not be used for purposes that are not in line with the general objectives and the level of ambition of this Directive.
- (41) Member States should encourage public bodies to take into account the wider benefits beyond energy savings, such as the quality of the indoor environment as well as an improvement of people's quality of life and the comfort of renovated public buildings, in particular schools, day care centres, nursing homes, sheltered housing, hospitals, and social housing.
- (42) Buildings and transport, alongside industry, are the main energy users and main source of emissions. Buildings are responsible for about 40 % of the Union's total energy consumption and for 36 % of its GHG from energy. The Commission communication of 14 October 2020, entitled 'Renovation Wave' addresses the twin challenge of energy and resource efficiency and affordability in the building sector and aims to double the renovation rate. It focuses on the worst performing buildings, energy poverty and on public buildings. Moreover, buildings are crucial to achieving the Union objective of reaching climate neutrality by 2050. Buildings that are owned by public bodies account for a considerable share of the building stock and have high visibility in public life. It is therefore appropriate to set an annual rate of renovation of buildings that are owned by public bodies on the territory of a

Member State to upgrade their energy performance and be transformed into at least nearly zero-energy buildings or zero-emission buildings. Member States are invited to set a higher renovation rate, where that is cost-effective in the framework of the renovation of their buildings stock in accordance with their long-term renovation strategies or national renovation programmes, or both. That renovation rate should be without prejudice to the obligations with regard to nearly zero-energy buildings set out in Directive 2010/31/EU. Member States should be able to apply less stringent requirements to some buildings, such as buildings with special architectural or historical merit. During the next review of Directive 2010/31/EU, the Commission should assess the progress Member States achieved regarding the renovation of public bodies' buildings. The Commission should consider submitting a legislative proposal to revise the renovation rate, while taking into account the progress achieved by the Member States, substantial economic or technical developments, or where needed, the Union's commitments for decarbonisation and zero pollution. The obligation to renovate public bodies' buildings in this Directive complements that in Directive 2010/31/EU, which requires Member States to ensure that when existing buildings undergo major renovation their energy performance is upgraded so that they meet the requirements on nearly zero-energy buildings.

- (43) Building automation and control systems and other solutions to provide active energy management are important tools for public bodies to improve and maintain the energy performance of buildings, as well as ensuring the necessary indoor conditions in the buildings they own or occupy, in accordance with Directive 2010/31/EU.
- (44) Promoting green mobility is a key part of the European Green Deal. The provision of charging infrastructure is one of the necessary elements in the transition. Charging infrastructure in buildings is particularly important since electric vehicles park in buildings regularly and for long periods of time, thus making charging easier and more efficient. Public bodies should make best efforts to install charging infrastructure in buildings they own or occupy in accordance with Directive 2010/31/EU.
- (45) To set the rate of renovations, Member States need to have an overview of the buildings that do not reach the nearly zero-energy buildings level. Therefore, Member States should publish and keep updated an inventory of public buildings, including, where appropriate, social housing, as part of an overall database of energy performance certificates. That inventory should also enable private actors, including energy service companies (ESCOs), to propose renovation solutions, which can be aggregated by the EU Building Stock Observatory.
- (46) The inventory could integrate data from existing building stock inventories. Member States should take appropriate measures to facilitate data collection and make the inventory accessible to private actors, including ESCOs to enable their active role in renovation solutions. Available and publicly shared data about building stock characteristics, buildings renovation and energy performance may be aggregated by the EU Building Stock Observatory to ensure a better understanding of the energy performance of the building sector through comparable data.
- (47) In 2020, more than half of the world's population lived in urban areas. That figure is expected to reach 68 % by 2050. In addition, half of the urban infrastructures by 2050 are still to be built. Cities and metropolitan areas are centres of economic activity, knowledge generation, innovation and new technologies. Cities influence the quality of life of the citizens who live or work in them. Member States should support municipalities technically and financially. A number of municipalities and other public bodies in the Member States have already put into place integrated approaches to energy saving and energy supply and sustainable mobility, for example via sustainable energy action plans or sustainable urban mobility plans, such as those developed under the Covenant of Mayors initiative, and integrated urban approaches which go beyond individual interventions in buildings or transport modes. Further efforts are needed in the area of improving the energy efficiency of urban mobility, for both passenger and freight transport, as it uses around 40 % of all road transport energy.

- (48) All the principles of Directives 2014/23/EU ⁽¹⁸⁾, 2014/24/EU ⁽¹⁹⁾ and 2014/25/EU ⁽²⁰⁾ of the European Parliament and of the Council remain fully applicable within the framework of this Directive.
- (49) With regard to the purchase of certain products and services and the purchase and rent of buildings, contracting authorities and contracting entities which conclude public works, supply or service contracts should lead by example and make energy-efficient purchasing decisions and apply the energy efficiency first principle, including for those public contracts and concessions for which no specific requirements are provided for in this Directive. This should apply to contracting authorities and contracting entities falling within the scope of Directives 2014/23/EU, 2014/24/EU or 2014/25/EU. Member States should remove barriers to joint procurement within a Member State or across borders if this can reduce the costs and enhance the benefits of the internal market by creating business opportunities for suppliers and energy service providers.
- (50) All public entities investing public resources through procurement should lead by example when awarding contracts and concessions by choosing products, buildings, works and services with the highest energy efficiency performance, also in relation to those procurements that are not subject to specific requirements under Directive 2009/30/EC. In that context, all award procedures for public contracts and concessions with a value above the thresholds set out in Article 8 of Directive 2014/23/EU, Article 4 of Directive 2014/24/EU, and Article 15 of Directive 2014/25/EU need to take into account the energy efficiency performance of the products, buildings and services set by Union or national law, by considering as priority the energy efficiency first principle in their procurement procedures.
- (51) It is also important that Member States monitor how the energy efficiency requirements are taken into account by contracting authorities and contracting entities in the procurement of products, buildings, works and services by ensuring that information about the impact on the energy efficiency of those winning tenders above the thresholds referred to in the procurement directives are made publicly available. That would allow stakeholders and citizens to assess the role of the public sector in ensuring energy efficiency first in public procurement in a transparent manner.
- (52) The obligation for Member States to ensure that contracting authorities and entities purchase only products, buildings, works and services with high energy efficiency performance should not, however, prevent Member States from purchasing goods necessary to protect, and respond to, public security or public health emergencies.
- (53) The European Green Deal recognises the role of the circular economy in contributing to overall Union decarbonisation objectives. The public sector and, in particular, the transport sector, should contribute to those objectives by using their purchasing power to, where appropriate, choose environmentally friendly products, buildings, works and services via available tools for green public procurement, and thus making an important contribution to reduce energy consumption and environmental impacts.
- (54) It is important that Member States provide the necessary support to public bodies in the uptake of energy efficiency requirements in public procurement and, where appropriate, in the use of green public procurement by providing necessary guidelines and methodologies on carrying out the assessment of life-cycle costs and environment impacts and costs. Well-designed tools, in particular digital tools, are expected to facilitate the procurement procedures and reduce the administrative costs especially in smaller Member States that may not have sufficient capacity to prepare tenders. In this regard, Member States should actively promote the use of digital tools and cooperation amongst contracting authorities including across borders for the purpose of exchanging best practices.

⁽¹⁸⁾ Directive 2014/23/EU of the European Parliament and of the Council of 26 February 2014 on the award of concession contracts (OJ L 94, 28.3.2014, p. 1).

⁽¹⁹⁾ Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65).

⁽²⁰⁾ Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC (OJ L 94, 28.3.2014, p. 243).

- (55) Given that buildings are responsible for GHG emissions before and after their operational lifetime, Member States should also consider the whole life cycle of carbon emissions of buildings. That should take place in the context of efforts to increase the attention given to whole life-cycle performance, circular economy aspects and environmental impacts, as part of the exemplary role of the public sector. Public procurement can thus serve as an opportunity to address the embodied carbon in buildings over their life cycle. In this regard, contracting authorities are important actors that can take action as part of procurement procedures by purchasing new buildings that address global warming potential over the full life cycle.
- (56) The global warming potential over the full life cycle measures the GHG emissions associated with the building at different stages along its life cycle. It therefore measures the building's overall contribution to emissions that lead to climate change. That is sometimes referred to as a carbon footprint assessment or the whole life carbon measurement. It brings together carbon emissions embodied in building materials with direct and indirect carbon emissions from use stage. Buildings are a significant material bank, being repositories for carbon intensive resources over many decades, and so it is important to explore designs that facilitate future reuse and recycling at the end of the operational life in line with the new circular economy action plan. Member States should promote circularity, durability, and adaptability of building materials, in order to address the sustainability performance of construction products.
- (57) The global warming potential is expressed as a numeric indicator in $\text{kgCO}_2\text{eq/m}^2$ (of useful internal floor area) for each life-cycle stage averaged for one year of a reference study period of 50 years. The data selection, scenario definition and calculations are carried out in accordance with standard EN 15978. The scope of building elements and technical equipment are set out in indicator 1,2 of the Level(s) common Union framework. Where a national calculation tool exists, or is required for making disclosures or for obtaining building permits, it should be possible to use that national tool to provide the required information. It should be possible to use other calculation tools, if they fulfil the minimum criteria laid down by the Level(s) common Union framework.
- (58) Directive 2010/75/EU of the European Parliament and of the Council ⁽²¹⁾ lays down rules on installations that contribute to energy production or use energy for production purposes, and provides that information on the energy used in or generated by the installation is to be included in applications for integrated permits in accordance with Article 12(1), point (b) of that Directive. Moreover, Article 11 of that Directive provides that efficient use of energy is one of the general principles governing the basic obligations of the operator and one of the criteria for determining best available techniques pursuant to Annex III to that Directive. The operational efficiency of energy systems at any given moment is influenced by the ability to feed power generated from different sources with different degrees of inertia and start-up times into the grid smoothly and flexibly. Improving efficiency will enable better use to be made of renewable energy.
- (59) Improvement in energy efficiency can contribute to higher economic output. Member States and the Union should aim to decrease energy consumption regardless of levels of economic growth.
- (60) The energy savings obligation established by this Directive should be increased and should also apply after 2030. That ensures stability for investors and thus encourages long-term investments and long-term energy efficiency measures, such as the deep renovation of buildings with the long-term objective of facilitating the cost effective transformation of existing buildings into nearly zero-energy buildings. The energy savings obligation plays an important role in the creation of local growth, jobs, competitiveness and alleviating energy poverty. It should ensure that the Union can achieve its energy and climate objectives by creating further opportunities and by breaking the link between energy consumption and growth. Cooperation with the private sector is important to assess the conditions on which private investment for energy efficiency projects can be unlocked and to develop new revenue models for innovation in the field of energy efficiency.

⁽²¹⁾ Directive 2010/75/EU of the European Parliament and of the Council of 24 November 2010 on industrial emissions (integrated pollution prevention and control) (OJ L 334, 17.12.2010, p. 17).

- (61) Energy efficiency improvement measures also have a positive impact on air quality, as more energy efficient buildings contribute to reducing the demand for heating fuels, including solid heating fuels. Energy efficiency measures therefore contribute to improving indoor and outdoor air quality and help achieve, in a cost-effective manner, the objectives of the Union's air quality policy, as laid down in particular by Directive (EU) 2016/2284 of the European Parliament and of the Council ⁽²²⁾.
- (62) With a view to ensuring a stable and predictable contribution towards achieving the Union's energy and climate targets for 2030 and the climate neutrality objective for 2050, Member States are required to achieve cumulative end-use energy savings for the entire obligation period up to 2030, equivalent to new annual savings of at least 0,8 % of final energy consumption up to 31 December 2023 and of at least 1,3 % from 1 January 2024, 1,5 % from 1 January 2026 and 1,9 % from 1 January 2028. That requirement could be met by new policy measures that are adopted during the obligation period from 1 January 2021 to 31 December 2030 or by new individual actions as a result of policy measures adopted during or before the previous period, provided that the individual actions that trigger energy savings are introduced during the following period. To that end, Member States should be able to make use of an energy efficiency obligation scheme, alternative policy measures, or both.
- (63) For the period from 1 January 2021 to 31 December 2023, Cyprus and Malta should be required to achieve cumulative end-use energy savings equivalent to new savings of 0,24 % of annual final energy consumption averaged over the most recent three-year period preceding 1 January 2019. For the period from 1 January 2024 to 31 December 2030, Cyprus and Malta should be required to achieve cumulative end-use energy savings of 0,45 % of annual final energy consumption, averaged over the most recent three-year period preceding 1 January 2019.
- (64) Where using an obligation scheme, Member States should designate obligated parties among transmission system operators, distribution system operators, energy distributors, retail energy sales companies and transport fuel distributors or transport fuel retailers on the basis of objective and non-discriminatory criteria. The designation or exemption from designation of certain categories of such entities should not be understood to be incompatible with the principle of non-discrimination. Member States are therefore able to choose whether such entities or only certain categories thereof are designated as obligated parties. To empower and protect people affected by energy poverty, vulnerable customers, people in low-income households and, where applicable, people living in social housing, and to implement policy measures as a priority among those people, Member States can require obligated parties to achieve energy savings among those people. For that purpose, Member States can also establish energy cost reduction targets. Obligated parties could achieve those targets by promoting the installation of measures that lead to energy savings and financial savings on energy bills, such as the installation of insulation and heating measures, and by supporting energy savings initiatives by renewable energy communities and citizen energy communities.
- (65) When designing policy measures to fulfil the energy savings obligation, Member States should respect the climate and environmental standards and priorities of the Union and comply with the principle of 'do no significant harm' within the meaning of Regulation (EU) 2020/852. Member States should not promote activities that are not environmentally sustainable such as the use of fossil fuels. The energy savings obligation aims at strengthening the response to climate change by promoting incentives to Member States to implement a sustainable and clean policy mix, which is resilient, and mitigates climate change. Therefore, energy savings from policy measures regarding the use of direct fossil fuel combustion may be eligible energy savings under the energy savings obligation under certain conditions and for a transitional period following the transposition of this Directive in accordance with an annex to this Directive. It will allow aligning the energy savings obligation with the objectives of the European Green Deal, the Climate Target Plan, the Renovation Wave, and mirror the need for action identified by the International Energy Agency in its net zero report. The restriction aims at encouraging Member States to spend public money into future-proof, sustainable technologies only. It is important that Member States provide a clear policy framework and investment certainty to market actors. The implementation of the calculation methodology under the energy

⁽²²⁾ Directive (EU) 2016/2284 of the European Parliament and of the Council of 14 December 2016 on the reduction of national emissions of certain atmospheric pollutants, amending Directive 2003/35/EC and repealing Directive 2001/81/EC (OJ L 344, 17.12.2016, p. 1).

savings obligation should allow all market actors to adapt their technologies in a reasonable timeframe. Where Member States support the uptake of efficient fossil fuel technologies or early replacement of such technology, for example through subsidy schemes or energy efficiency obligation schemes, any resulting energy savings may no longer be eligible under the energy savings obligation. While energy savings resulting, for example, from the promotion of natural gas-based cogeneration would not be eligible under the energy savings obligation, the restriction would not apply for indirect fossil fuel usage, for example where the electricity production includes fossil fuel generation. Policy measures targeting behavioural changes to reduce the consumption of fossil fuels, for example through information campaigns and eco-driving, should remain eligible. Policy measures which target building renovations may include measures such as the replacement of fossil fuel heating systems together with building fabric improvements. Those measures should be limited to technologies that allow the required energy savings to be achieved in accordance with the national building codes established in a Member State. Nevertheless, Member States should promote upgrading heating systems as part of deep renovations in line with the long-term objective of carbon neutrality, namely reducing the heating demand and covering the remaining heating demand with a carbon-free energy source. When accounting for the savings needed to achieve a share of the energy savings obligation among people affected by energy poverty, Member States may take into account their climatic conditions.

- (66) Member States' energy efficiency improvement measures in transport are eligible to be taken into account for achieving their end-use energy savings obligation. Such measures include policies that are, inter alia, dedicated to promoting more efficient vehicles, a modal shift to cycling, walking and collective transport, or mobility and urban planning that reduces demand for transport. In addition, schemes which accelerate the uptake of new, more efficient vehicles or policy measures which foster a shift to fuels with reduced levels of emissions, except schemes or policy measures regarding the use of direct fossil fuel combustion that reduce energy use per kilometre, are also capable of being eligible, subject to compliance with the rules on materiality and additionality set out in this Directive. Policy measures promoting the uptake of new fossil fuel vehicles should not qualify as eligible measures under the energy savings obligation.
- (67) Measures taken by Member States pursuant to Regulation (EU) 2018/842 of the European Parliament and of the Council ⁽²³⁾ and which result in verifiable and measurable or estimable energy efficiency improvements can be considered to be a cost-effective way for Member States to fulfil their energy savings obligation under this Directive.
- (68) As an alternative to requiring obligated parties to achieve the amount of cumulative end-use energy savings required under the energy savings obligation laid down in this Directive, it should be possible for Member States, in their obligation schemes, to permit or require obligated parties to contribute to a national energy efficiency fund, which could be used to implement policy measures as a priority among people affected by energy poverty, vulnerable customers, people in low income households and, where applicable, people living in social housing.
- (69) Member States and obligated parties should make use of all available means and technologies, except with regard to the use of direct fossil fuel combustion technologies, to achieve the cumulative end-use energy savings required, including by promoting smart and sustainable technologies in efficient district heating and cooling systems, efficient heating and cooling infrastructure, efficient and smart buildings, electrical vehicles and industries and energy audits or equivalent management systems, provided that the energy savings claimed comply with this Directive. Member States should aim for a high degree of flexibility in the design and implementation of alternative policy measures. Member States should encourage actions resulting in energy savings over a long lifetime.

⁽²³⁾ Regulation (EU) 2018/842 of the European Parliament and of the Council of 30 May 2018 on binding annual greenhouse gas emission reductions by Member States from 2021 to 2030 contributing to climate action to meet commitments under the Paris Agreement and amending Regulation (EU) No 525/2013 (OJ L 156, 19.6.2018, p. 26).

- (70) Long-term energy efficiency measures continue to deliver energy savings after 2020 but, in order to contribute to the Union's 2030 energy efficiency target, those measures should deliver new savings after 2020. On the other hand, energy savings achieved after 31 December 2020 should not count towards the cumulative end-use energy savings required for the period from 1 January 2014 to 31 December 2020.
- (71) Additionality is a fundamental underlying principle of the energy savings obligation provided for in this Directive, in so far as it ensures that Member States put in place policies and measures specifically designed for the purpose of fulfilling the energy savings obligation. New savings should be additional to 'business as usual', so that savings that would have occurred in any event should not count towards fulfilling the energy savings obligation. In order to calculate the impact of the measures introduced, only net savings, measured as the change of energy consumption that is directly attributable to the energy efficiency measure in question implemented for the purpose of the energy savings obligation provided for in this Directive, should be counted. To calculate net savings, Member States should establish a baseline scenario of how the situation would evolve in the absence of the measure in question. The policy measure in question should be evaluated against that baseline. Member States should take into account minimum requirements provided by the relevant legislative framework at Union level and the fact that other policy measures may be carried out in the same time frame which may also have an impact on the amount of energy savings, so that not all changes observed since the introduction of a particular policy measure can be attributed to that policy measure alone. The actions of the obligated, participating or entrusted party should in fact contribute to the achievement of the energy savings claimed in order to ensure the fulfilment of the materiality requirement.
- (72) It is important to consider, where relevant, all steps in the energy chain in the calculation of energy savings in order to increase the energy savings potential in the transmission and distribution of electricity. Studies and the consultation of stakeholders have revealed a significant potential. However, the physical and economic conditions are quite different among Member States, and often within several Member States, and there is a large number of system operators. Those circumstances point to a decentralised approach, pursuant to the subsidiarity principle. National Regulatory Authorities have the required knowledge, legal competences and the administrative capacity to promote the development of an energy efficient electricity grid. Entities such as the European Network of Transmission System Operators for Electricity (ENTSO-E) and the European Entity for Distribution System Operators can also provide useful contributions to, and should support their members in, the uptake of energy efficiency measures.
- (73) Similar considerations apply for the very large number of natural gas system operators. The role of natural gas and the rate of supply and coverage of the territory is highly variable among Member States. In those cases, National Regulatory Authorities are best placed to monitor and steer the system evolution towards an increased efficiency, and entities such as the European Network of Transmission System Operators for Gas can provide useful contributions to, and should support their members in, the uptake of energy efficiency measures.
- (74) The role of ESCOs is important in developing, designing, building, and arranging financing for projects that save energy, reduce energy costs, and decrease operations and maintenance costs in sectors such as buildings, industry and transport.
- (75) Consideration of the water-energy nexus is particularly important to address the interdependent use of energy and water and the increasing pressure on both resources. The effective management of water can make a significant contribution to energy savings yielding not only climate benefits, but also economic and social benefits. The water and wastewater sectors account for 3,5 % of electricity use in the Union and that share is expected to rise. At the same time, water leaks account for 24 % of total water consumed in the Union and the energy sector is the largest consumer of water, accounting for 44 % of consumption. The potential for energy savings through the use of smart technologies and processes across all industrial, residential and commercial water cycles and applications should be fully explored and realised whenever cost-effective, and the energy efficiency first principle should be considered. In addition, advanced irrigation technologies, rainwater harvesting and water reuse technologies could substantially reduce water consumption in agriculture, buildings and industry and the energy used for treating and transporting it.

- (76) In accordance with Article 9 of the Treaty on the Functioning of the European Union (TFEU), the Union's energy efficiency policies should be inclusive and should therefore ensure equal access to energy efficiency measures for all consumers affected by energy poverty. Improvements in energy efficiency should be implemented as a priority among people affected by energy poverty, vulnerable customers and final users, people in low-income or medium-income households, people living in social housing, older people as well as people living in rural and remote areas and in the outermost regions. In that context, specific attention should be paid to particular groups which are more at risk of being affected by energy poverty or are more susceptible to the adverse impacts of energy poverty, such as women, persons with disabilities, older people, children, and people with a minority racial or ethnic background. Member States can require obligated parties to include social aims in energy-saving measures in relation to energy poverty, and this possibility has already been extended to alternative policy measures and national energy efficiency funds. That should be transformed into an obligation to protect and empower vulnerable customers and final users and to alleviate energy poverty, while allowing Member States to retain full flexibility with regard to the type of policy measure, its size, scope and content. If an energy efficiency obligation scheme does not permit measures relating to individual energy consumers, the Member State may take measures to alleviate energy poverty by means of alternative policy measures alone. Within their policy mix, Member States should ensure that other policy measures do not have an adverse effect on people affected by energy poverty vulnerable customers, final users and, where applicable, people living in social housing. Member States should make best possible use of public funding investments into energy efficiency improvement measures, including funding and financial facilities established at Union level.
- (77) Each Member State should define the concept of vulnerable customers, which may refer to energy poverty and, inter alia, to the prohibition of disconnection of electricity to such customers in critical times. The concept of vulnerable customers may include income levels, the share of energy expenditure of disposable income, the energy efficiency of homes, critical dependence on electrical equipment for health reasons, age or other criteria. This allows Member States to include people in low-income households.
- (78) According to Recommendation (EU) 2020/1563, around 34 million households in the Union were unable to keep their home adequately warm in 2019. The European Green Deal prioritises the social dimension of the transition by committing to the principle that 'no one is left behind'. The green transition, including the clean transition, affects women and men differently and may have a particular impact on some disadvantaged groups including people with disabilities. Energy efficiency measures must therefore be central to any cost-effective strategy to address energy poverty and consumer vulnerability and are complementary to social security policies at Member State level. To ensure that energy efficiency measures reduce energy poverty for tenants sustainably, the cost-effectiveness of such measures, as well as their affordability to property owners and tenants, should be taken into account, and adequate financial and technical support for such measures should be guaranteed at Member State level. Member States should support the local and regional level in identifying and alleviating energy poverty. The Union's building stock needs, in the long term, to be converted to nearly zero-energy buildings in accordance with the objectives of the Paris Agreement. Current building renovation rates are insufficient and buildings occupied by citizens on low incomes who are affected by energy poverty are the hardest to reach. The measures laid down in this Directive with regard to energy savings obligations, energy efficiency obligation schemes and alternative policy measures are therefore of particular importance.
- (79) Member States should strive to ensure that measures to promote or facilitate energy efficiency, in particular those concerning buildings and mobility, do not lead to a disproportionate increase in the cost of services relating to such measures or to greater social exclusion.
- (80) To tap the energy savings potential in certain market segments where energy audits are generally not offered commercially, such as small and medium-sized enterprises (SMEs), Member States should develop programmes to encourage and support SMEs to undergo energy audits and to implement the recommendations arising from those energy audits. Energy audits should be mandatory and regular for enterprises with an average annual energy consumption above a certain threshold, as energy savings can be significant. Energy audits should take into account relevant European or international standards, such as EN ISO 50001 (Energy Management Systems), or EN 16247-1 (Energy Audits), or, if including an energy audit, EN ISO 14000 (Environmental Management Systems) and thus be also in accordance with this Directive, which does not go beyond the requirements of those relevant standards. A

specific European standard on energy audits is currently under development. Energy audits may be carried out on a stand-alone basis or be part of a broader environmental management system or an energy performance contract. In all such cases those systems should comply with the minimum requirements laid down in this Directive. In addition, specific mechanisms and schemes established to monitor emissions and fuel consumption by certain transport operators, for example under Union law the EU ETS, may be considered compatible with energy audits, including in energy management systems, if they comply with the minimum requirements laid down in this Directive. For those enterprises already implementing the energy audit obligation, energy audits should continue to be carried out at least every four years from the date of the previous energy audit, in accordance with this Directive.

- (81) Member States could establish guidelines for enterprises to follow in implementing measures to achieve new annual savings identified in the energy audit.
- (82) The enterprise's average consumption should be the criterion to define the application of energy management systems and of energy audits in order to increase the sensitivity of those mechanisms in identifying relevant opportunities for cost-effective energy savings. An enterprise that is below the consumption thresholds defined for energy management systems and energy audits should be encouraged to undergo energy audits and to implement the recommendations resulting from those audits.
- (83) Where energy audits are carried out by in-house experts, they should not be directly engaged in the activity audited in order to guarantee their independence.
- (84) Member States should promote the implementation of energy management systems and energy audits within the public administration at national, regional and local level.
- (85) The ICT sector is another important sector which receives increasing attention. In 2018 the energy consumption of data centres in the Union was 76,8 TWh. This is expected to rise to 98,5 TWh by 2030, a 28 % increase. This increase in absolute terms can also be seen in relative terms: within the Union, data centres accounted for 2,7 % of electricity demand in 2018 and will reach 3,21 % by 2030 if development continues on the current trajectory. The Union's Digital Strategy already highlighted the need for highly energy-efficient and sustainable data centres and calls for transparency measures for telecommunication operators on their environmental footprint. To promote sustainable development in the ICT sector, particularly of data centres, Member States should require the collection and publication of data which are relevant for the energy performance, water footprint and demand-side flexibility of data centres, on the basis of a common Union template. Member States should require the collection and publication of data only about data centres with a significant footprint, for which appropriate design or efficiency interventions, for new or existing installations respectively, can result in a considerable reduction of energy and water consumption, an increase in systems' efficiency promoting decarbonisation of the grid or in the reuse of waste heat in nearby facilities and heat networks. Data centre sustainability indicators could be established on the basis of that data collected, taking also into account already existing initiatives in the sector.
- (86) The reporting obligation applies to those data centres, which meet the threshold set out in this Directive. In all cases and specifically for onsite enterprise data centres, the reporting obligation should be understood as referring to the spaces and equipment that serve primarily or exclusively for data-related functions (server rooms), including the necessary associated equipment, for example, associated cooling, lighting, battery arrays, or uninterruptible power supplies. Any IT equipment placed or installed in primarily public access, common use or office space or supporting other corporate functions, such as workstations, laptops, photocopiers, sensors, security equipment, or white goods and audiovisual appliances should be excluded from the reporting obligation. The same exclusion should also apply to server, networking, storage, and associated equipment that would be scattered across a site such as single servers, single racks, or Wi-Fi and networking points.

- (87) The collected data should be used to measure at least some basic dimensions of a sustainable data centre, namely how efficiently it uses energy, how much of that energy comes from renewable energy sources, the reuse of any waste heat that it produces, the effectiveness of cooling, the effectiveness of carbon usage and the usage of freshwater. The collected data and the sustainability indicators should raise awareness among data centre owners and operators, manufacturers of equipment, developers of software and services, users of data centre services at all levels as well as entities and organisations that deploy, use or procure cloud and data centre services. The collected data and the sustainability indicators should also give confidence about the actual improvements following efforts and measures to increase the sustainability in new or existing data centres. Finally, those data and indicators should be used as a basis for transparent and evidence-based planning and decision making. The Commission should assess the efficiency of data centres on the basis of the information communicated by the obligated data centres.
- (88) Following an assessment, when establishing the possible sector-specific energy efficiency partnerships, the Commission should bring together key stakeholders, including non-governmental organisations and the social partners, in sectors such as ICT, transport, finance and buildings in an inclusive and representative manner.
- (89) Lower consumer spending on energy should be achieved by assisting consumers in reducing their energy use by reducing the energy needs of buildings and improvements in the efficiency of appliances, which should be combined with the availability of low-energy transport modes integrated with public transport, shared mobility and cycling. Member States should also consider improving connectivity in rural and remote areas.
- (90) It is crucial to raise the awareness of all Union citizens about the benefits of increased energy efficiency and to provide them with accurate information on the ways in which it can be achieved. Citizens of all ages should also be involved in the energy transition via the European Climate Pact and the Conference on the Future of Europe. Increased energy efficiency is also highly important for the security of energy supply of the Union through lowering its dependence on import of fuels from third countries.
- (91) The costs and benefits of all energy efficiency measures taken, including pay-back periods, should be made fully transparent to consumers.
- (92) When implementing this Directive and taking other measures in the field of energy efficiency, Member States should pay particular attention to synergies between energy efficiency measures and the efficient use of natural resources in line with the principles of the circular economy.
- (93) Taking advantage of new business models and technologies, Member States should endeavour to promote and facilitate the uptake of energy efficiency measures, including through innovative energy services for large and small customers.
- (94) It is necessary to provide for frequent and enhanced feedback on energy consumption where technically feasible and cost-efficient in view of the measurement devices in place. This Directive clarifies that the cost-efficiency of sub-metering depends on whether the related costs are proportionate to the potential energy savings. The assessment of whether sub-metering is cost-efficient may take into account the effect of other concrete, planned measures in a given building, such as any forthcoming renovation.
- (95) This Directive also clarifies that rights relating to billing, and information about billing or consumption should apply to consumers of heating, cooling or domestic hot water supplied from a central source even where they have no direct, individual contractual relationship with an energy supplier.

- (96) In order to achieve the transparency of accounting for individual consumption of thermal energy, and thereby facilitate the implementation of sub-metering, Member States should ensure they have in place transparent, publicly available national rules on the allocation of the cost of heating, cooling and domestic hot water consumption in multi-apartment and multi-purpose buildings. In addition to transparency, Member States could consider taking measures to strengthen competition in the provision of sub-metering services and thereby help ensure that any costs borne by the final users are reasonable.
- (97) Newly installed heat meters and heat cost allocators should be remotely readable to ensure cost-effective, and frequent provision of, consumption information. The provisions of this Directive relating to metering for heating, cooling and domestic hot water; sub-metering and cost allocation for heating, cooling and domestic hot water; remote reading requirement; billing and consumption information for heating and cooling and domestic hot water; the cost of access to metering and billing and consumption information for heating, cooling and domestic hot water; and the minimum requirements for billing and consumption information for heating, cooling and domestic hot water, are intended to apply only to heating, cooling and domestic hot water supplied from a central source. Member States are free to decide whether walk-by or drive-by technologies are to be considered remotely readable or not. Remotely readable devices do not require access to individual apartments or units to be read.
- (98) Member States should take into account the fact that the successful implementation of new technologies for measuring energy consumption requires enhanced investment in education and skills for both users and energy suppliers.
- (99) Billing information and annual statements are an important means by which customers are informed of their energy consumption. Data on consumption and costs can also convey other information that helps consumers to compare their current deal with other offers and to make use of complaint-management and alternative dispute-resolution mechanisms. However, considering that bill-related disputes are a common source of consumer complaints and a factor which contributes to persistently low levels of consumer satisfaction and engagement with their energy providers, it is necessary to make bills simpler, clearer and easier to understand, while ensuring that separate instruments, such as billing information, information tools and annual statements, provide all the necessary information to enable consumers to regulate their energy consumption, compare offers and switch suppliers.
- (100) When designing energy efficiency improvement measures, Member States should take due account of the need to ensure the correct functioning of the internal market and the consistent implementation of the *acquis*, in accordance with the TFEU.
- (101) High-efficiency cogeneration and efficient district heating and cooling have significant potential for saving primary energy in the Union. Member States should carry out a comprehensive assessment of the potential for high-efficiency cogeneration and efficient district heating and cooling. Those assessments should be consistent with Member States' integrated national energy and climate plans and their long-term renovation strategies, and could include trajectories leading to a renewable energy and waste heat based national heating and cooling sector within a timeframe compatible with the achievement of the climate neutrality objective. New electricity generation installations and existing installations which are substantially refurbished or whose permit or licence is updated should, subject to a cost-benefit analysis showing a cost-benefit surplus, be equipped with high-efficiency cogeneration units to recover waste heat stemming from the production of electricity. Similarly, other facilities with substantial annual average energy input should be equipped with technical solutions to deploy waste heat from the facility where the cost-benefit analysis shows a cost-benefit surplus. This waste heat could be transported where it is needed through district heating networks. The events that trigger a requirement for authorisation criteria to be applied will generally be such as to also trigger requirements for permits under Directive 2010/75/EU and for authorisation under Directive (EU) 2019/944.

- (102) It may be appropriate for electricity generation installations that are intended to make use of geological storage permitted under Directive 2009/31/EC of the European Parliament and of the Council ⁽²⁴⁾ to be located in places where the recovery of waste heat, through high-efficiency cogeneration or by supplying a district heating or cooling network, is not cost-effective. Member States should therefore be able to exempt those installations from the obligation to carry out a cost-benefit analysis for providing the installation with equipment allowing the recovery of waste heat by means of a high-efficiency cogeneration unit. It should also be possible to exempt peak-load and back-up electricity generation installations which are planned to operate under 1 500 operating hours per year as a rolling average over a period of five years from the requirement to also provide heat.
- (103) It is appropriate for Member States to encourage the introduction of measures and procedures to promote cogeneration installations with a total rated thermal input of less than 5 MW in order to encourage distributed energy generation.
- (104) To implement national comprehensive assessments, Member States should encourage the assessments of the potential for high-efficiency cogeneration and efficient district heating and cooling at regional and local level. Member States should take steps to promote and facilitate the realisation of the identified cost-efficient potential of high-efficiency cogeneration and efficient district heating and cooling.
- (105) Requirements for efficient district heating and cooling should be consistent with long-term climate policy goals, the climate and environmental standards and the priorities of the Union, and should comply with the principle of 'do no significant harm' within the meaning of Regulation (EU) 2020/852. All the district heating and cooling systems should aim for improved ability to interact with other parts of the energy system in order to optimise the use of energy and prevent energy waste by using the full potential of buildings to store heat or cold, including the excess heat from service facilities and nearby data centres. For that reason, efficient district heating and cooling systems should ensure the increase of primary energy efficiency and a progressive integration of renewable energy and waste heat and cold as defined in Directive (EU) 2018/2001 of the European Parliament and of the Council ⁽²⁵⁾. Therefore, this Directive introduces progressively stricter requirements for heating and cooling supply which should be applicable during specific established time periods and should be permanently applicable from 1 January 2050 onwards.
- (106) The principles to calculate the share of the heat or cold from renewable energy sources in efficient district heating and cooling should be consistent with Directive (EU) 2018/2001 and Eurostat methodologies for statistical reporting. Pursuant to Article 7(1) of Directive (EU) 2018/2001, the gross final consumption of energy from renewable sources includes gross final consumption of energy from renewable sources in the heating and cooling sector. A gross final energy consumption of heat or cold in district heating or cooling equals heat or cold energy supply going into the network serving the final customers or energy distributors.
- (107) Heat pumps are important for the decarbonisation of the heating and cooling supply, also in district heating. The methodology established in Annex VII to Directive (EU) 2018/2001 provides rules to count energy captured by heat pumps as energy from renewable sources and prevents double counting of the electricity from renewable sources. For the purposes of calculating the share of renewable energy in a district heating network, all the heat originating from the heat pump and going into the network should be accounted as renewable energy, provided that the heat pump meets the minimum efficiency criteria set out in Annex VII to Directive (EU) 2018/2001 at the time of its installation.

⁽²⁴⁾ Directive 2009/31/EC of the European Parliament and of the Council of 23 April 2009 on the geological storage of carbon dioxide and amending Council Directive 85/337/EEC, European Parliament and Council Directives 2000/60/EC, 2001/80/EC, 2004/35/EC, 2006/12/EC, 2008/1/EC and Regulation (EC) No 1013/2006 (OJ L 140, 5.6.2009, p. 114).

⁽²⁵⁾ Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (OJ L 328, 21.12.2018, p. 82).

- (108) High-efficiency cogeneration has been defined by the energy savings obtained by combined production instead of separate production of heat and electricity. Requirements for high-efficiency cogeneration should be consistent with long-term climate policy goals. The definitions of cogeneration and high-efficiency cogeneration used in Union legislation should be without prejudice to the use of different definitions in national legislation for purposes other than those of the Union legislation in question. To maximise energy savings and avoid energy saving opportunities being missed, the greatest attention should be paid to the operating conditions of cogeneration units.
- (109) To ensure transparency and allow the final customer to choose between electricity from cogeneration and electricity produced by other techniques, the origin of high-efficiency cogeneration should be guaranteed on the basis of harmonised efficiency reference values. Guarantee of origin schemes do not of themselves imply a right to benefit from national support mechanisms. It is important that all forms of electricity produced from high-efficiency cogeneration can be covered by guarantees of origin. Guarantees of origin should be distinguished from exchangeable certificates.
- (110) The specific structure of the cogeneration and district heating and cooling sectors, which include many producers that are SMEs, should be taken into account, especially when reviewing the administrative procedures for obtaining permission to construct cogeneration capacity or associated networks, in application of the 'think small first' principle.
- (111) Most Union businesses are SMEs. They represent an enormous energy saving potential for the Union. To help them adopt energy efficiency measures, Member States should establish a favourable framework aimed at providing SMEs with technical assistance and targeted information.
- (112) Member States should establish, on the basis of objective, transparent and non-discriminatory criteria, rules governing the bearing and sharing of costs of grid connections and grid reinforcements and rules for technical adaptations needed to integrate new producers of electricity produced from high-efficiency cogeneration, taking into account network codes and guidelines developed in accordance with Regulations (EU) 2019/943 ⁽²⁶⁾ and (EC) No 715/2009 of the European Parliament and of the Council ⁽²⁷⁾. Producers of electricity generated from high-efficiency cogeneration should be allowed to issue a call for tender for the connection work. Access to the grid system for electricity produced from high-efficiency cogeneration, especially for small scale and micro-cogeneration units, should be facilitated. In accordance with Article 3(2) of Directive 2009/73/EC and Article 9(2) of Directive (EU) 2019/944, it is possible for Member States to impose public service obligations, including in relation to energy efficiency, on enterprises operating in the electricity and gas sectors.
- (113) It is necessary to set out provisions relating to billing, single point of contact, out-of-court dispute settlement, energy poverty and basic contractual rights, with the aim of aligning them, where appropriate, with the relevant provisions regarding electricity pursuant to Directive (EU) 2019/944, in order to strengthen consumer protection and enable final customers to receive more frequent, clear and up-to-date information about their heating, cooling or domestic hot water consumption and to regulate their energy use.
- (114) This Directive strengthens the protection of consumers by introducing basic contractual rights for district heating, cooling and domestic hot water, coherent with the level of rights, protection and empowerment that Directive (EU) 2019/944 has introduced for final customers in the electricity sector. Plain and unambiguous information concerning their rights should be made available to consumers. Several factors impede consumers from accessing, understanding and acting upon the various sources of market information available to them. The introduction of basic contractual rights can help, among others, with a proper understanding of the baseline of the quality of services offered in the contract by the supplier, including the quality and characteristics of the supplied energy. In addition, it can contribute to the minimisation of hidden or extra costs that could result from the introduction of

⁽²⁶⁾ Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (OJ L 158, 14.6.2019, p. 54).

⁽²⁷⁾ Regulation (EC) No 715/2009 of the European Parliament and of the Council of 13 July 2009 on conditions for access to the natural gas transmission networks and repealing Regulation (EC) No 1775/2005 (OJ L 211, 14.8.2009, p. 36).

either upgraded or new services after the signing of the contract without a clear understanding and agreement by the customer. Those services could concern, among others, the energy supplied, metering and billing services, purchase and installation or ancillary and maintenance services and costs relating to the network, metering devices, local heating or cooling equipment. The requirements will contribute to the improvement of comparability of offers and ensure the same level of basic contractual rights for all Union citizens regarding heating, cooling and domestic hot water, without restricting national competences.

- (115) In the case of planned disconnection from heating, cooling and domestic hot water, suppliers should provide the customers concerned with adequate information on alternative measures, such as sources of support to avoid disconnection, prepayment systems, energy audits, energy consultancy services, alternative payment plans, debt management advice or disconnection moratoria.
- (116) Greater consumer protection should be guaranteed through the availability of effective, independent out-of-court dispute settlement mechanisms for all consumers, such as an energy ombudsperson, a consumer body or a regulatory authority. Member States should, therefore, introduce speedy and effective complaint-handling procedures.
- (117) The contribution of renewable energy communities, pursuant to Directive (EU) 2018/2001, and citizen energy communities, pursuant to Directive (EU) 2019/944, towards the objectives of the European Green Deal and the Climate Target Plan, should be recognised and actively supported. Member States should, therefore, consider and promote the role of renewable energy communities and citizen energy communities. Those communities can help Member States to achieve the objectives of this Directive by advancing energy efficiency at local or household level, as well as in public buildings, in cooperation with local authorities. They can empower and engage consumers and enable certain groups of household customers, including in rural and remote areas, to participate in energy efficiency projects and interventions that can combine actions with investment in renewable energy. Energy communities can have a strong role to play in educating and increasing citizens' awareness of measures designed to achieve energy savings. If properly supported by Member States, energy communities can help fighting energy poverty through the facilitation of energy efficiency projects, reduced energy consumption and lower supply tariffs.
- (118) Long-term behavioural changes in energy consumption can be achieved through the empowerment of citizens. Energy communities can help deliver long-term energy savings, particularly among households, and an increase in sustainable investments from citizens and small businesses. Member States should empower such actions by citizens through support for community energy projects and organisations. In addition, engagement strategies, involving all relevant stakeholders at national and local level in the policy-making process, can be part of the local or regional decarbonisation plans or national buildings renovation plans, with the objective of increasing awareness, obtaining feedback on policies and improving their acceptance by the public.
- (119) The contribution of one-stop shops or similar structures as mechanisms that can enable multiple target groups, including citizens, SMEs and public authorities, to design and implement projects and measures relating to the clean energy transition should be recognised. The contribution of one-stop shops can be very important for vulnerable customers, as they could receive reliable and accessible information about energy efficiency improvements. That contribution can include the provision of technical, administrative and financial advice and assistance, the facilitation of the necessary administrative procedures or of access to financial markets, guidance with regard to the Union and national legal frameworks, including public procurement rules and criteria, and the EU taxonomy.
- (120) The Commission should review the impact of its measures to support the development of platforms or fora, involving, inter alia, the European social dialogue bodies, on fostering training programmes for energy efficiency, and should propose further measures where appropriate. The Commission should also encourage the European social partners in their discussions on energy efficiency, especially for vulnerable customers and final users, including those in energy poverty.

- (121) A fair transition towards a climate-neutral Union by 2050 is central to the European Green Deal. The European Pillar of Social Rights, jointly proclaimed by the European Parliament, the Council and the Commission on 17 November 2017, includes energy among the essential services that everyone is entitled to access. Support for access to such services must be available for those in need, particularly in a context of inflationary pressure and significant increases in energy prices.
- (122) It is necessary to ensure that people affected by energy poverty, vulnerable customers, people in low-income households and, where applicable, people living in social housing are protected and, to that end, empowered to actively participate in the energy efficiency improvement interventions, measures and related consumer protection or information measures that Member States implement. Targeted awareness-raising campaigns should be developed to illustrate the benefits of energy efficiency as well to provide information on the financial support available.
- (123) Public funding available at Union and national level should be strategically invested into energy efficiency improvement measures, in particular for the benefit of people affected by energy poverty, vulnerable customers, people in low-income households and, where applicable, people living in social housing. Member States should take advantage of any financial contribution they might receive from the Social Climate Fund established by Regulation (EU) 2023/955 of the European Parliament and of the Council ⁽²⁸⁾, and of revenues from allowances from the EU ETS. Those revenues will support Member States in fulfilling their obligation to implement energy efficiency measures and policy measures under the energy savings obligation as a priority among people affected by energy poverty, vulnerable customers, people in low-income households and, where applicable, people living in social housing including those living in rural and remote regions.
- (124) National funding schemes should be complemented by suitable schemes of better information, technical and administrative assistance, and easier access to finance that will enable the best use of the available funds especially by people affected by energy poverty, vulnerable customers, people in low-income households and, where applicable, people living in social housing.
- (125) Member States should empower and protect all people equally, irrespective of sex, gender, age, disability, race or ethnic origin, sexual orientation, religion or belief, and ensure that those most affected, those put at greater risk of being affected by energy poverty, or those most exposed to the adverse impacts of energy poverty are adequately protected. In addition, Member States should ensure that energy efficiency measures do not exacerbate any existing inequalities, in particular with respect to energy poverty.
- (126) Pursuant to Article 15(2) of Directive 2012/27/EU, all Member States have undertaken an assessment of the energy efficiency potential of their gas and electricity infrastructure, and have identified concrete measures and investments for the introduction of cost-effective energy efficiency improvements in the network infrastructure, with a timetable for their introduction. The results of those actions represent a solid basis for the application of the energy efficiency first principle in their network planning, network development and investment decisions.
- (127) National energy regulatory authorities should take an integrated approach encompassing potential savings in the energy supply and the end-use sectors. Without prejudice to security of supply, market integration and anticipatory investments in offshore grids necessary for the deployment of offshore renewable energy, national energy regulatory authorities should ensure that the energy efficiency first principle is applied in the planning and decision-making processes and that network tariffs and regulations incentivise improvements in energy efficiency. Member States should also ensure that transmission and distribution system operators consider the energy efficiency first principle. That would help transmission and distribution system operators to consider better energy efficiency solutions for and incremental costs incurred from the procurement of demand-side resources, as well as the

⁽²⁸⁾ Regulation (EU) 2023/955 of the European Parliament and of the Council of 10 May 2023 establishing a Social Climate Fund and amending Regulation (EU) 2021/1060 (OJ L 130, 16.5.2023, p. 1).

environmental and socio-economic impacts of different network investments and operation plans. Such an approach requires a shift from the narrow economic efficiency perspective to maximised social welfare. The energy efficiency first principle should in particular be applied in the context of scenario building for energy infrastructure expansion where demand-side solutions could be considered as viable alternatives and need to be properly assessed, and should become an intrinsic part of the assessment of network planning projects. Its application should be scrutinised by national regulatory authorities.

- (128) A sufficient number of reliable professionals competent in the field of energy efficiency should be available to ensure the effective and timely implementation of this Directive, for instance as regards compliance with the requirements on energy audits and implementation of energy efficiency obligation schemes. Member States should therefore put in place certification or equivalent qualification, or both, and suitable training schemes for the providers of energy services, energy audits and other energy efficiency improvement measures in close cooperation with the social partners, training providers and other relevant stakeholders. The schemes should be assessed every four years starting as of December 2024 and, if needed, be updated to ensure the necessary level of competences for energy services providers, energy auditors, energy managers and installers of building elements.
- (129) It is necessary to continue developing the market for energy services to ensure the availability of both the demand for and the supply of energy services. Transparency, for example by means of lists of certified energy services providers and available model contracts, exchange of best practices and guidelines greatly contribute to the uptake of energy services and energy performance contracting and can also help stimulate demand and increase the trust in energy services providers. In an energy performance contract the beneficiary of the energy service avoids investment costs by using part of the financial value of energy savings to fully or partially repay the investment carried out by a third party. That can help attract private capital which is key for increasing building renovation rates in the Union, bring expertise into the market and create innovative business models. Therefore, non-residential buildings with the useful floor area above 750 m² should be required to assess the feasibility of using energy performance contracting for renovation. That is a step ahead to increase the trust in energy services companies and pave the way for increasing such projects in the future.
- (130) Given the ambitious renovation objectives over the next decade in the context of the Renovation Wave, it is necessary to increase the role of independent market intermediaries including one-stop shops or similar support mechanisms in order to stimulate market development on the demand and supply sides and to promote energy performance contracting for renovation of both private and public buildings. Local energy agencies could play a key role in that regard, and identify and support setting up potential facilitators or one-stop shops. This Directive should help improve the availability of products, services and advice, including by promoting the potential for entrepreneurs to fill the gaps in the market and to provide for innovative ways to enhance energy efficiency, while ensuring respect for the principle of non-discrimination.
- (131) Energy performance contracting still faces important barriers in several Member States due to remaining regulatory and non-regulatory barriers. It is therefore necessary to address the ambiguities of the national legislative frameworks, lack of expertise, especially as regards tendering procedures, and competing loans and grants.
- (132) Member States should continue supporting the public sector in the uptake of energy performance contracting by providing model contracts that take into account the available European or international standards, tendering guidelines and the Guide to the Statistical Treatment of Energy Performance Contracts published in May 2018 by Eurostat and the European Investment Bank (EIB) on the treatment of energy performance contracting in government accounts, which have provided opportunities for addressing remaining regulatory barriers to those contracts in Member States.

- (133) Member States have taken measures to identify and address regulatory and non-regulatory barriers. However, there is a need to increase the effort to remove regulatory and non-regulatory barriers to the use of energy performance contracting and third-party financing arrangements which help achieve energy savings. Those barriers include accounting rules and practices that prevent capital investments and annual financial savings resulting from energy efficiency improvement measures from being adequately reflected in the accounts for the whole life of the investment.
- (134) Member States used the 2014 and 2017 national energy efficiency action plans to report progress in removing regulatory and non-regulatory barriers to energy efficiency, as regards split incentives between owners and tenants or among owners of a building or building units. Member States should continue working in that direction and tap the potential for energy efficiency in the context of the 2016 Eurostat statistics, in particular the fact that more than four out of ten Europeans live in flats and more than three out of ten Europeans are tenants.
- (135) Member States, including regional and local authorities, should be encouraged to make full use of the European funds available under the multiannual financial framework for the years 2021 to 2027 laid down in Council Regulation (EU, Euratom) 2020/2093 ⁽²⁹⁾ the Recovery and Resilience Facility, established by Regulation (EU) 2021/241 of the European Parliament and of the Council ⁽³⁰⁾, as well as the financial instruments and technical assistance available under the InvestEU programme, established by Regulation (EU) 2021/523 of the European Parliament and of the Council ⁽³¹⁾, to trigger private and public investments in energy efficiency improvement measures. Investment in energy efficiency has the potential to contribute to economic growth, employment, innovation and a reduction in energy poverty in households, and therefore makes a positive contribution to economic, social and territorial cohesion and green recovery. Potential areas for funding include energy efficiency measures in public buildings and housing, and providing new skills through the development of training, reskilling and upskilling of professionals, in particular in jobs related to building renovation, to promote employment in the energy efficiency sector. The Commission will ensure synergies between the different funding instruments, in particular the funds in shared management and in direct management, such as the centrally-managed programmes Horizon Europe and LIFE, as well as between grants, loans and technical assistance to maximise their leverage effect on private financing and their impact on the achievement of energy efficiency policy objectives.
- (136) Member States should encourage the use of financing facilities to further the objectives of this Directive. Such financing facilities could include financial contributions and fines for infringements of certain provisions of this Directive, resources allocated to energy efficiency under Article 10(3) of Directive 2003/87/EC, and resources allocated to energy efficiency in the European funds and programmes, and dedicated European financial instruments, such as the European Energy Efficiency Fund.
- (137) Financing facilities could be based, where applicable, on resources allocated to energy efficiency from Union project bonds, resources allocated to energy efficiency from the EIB and other European financial institutions, in particular the European Bank for Reconstruction and Development (EBRD) and the Council of Europe Development Bank, resources leveraged in financial institutions, national resources, including through the creation of regulatory and fiscal frameworks encouraging the implementation of energy efficiency initiatives and programmes, and revenues from annual emission allocations under Decision No 406/2009/EC of the European Parliament and of the Council ⁽³²⁾.

⁽²⁹⁾ Council Regulation (EU, Euratom) 2020/2093 of 17 December 2020 laying down the multiannual financial framework for the years 2021 to 2027 (OJ L 433 I, 22.12.2020, p. 11).

⁽³⁰⁾ Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility (OJ L 57, 18.2.2021, p. 17).

⁽³¹⁾ Regulation (EU) 2021/523 of the European Parliament and of the Council of 24 March 2021 establishing the InvestEU Programme and amending Regulation (EU) 2015/1017 (OJ L 107, 26.3.2021, p. 30).

⁽³²⁾ Decision No 406/2009/EC of the European Parliament and of the Council of 23 April 2009 on the effort of Member States to reduce their greenhouse gas emissions to meet the Community's greenhouse gas emission reduction commitments up to 2020 (OJ L 140, 5.6.2009, p. 136).

- (138) The financing facilities could in particular use contributions, resources and revenues from those resources to enable and encourage private capital investment, in particular drawing on institutional investors, while using criteria ensuring the achievement of both environmental and social objectives for the granting of funds; make use of innovative financing mechanisms, including loan guarantees for private capital, loan guarantees to foster energy performance contracting, grants, subsidised loans and dedicated credit lines, third-party financing systems, that reduce the risks of energy efficiency projects and allow for cost-effective renovations even among low- and medium-revenue households; be linked to programmes or agencies which will aggregate and assess the quality of energy saving projects, provide technical assistance, promote the energy services market and help to generate consumer demand for energy services.
- (139) The financing facilities could also provide appropriate resources to support training and certification programmes which improve and accredit skills for energy efficiency, provide resources for research on and demonstration and acceleration of uptake of small-scale and micro technologies in the generation of energy and the optimisation of the connections of those generators to the grid, be linked to programmes undertaking action to promote energy efficiency in all dwellings to prevent energy poverty and stimulate landlords letting dwellings to render their property as energy-efficient as possible, and provide appropriate resources to support social dialogue and standard-setting with the aim of improving energy efficiency and ensuring good working conditions and health and safety at work.
- (140) Available Union funding programmes, financial instruments and innovative financing mechanisms should be used to give practical effect to the objective of improving the energy performance of public bodies' buildings. In that respect, Member States may use their revenues from annual emission allocations under Decision No 406/2009/EC in the development of such mechanisms on a voluntary basis and taking into account national budgetary rules. The Commission and the Member States should provide regional and local administrations with adequate information on such Union funding programmes, financial instruments and innovative financing mechanisms.
- (141) In the implementation of the energy efficiency target, the Commission should monitor the impact of the relevant measures on Directive 2003/87/EC in order to maintain the incentives in the EU ETS rewarding low carbon investments and to prepare the EU ETS sectors for the innovations needed in the future. It will need to monitor the impact on those industry sectors which are exposed to a significant risk of carbon leakage as listed in the Annex to Commission Decision 2014/746/EU ⁽³³⁾, in order to ensure that this Directive promotes and does not impede the development of those sectors.
- (142) Member State measures should be supported by well-designed and effective Union financial instruments under the InvestEU programme, and by financing from the EIB and the EBRD, which should support investments in energy efficiency at all stages of the energy chain and use a comprehensive cost-benefit analysis with a model of differentiated discount rates. Financial support should focus on cost-effective methods for increasing energy efficiency, which would lead to a reduction in energy consumption. The EIB and the EBRD should, together with national promotional banks, design, generate and finance programmes and projects tailored for the efficiency sector, including for energy-poor households.
- (143) Cross-sectoral law provides a strong basis for consumer protection for a wide range of current energy services, and is likely to evolve. Nevertheless, certain basic contractual rights of customers should be clearly established. Plain and unambiguous information should be made available to consumers concerning their rights in relation to the energy sector.
- (144) In order to be able to evaluate the effectiveness of this Directive, a requirement to conduct a general review of this Directive and to submit a report to the European Parliament and to the Council by 28 February 2027 should be laid down. That review should allow necessary alignments, also taking into account economic and innovation developments.

⁽³³⁾ Commission Decision 2014/746/EU of 27 October 2014 determining, pursuant to Directive 2003/87/EC of the European Parliament and of the Council, a list of sectors and subsectors which are deemed to be exposed to a significant risk of carbon leakage, for the period 2015 to 2019 (OJ L 308, 29.10.2014, p. 114).

- (145) Local and regional authorities should be given a leading role in the development and design, execution and assessment of the measures laid down in this Directive, so that they are able properly to address the specific features of their own climate, culture and society.
- (146) Reflecting technological progress and the growing share of renewable energy sources in the electricity generation sector, the default coefficient for savings in kWh electricity should be reviewed in order to reflect changes in the primary energy factor for electricity and other energy carriers. The calculation methodology is in accordance with the Eurostat energy balances and definitions, except for the allocation method of fuel input for heat and electricity in combined heat and power plants, for which the efficiency of the reference system, required for the allocation of fuel consumption, was aligned with Eurostat data for 2015 and 2020. Calculations reflecting the energy mix of the primary energy factor for electricity are based on annual average values. The 'physical energy content' accounting method is used for nuclear electricity and heat generation and the 'technical conversion efficiency' method is used for electricity and heat generation from fossil fuels and biomass. For non-combustible renewable energy, the method is the direct equivalent based on the 'total primary energy' approach. To calculate the primary energy share for electricity in cogeneration, the method set out in this Directive is applied. An average rather than a marginal market position is used. Conversion efficiencies are assumed to be 100 % for non-combustible renewables, 10 % for geothermal power stations and 33 % for nuclear power stations. The calculation of total efficiency for cogeneration is based on the most recent data from Eurostat. The conversion, transmission and distribution losses are taken into account. Distribution losses for energy carriers other than electricity are not considered in the calculations, due to the lack of reliable data and the complexity of the calculation. As for system boundaries, the primary energy factor is 1 for all energy sources. The selected coefficient for the primary energy factor for electricity is the average of 2024 and 2025 values, since a forward-looking primary energy factor will provide a more appropriate indicator than a historical one. The analysis covers the Member States and Norway. The dataset for Norway is based on the ENTSO-E data.
- (147) Energy savings which result from the implementation of Union law should not be claimed unless they result from a measure that goes beyond the minimum required by the Union legal act in question, whether by setting more ambitious energy efficiency requirements at Member State level or by increasing the take-up of the measure. Buildings present a substantial potential for further increasing energy efficiency, and the renovation of buildings is an essential and long-term element with economies of scale in increasing energy savings. It is therefore necessary to clarify that it is possible to claim all energy savings stemming from measures promoting the renovation of existing buildings, provided that they exceed the savings that would have occurred in the absence of the policy measure and provided that the Member State demonstrates that the obligated, participating or entrusted party has in fact contributed to the achievement of the energy savings claimed.
- (148) In accordance with the communication of the Commission of 25 February 2015 on 'A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy' and the principles of better regulation, monitoring and verification rules for the implementation of energy efficiency obligation schemes and alternative policy measures, including the requirement to check a statistically representative sample of measures, should be given greater prominence.
- (149) Energy generated on or in buildings from renewable energy technologies reduces the amount of energy supplied from fossil fuels. The reduction of energy consumption and the use of energy from renewable sources in the buildings sector are important measures to reduce the Union's energy dependence and GHG emissions, especially in view of the ambitious climate and energy objectives set for 2030 as well as the global commitment made in the context of the Paris Agreement. For the purposes of their cumulative energy savings obligation, it is possible for Member States to take into account energy savings from policy measures promoting renewable technologies to meet their energy savings requirements in accordance with the calculation methodology provided for in this Directive. Energy savings from policy measures regarding the use of direct fossil fuel combustion should not be counted.

- (150) Some of the changes introduced by this Directive might require a subsequent amendment to Regulation (EU) 2018/1999 in order to ensure coherence between the two legal acts. New provisions, mainly relating to setting national contributions, gap filling mechanisms and reporting obligations, should be streamlined with and transferred to that Regulation, once it is amended. Some provisions of Regulation (EU) 2018/1999 might also need to be reassessed in view of the changes proposed in this Directive. The additional reporting and monitoring requirements should not create any new parallel reporting systems but would be subject to the existing monitoring and reporting framework under Regulation (EU) 2018/1999.
- (151) To foster the practical implementation of this Directive at national, regional and local level, the Commission should continue to support the exchange of experiences on practices, benchmarking, networking activities, as well as innovative practices by means of an online platform.
- (152) Since the objectives of this Directive, namely to achieve the Union's energy efficiency target and to pave the way towards further energy efficiency improvements and towards climate neutrality, cannot be sufficiently achieved by the Member States but can rather, by reason of the scale and effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.
- (153) In order to permit adaptation to technical progress and changes in the distribution of energy sources, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of the review of the harmonised efficiency reference values laid down on the basis of this Directive, in respect of the values, calculation methods, default primary energy coefficient and requirements in the Annexes to this Directive and in respect of supplementing this Directive by establishing a common Union scheme for rating the sustainability of data centres located in its territory. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making ⁽³⁴⁾. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.
- (154) Regulation (EU) 2023/955 should be amended in order to take account of the definition of energy poverty established in this Directive. That would ensure consistency, coherence, complementarity and synergy among different instruments and funding in particular addressing households in energy poverty.
- (155) The obligation to transpose this Directive into national law should be confined to those provisions which represent a substantive amendment as compared to the earlier Directive. The obligation to transpose the provisions which are unchanged arises under the earlier Directive.
- (156) This Directive should be without prejudice to the obligations of the Member States relating to the time-limits for the transposition into national law of the Directives set out in Part B of Annex XVI,

⁽³⁴⁾ OJ L 123, 12.5.2016, p. 1.

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

SUBJECT MATTER, SCOPE, DEFINITIONS AND ENERGY EFFICIENCY TARGETS

Article 1

Subject matter and scope

1. This Directive establishes a common framework of measures to promote energy efficiency within the Union in order to ensure that the Union's targets on energy efficiency are met and enables further energy efficiency improvements. The aim of that common framework is to contribute to the implementation of Regulation (EU) 2021/1119 of the European Parliament and of the Council ⁽³⁵⁾ and to the Union's security of energy supply by reducing its dependence on energy imports, including fossil fuels.

This Directive lays down rules designed to implement energy efficiency as a priority across all sectors, remove barriers in the energy market and overcome market failures that impede efficiency in the supply, transmission, storage and use of energy. It also provides for the establishment of indicative national energy efficiency contributions for 2030.

This Directive contributes to the implementation of the energy efficiency first principle, thus also contributing to the Union being an inclusive, fair and prosperous society with a modern, resource-efficient and competitive economy.

2. The requirements laid down in this Directive are minimum requirements and shall not prevent any Member State from maintaining or introducing more stringent measures. Such measures shall comply with Union law. Where national legislation provides for more stringent measures, the Member State shall notify such legislation to the Commission.

Article 2

Definitions

For the purposes of this Directive, the following definitions apply:

- (1) 'energy' means energy products as defined in Article 2, point (d), of Regulation (EC) No 1099/2008 of the European Parliament and of the Council ⁽³⁶⁾;
- (2) 'energy efficiency first' means energy efficiency first as defined in Article 2, point (18), of Regulation (EU) 2018/1999;
- (3) 'energy system' means a system primarily designed to supply energy-services to satisfy the demand of end-use sectors for energy in the forms of heat, fuels, and electricity;
- (4) 'system efficiency' means the selection of energy-efficient solutions where they also enable a cost-effective decarbonisation pathway, additional flexibility and the efficient use of resources;
- (5) 'primary energy consumption' or 'PEC' means gross available energy, excluding international maritime bunkers, final non-energy consumption and ambient energy;

⁽³⁵⁾ Regulation (EU) 2021/1119 of the European Parliament and of the Council of 30 June 2021 establishing the framework for achieving climate neutrality and amending Regulations (EC) No 401/2009 and (EU) 2018/1999 ('European Climate Law') (OJ L 243, 9.7.2021, p. 1).

⁽³⁶⁾ Regulation (EC) No 1099/2008 of the European Parliament and of the Council of 22 October 2008 on energy statistics (OJ L 304, 14.11.2008, p. 1).

- (6) 'final energy consumption' or 'FEC' means all energy supplied to industry, to transport, including energy consumption in international aviation, to households, to public and private services, to agriculture, to forestry, to fishing and to other end-use sectors, excluding energy consumption in international maritime bunkers, ambient energy and deliveries to the transformation sector and to the energy sector, and losses due to transmission and distribution as defined in Annex A to Regulation (EC) No 1099/2008;
- (7) 'ambient energy' means ambient energy as defined in Article 2, point (2), of Directive (EU) 2018/2001;
- (8) 'energy efficiency' means the ratio of output of performance, service, goods or energy to input of energy;
- (9) 'energy savings' means an amount of saved energy determined by measuring or estimating consumption, or both, before and after the implementation of an energy efficiency improvement measure, whilst ensuring normalisation for external conditions that affect energy consumption;
- (10) 'energy efficiency improvement' means an increase in energy efficiency as a result of any technological, behavioural or economic changes;
- (11) 'energy service' means the physical benefit, utility or good derived from a combination of energy with energy-efficient technology or with action, which may include the operations, maintenance and control necessary to deliver the service, which is delivered on the basis of a contract and in normal circumstances has proven to result in verifiable and measurable or estimable energy efficiency improvement or primary energy savings;
- (12) 'public bodies' means national, regional or local authorities and entities directly financed and administered by those authorities but not having an industrial or commercial character;
- (13) 'total useful floor area' means the floor area of a building, or part of a building, where energy is used to condition the indoor climate;
- (14) 'contracting authorities' means contracting authorities as defined in Article 6(1) of Directive 2014/23/EU, Article 2(1), point (1), of Directive 2014/24/EU and Article 3(1) of Directive 2014/25/EU;
- (15) 'contracting entities' means contracting entities as defined in Article 7(1) of Directive 2014/23/EU and Article 4(1) of Directive 2014/25/EU;
- (16) 'energy management system' means a set of interrelated or interacting elements of a strategy which sets an energy efficiency objective and a plan to achieve that objective, including the monitoring of actual energy consumption, actions taken to increase energy efficiency and the measurement of progress;
- (17) 'European standard' means a standard adopted by the European Committee for Standardization, the European Committee for Electrotechnical Standardization or the European Telecommunications Standards Institute, which is made available for public use;
- (18) 'international standard' means a standard adopted by the International Organization for Standardization, which is made available for public use;
- (19) 'obligated party' means an energy distributor, retail energy sales company or transmission system operator, which is bound by the national energy efficiency obligation schemes referred to in Article 9;
- (20) 'entrusted party' means a legal entity with delegated power from a government or other public body to develop, manage or operate a financing scheme on behalf of that government or other public body;
- (21) 'participating party' means an enterprise or public body that has committed itself to reaching certain objectives under a voluntary agreement, or that is covered by a national regulatory policy instrument;

- (22) 'implementing public authority' means a body governed by public law which is responsible for the carrying out or monitoring of energy or carbon taxation, financial schemes and instruments, fiscal incentives, standards and norms, energy labelling schemes, training or education;
- (23) 'policy measure' means a regulatory, financial, fiscal, voluntary or information provision instrument formally established and implemented in a Member State to create a supportive framework, requirement or incentive for market actors to provide and purchase energy services and to undertake other energy efficiency improvement measures;
- (24) 'individual action' means an action that leads to verifiable and measurable or estimable energy efficiency improvements and that is undertaken as a result of a policy measure;
- (25) 'energy distributor' means a natural or legal person, including a distribution system operator, who is responsible for transporting energy with a view to its delivery to final customers or to distribution stations that sell energy to final customers;
- (26) 'distribution system operator' means distribution system operator as defined in Article 2, point (29), of Directive (EU) 2019/944 as regards electricity or Article 2, point (6), of Directive 2009/73/EC as regards gas;
- (27) 'retail energy sales company' means a natural or legal person who sells energy to final customers;
- (28) 'final customer' means a natural or legal person who purchases energy for own end use;
- (29) 'energy service provider' means a natural or legal person who delivers energy services or energy efficiency improvement measures in a final customer's facility or premises;
- (30) 'small and medium-sized enterprises' or 'SMEs' means enterprises as defined in Article 2(1) of the Annex to Commission Recommendation 2003/361/EC ⁽³⁷⁾;
- (31) 'microenterprise' means an enterprise as defined in Article 2(3) of the Annex to Recommendation 2003/361/EC;
- (32) 'energy audit' means a systematic procedure with the purpose of obtaining adequate knowledge of the energy consumption profile of a building or group of buildings, an industrial or commercial operation or installation or a private or public service, identifying and quantifying opportunities for cost-effective energy savings, identifying the potential for cost-effective use or production of renewable energy and reporting the findings;
- (33) 'energy performance contracting' means a contractual arrangement between the beneficiary and the provider of an energy efficiency improvement measure, verified and monitored during the whole term of the contract, where the works, supply or service in that measure are paid for in relation to a contractually agreed level of energy efficiency improvement or another agreed energy performance criterion, such as financial savings;
- (34) 'smart metering system' means smart metering system as defined in Article 2, point (23), of Directive (EU) 2019/944 or intelligent metering system as referred to in Directive 2009/73/EC;
- (35) 'transmission system operator' means transmission system operator as defined in Article 2, point (35), of Directive (EU) 2019/944 as regards electricity or Article 2, point (4), of Directive 2009/73/EC as regards gas;
- (36) 'cogeneration' means the simultaneous generation in one process of thermal energy and electrical or mechanical energy;
- (37) 'economically justifiable demand' means a demand that does not exceed the needs for heating or cooling and which would otherwise be satisfied at market conditions by energy generation processes other than cogeneration;

⁽³⁷⁾ Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

- (38) 'useful heat' means heat produced in a cogeneration process to satisfy an economically justifiable demand for heating or cooling;
- (39) 'electricity from cogeneration' means electricity generated in a process linked to the production of useful heat and calculated in accordance with the general principles set out in Annex II;
- (40) 'high-efficiency cogeneration' means cogeneration meeting the criteria laid down in Annex III;
- (41) 'overall efficiency' means the annual sum of electricity and mechanical energy production and useful heat output divided by the fuel input used for heat produced in a cogeneration process and gross electricity and mechanical energy production;
- (42) 'power-to-heat ratio' means the ratio of electricity from cogeneration to useful heat when operating in full cogeneration mode using operational data of the specific unit;
- (43) 'cogeneration unit' means a unit that is able to operate in cogeneration mode;
- (44) 'small-scale cogeneration unit' means a cogeneration unit with installed capacity below 1 MW_e;
- (45) 'micro-cogeneration unit' means a cogeneration unit with a maximum capacity below 50 kW_e;
- (46) 'efficient district heating and cooling' means a district heating or cooling system meeting the criteria laid down in Article 26;
- (47) 'efficient heating and cooling' means a heating and cooling option that, compared to a baseline scenario reflecting a business-as-usual situation, measurably reduces the input of primary energy needed to supply one unit of delivered energy within a relevant system boundary in a cost-effective way, as assessed in the cost-benefit analysis referred to in this Directive, taking into account the energy required for extraction, conversion, transport and distribution;
- (48) 'efficient individual heating and cooling' means an individual heating and cooling supply option that, compared to efficient district heating and cooling, measurably reduces the input of non-renewable primary energy needed to supply one unit of delivered energy within a relevant system boundary or requires the same input of non-renewable primary energy but at a lower cost, taking into account the energy required for extraction, conversion, transport and distribution;
- (49) 'data centre' means data centre as defined in Annex A, point 2.6.3.1.16, of Regulation (EC) No 1099/2008;
- (50) 'substantial refurbishment' means a refurbishment the cost of which exceeds 50 % of the investment cost for a new comparable unit;
- (51) 'aggregator' means independent aggregator as defined in Article 2, point (19), of Directive (EU) 2019/944;
- (52) 'energy poverty' means a household's lack of access to essential energy services, where such services provide basic levels and decent standards of living and health, including adequate heating, hot water, cooling, lighting, and energy to power appliances, in the relevant national context, existing national social policy and other relevant national policies, caused by a combination of factors, including at least non-affordability, insufficient disposable income, high energy expenditure and poor energy efficiency of homes;
- (53) 'final user' means a natural or legal person purchasing heating, cooling or domestic hot water for their own end use, or a natural or legal person occupying an individual building or a unit in a multi-apartment or multi-purpose building supplied with heating, cooling or domestic hot water from a central source, where such a person has no direct or individual contract with the energy supplier;

- (54) 'split incentives' means the lack of fair and reasonable distribution of financial obligations and rewards relating to energy efficiency investments among the actors concerned, for example the owners and tenants or the different owners of building units, or owners and tenants or different owners of multi-apartment or multi-purpose buildings.
- (55) 'engagement strategy' means a strategy that sets objectives, develops techniques and establishes the process by which to involve all relevant stakeholders at national or local level, including civil society representatives such as consumer organisations, in the policy-making process, with the goal of increasing awareness, obtaining feedback on such policies and improving their public acceptance.
- (56) 'statistically significant proportion and representative sample of the energy efficiency improvement measures' means such a proportion and sample which require the establishment of a subset of a statistical population of the energy savings measures in question in such a way as to reflect the entire population of all energy savings measures, and thus allow for reasonably reliable conclusions regarding confidence in the totality of the measures.

Article 3

Energy efficiency first principle

1. In accordance with the energy efficiency first principle, Member States shall ensure that energy efficiency solutions, including demand-side resources and system flexibilities, are assessed in planning, policy and major investment decisions of a value of more than EUR 100 000 000 each or EUR 175 000 000 for transport infrastructure projects, relating to the following sectors:

- (a) energy systems; and
- (b) non-energy sectors, where those sectors have an impact on energy consumption and energy efficiency such as buildings, transport, water, information and communications technology (ICT), agriculture and financial sectors.

2. By 11 October 2027, the Commission shall carry out an assessment of the thresholds set out in paragraph 1, with the aim of downward revision, taking into account possible developments in the economy and in the energy market. The Commission shall, by 11 October 2028, submit a report to the European Parliament and to the Council, followed, where appropriate, by legislative proposals.

3. In applying this Article, Member States are encouraged to take into account Commission Recommendation (EU) 2021/1749 ⁽³⁸⁾.

4. Member States shall ensure that the competent authorities monitor the application of the energy efficiency first principle, including, where appropriate, sector integration and cross-sectoral impacts, where policy, planning and investment decisions are subject to approval and monitoring requirements.

5. In applying the energy efficiency first principle, Member States shall:

- (a) promote and, where cost-benefit analyses are required, ensure the application of, and make publicly available, cost-benefit methodologies that allow proper assessment of the wider benefits of energy efficiency solutions where appropriate, taking into account the entire life cycle and long-term perspective, system and cost efficiency, security of supply and quantification from the societal, health, economic and climate neutrality perspectives, sustainability and circular economy principles in transition to climate neutrality;
- (b) address the impact on energy poverty;

⁽³⁸⁾ Commission Recommendation (EU) 2021/1749 of 28 September 2021 on Energy Efficiency First: from principles to practice — Guidelines and examples for its implementation in decision-making in the energy sector and beyond (OJ L 350, 4.10.2021, p. 9).

- (c) identify an entity or entities responsible for monitoring the application of the energy efficiency first principle and the impacts of regulatory frameworks, including financial regulations, planning, policy and the major investment decisions referred to in paragraph 1 on energy consumption, energy efficiency and energy systems;
 - (d) report to the Commission, as part of their integrated national energy and climate progress reports submitted pursuant to Article 17 of Regulation (EU) 2018/1999, on how the energy efficiency first principle was taken into account in the national and, where applicable, regional and local planning, policy and major investment decisions related to the national and regional energy systems including at least the following:
 - (i) an assessment of the application and benefits of the energy efficiency first principle in energy systems, in particular in relation to energy consumption;
 - (ii) a list of actions taken to remove any unnecessary regulatory or non-regulatory barriers to the implementation of the energy efficiency first principle and of demand-side solutions, including through the identification of national legislation and measures that are contrary to the energy efficiency first principle.
6. By 11 April 2024, the Commission shall adopt guidelines providing a common general framework including supervision, the monitoring and reporting procedure, which Member States may use to design the cost-benefit methodologies referred to in paragraph 5, point (a), for the purpose of comparability, while leaving the possibility for Member States to adapt to national and local circumstances.

Article 4

Energy efficiency targets

1. Member States shall collectively ensure a reduction of energy consumption of at least 11,7 % in 2030 compared to the projections of the 2020 EU Reference Scenario so that the Union's final energy consumption amounts to no more than 763 Mtoe. Member States shall make efforts to collectively contribute to the indicative Union primary energy consumption target amounting to no more than 992,5 Mtoe in 2030.
2. Each Member State shall set an indicative national energy efficiency contribution based on final energy consumption to meet, collectively, the Union's binding final energy consumption target referred to in paragraph 1 of this Article and shall make efforts to contribute collectively to the Union's indicative primary energy consumption target referred to in that paragraph. Member States shall notify those contributions to the Commission, together with an indicative trajectory for those contributions, as part of the updates of their integrated national energy and climate plans submitted pursuant to Article 14(2) of Regulation (EU) 2018/1999, and of their integrated national energy and climate plans notified pursuant to Article 3 and Articles 7 to 12 of that Regulation. When doing so, Member States shall also express their contributions in terms of an absolute level of primary energy consumption in 2030. When setting their indicative national energy efficiency contributions, Member States shall take into account the requirements set out in paragraph 3 of this Article and explain how, and on the basis of which data, the contributions have been calculated. To that end, they may use the formula set out in Annex I to this Directive.

Member States shall provide the shares of primary energy consumption and final energy consumption of energy end-use sectors, as defined in Regulation (EC) No 1099/2008, including industry, residential, services and transport, in their national energy efficiency contributions. Member States shall also indicate projections for energy consumption in ICT.

3. In setting their indicative national energy efficiency contributions referred to in paragraph 2, Member States shall take into account:
- (a) the Union's 2030 final energy consumption target of no more than 763 Mtoe and the primary energy consumption target of no more than 992,5 Mtoe, as provided for in paragraph 1;

- (b) the measures provided for in this Directive;
- (c) other measures to promote energy efficiency within Member States and at Union level;
- (d) any relevant factors affecting efficiency efforts:
 - (i) early efforts and actions in energy efficiency;
 - (ii) the equitable distribution of efforts across the Union;
 - (iii) the energy intensity of the economy;
 - (iv) the remaining cost-effective energy-saving potential;
- (e) other national circumstances affecting energy consumption, in particular:
 - (i) GDP and demographic evolution and forecast;
 - (ii) changes of energy imports and exports, developments in the energy mix and the deployment of new sustainable fuels;
 - (iii) the development of all sources of renewable energies, nuclear energy, carbon capture and storage;
 - (iv) the decarbonisation of energy intensive industries;
 - (v) the level of ambition in the national decarbonisation or climate neutrality plans;
 - (vi) economic energy savings potential;
 - (vii) current climate conditions and climate change forecast.

4. When applying the requirements set out in paragraph 3, a Member State shall ensure that its contribution in Mtoe is not more than 2,5 % above what it would have been had it resulted from the formula set out in Annex I.

5. The Commission shall assess that the collective contribution of Member States is at least equal to the Union's binding target for final energy consumption set out in paragraph 1 of this Article. Where the Commission concludes that it is insufficient, as part of its assessment of the draft updated national energy and climate plans pursuant to Article 9(2) of Regulation (EU) 2018/1999, or at the latest by 1 March 2024, taking into consideration the updated 2020 EU Reference Scenario pursuant to this paragraph, the Commission shall submit to each Member State a corrected indicative national energy efficiency contribution for final energy consumption on the basis of:

- (a) the remaining collective reduction of final energy consumption needed to achieve the Union's binding target set out in paragraph 1;
- (b) the relative GHG intensity per GDP unit in 2019 among the Member States concerned;
- (c) the GDP of those Member States in 2019.

Before applying the formula in Annex I for the mechanism established in this paragraph and at the latest by 30 November 2023, the Commission shall update the 2020 EU Reference Scenario on the basis of the latest Eurostat data reported by the Member States, in accordance with Article 4(2), point (b), and Article 14 of Regulation (EU) 2018/1999.

Notwithstanding Article 37 of this Directive, Member States that wish to update their indicative national energy efficiency contributions pursuant to paragraph 2 of this Article, using the updated 2020 EU Reference Scenario, shall notify their updated indicative national energy efficiency contribution at the latest by 1 February 2024. Where a Member State wishes to update its indicative national energy efficiency contribution, it shall ensure that its contribution in Mtoe is not more than 2,5 % above what it would have been had it resulted from the formula set out in Annex I with the use of the updated 2020 EU Reference Scenario.

Member States to which a corrected indicative national energy efficiency contribution was submitted by the Commission shall update their indicative national energy efficiency contributions pursuant to paragraph 2 of this Article, with the corrected indicative national energy efficiency contribution for final energy consumption together with an update of their indicative trajectory for those contribution and, where applicable, their additional measures, as part of the updates of their integrated national energy and climate plans submitted pursuant to Article 14(2) of Regulation (EU) 2018/1999. The Commission shall, in accordance with that Regulation, require Member States to submit, without delay, their corrected indicative energy efficiency contribution and, where applicable, their additional measures to ensure the application of the mechanism set out in this paragraph.

Where a Member State has notified an indicative national energy efficiency contribution for final energy consumption in Mtoe equal to or below what it would have been had it resulted from the formula set out in Annex I, the Commission shall not amend that contribution.

When applying the mechanism set out in this paragraph, the Commission shall ensure that there is no difference left between the sum of the national contributions of all Member States and the Union's binding target set out in paragraph 1.

6. Where the Commission concludes, on the basis of its assessment pursuant to Article 29(1) and (3) of Regulation (EU) 2018/1999, that insufficient progress has been made towards meeting the energy efficiency contributions, Member States that are above their indicative trajectories for final energy consumption referred to in paragraph 2 of this Article shall ensure that additional measures are implemented within one year of the date of receipt of the Commission's assessment in order to get back on track to reach their energy efficiency contributions. Those additional measures shall include, but shall not be limited to, at least one of the following measures:

- (a) national measures delivering additional energy savings, including stronger project development assistance for the implementation of energy efficiency investment measures;
- (b) increasing the energy savings obligation set out in Article 8 of this Directive;
- (c) adjusting the obligation for public sector;
- (d) making a voluntary financial contribution to the national energy efficiency fund referred to in Article 30 of this Directive or another financing instrument dedicated to energy efficiency, where the annual financial contributions shall be equal to the investments required to reach the indicative trajectory.

Where a Member State's final energy consumption is above its indicative trajectory for final energy consumption referred to in paragraph 2 of this Article, it shall include in its integrated national energy and climate progress report submitted pursuant to Article 17 of Regulation (EU) 2018/1999 an explanation of the measures it will take to cover the gap in order to ensure that it reaches its national energy efficiency contributions and the amount of energy savings expected to be delivered.

The Commission shall assess whether the national measures referred to in this paragraph are sufficient to achieve the Union's energy efficiency targets. Where national measures are deemed to be insufficient, the Commission shall, as appropriate, propose measures and exercise its power at Union level in order to ensure, in particular, the achievement of the Union's 2030 targets for energy efficiency.

7. The Commission shall assess by 31 December 2026 any methodological changes in the data reported pursuant to Regulation (EC) No 1099/2008, in the methodology for calculating energy balance, and in energy models for European energy use, and, if necessary, propose technical calculation adjustments to the Union's 2030 targets with a view to maintaining the level of ambition set out in paragraph 1 of this Article.

CHAPTER II

EXEMPLARY ROLE OF PUBLIC SECTOR

*Article 5***Public sector leading on energy efficiency**

1. Member States shall ensure that the total final energy consumption of all public bodies combined is reduced by at least 1,9 % each year, when compared to 2021.

Member States may choose to exclude public transport or the armed forces from the obligation laid down in the first subparagraph.

For the purposes of the first and second subparagraphs, Member States shall establish a baseline, which includes the final energy consumption of all public bodies, except in public transport or the armed forces, for 2021. Energy consumption reduction of public transport and armed forces is indicative and may still count for fulfilling the obligation under the first subparagraph even if excluded from the baseline under this Article.

2. During a transitional period ending on 11 October 2027 the target set out in paragraph 1 shall be indicative. During that transitional period, Member States may use estimated consumption data, and, by the same date, Member States shall adjust the baseline and align the estimated final energy consumption of all public bodies to the actual final energy consumption of all public bodies.

3. The obligation laid down in paragraph 1 shall not include, until 31 December 2026, the energy consumption of public bodies in local administrative units with a population of less than 50 000 and, until 31 December 2029, the energy consumption of public bodies in local administrative units with a population of less than 5 000 inhabitants.

4. A Member State may take into account climatic variations within it when calculating its public bodies' final energy consumption.

5. Member States shall include in the updates, submitted pursuant to Article 14(2) of Regulation (EU) 2018/1999, of their national energy and climate plans, notified pursuant to Article 3 and Articles 7 to 12 of that Regulation, the amount of energy consumption reduction to be achieved by all public bodies, disaggregated by sector, and the measures that they plan to adopt for the purpose of achieving those reductions. As part of their integrated national energy and climate progress reports submitted pursuant to Article 17 of Regulation (EU) 2018/1999, Member States shall report to the Commission the final energy consumption reduction achieved every year.

6. Member States shall ensure that regional and local authorities establish specific energy efficiency measures in their long-term planning tools, such as decarbonisation or sustainable energy plans, after consulting relevant stakeholders, including energy agencies where appropriate, and the public, including, in particular, vulnerable groups which are at risk of being affected by energy poverty or are more susceptible to its effects.

Member States shall also ensure that the competent authorities take actions to mitigate significant negative direct or indirect impacts of energy efficiency measures on energy poor, low-income households or vulnerable groups when designing and implementing energy efficiency measures.

7. Member States shall support public bodies. Such support may, without prejudice to the State aid rules, include financial and technical support, for the purpose of taking up energy efficiency improvement measures and encouraging public bodies to take into account the wider benefits beyond energy savings, for example the quality of the indoor environment, including at regional and local level, by providing guidelines, promoting competence building, the acquisition of skills and training opportunities, and by encouraging cooperation among public bodies.

8. Member States shall encourage public bodies to consider life cycle carbon emissions as well as the economic and social benefits of their public bodies' investment and policy activities.

9. Member States shall encourage public bodies to improve the energy performance of buildings owned or occupied by public bodies, including by means of the replacement of old and inefficient heaters.

Article 6

Exemplary role of public bodies' buildings

1. Without prejudice to Article 7 of Directive 2010/31/EU, each Member State shall ensure that at least 3 % of the total floor area of heated and/or cooled buildings that are owned by public bodies is renovated each year to be transformed into at least nearly zero-energy buildings or zero-emission buildings in accordance with Article 9 of Directive 2010/31/EU.

Member States may choose which buildings to include in the 3 % renovation requirement, giving due consideration to cost-effectiveness and technical feasibility in the choice of buildings to renovate.

Member States may exempt social housing from the obligation to renovate referred to in the first subparagraph where such renovations would not be cost neutral or would lead to rent increases for people living in social housing unless such rent increases are no higher than the economic savings on the energy bill.

Where public bodies occupy a building that they do not own, they shall negotiate with the owner, in particular when reaching a trigger point such as the renewal of rental, change of use, significant repair or maintenance work, with the aim of establishing contractual clauses for the building to become at least a nearly zero-energy building or zero-emission building.

The rate of at least 3 % shall be calculated on the total floor area of buildings which have a total useful floor area of over 250 m², that are owned by public bodies and that, on 1 January 2024, are not nearly zero-energy buildings.

2. Member States may apply requirements that are less stringent than those laid down in paragraph 1 for the following categories of buildings:

- (a) buildings officially protected as part of a designated environment, or because of their special architectural or historical merit, in so far as compliance with certain minimum energy performance requirements would alter their character or appearance unacceptably;
- (b) buildings owned by the armed forces or central government and serving national defence purposes, apart from single living quarters or office buildings for the armed forces and other staff employed by national defence authorities;
- (c) buildings used as places of worship and for religious activities.

Member States may decide not to renovate any building that is not referred to in the first subparagraph of this paragraph up to the level provided for in paragraph 1 if they assess that it is not technically, economically or functionally feasible for that building to be transformed into a nearly zero-energy building. Where they so decide, Member States shall not count the renovation of that building towards the fulfilment of the requirement set out in paragraph 1.

3. In order to front load energy savings and to provide an incentive for early action, a Member State that renovates more than 3 % of the total floor area of its buildings in accordance with paragraph 1 in any year until 31 December 2026 may count the surplus towards the annual renovation rate of any of the following three years. A Member State that renovates more than 3 % of the total floor area of its buildings as of 1 January 2027 may count the surplus towards the annual renovation rate of the following two years.

4. Member States may count towards the annual renovation rate of buildings new buildings owned as replacements for specific public bodies' buildings demolished in any of the two previous years. This shall apply only where they would be more cost effective and sustainable in terms of the energy and lifecycle CO₂ emissions achieved compared to the renovations of such buildings. The general criteria, methodologies and procedures to identify such exceptional cases shall be clearly set out and published by each Member State.

5. By 11 October 2025, Member States shall, for the purposes of this Article, establish and make publicly available and accessible an inventory of heated and/or cooled buildings that are owned or occupied by public bodies and that have a total useful floor area of more than 250 m². Member States shall update that inventory at least every two years. The inventory shall be linked to the building stock overview carried out in the framework of the national building renovation plans in accordance with Directive 2010/31/EU and the relevant databases.

Publicly available and accessible data about building stock characteristics, buildings renovation and energy performance may be aggregated by the EU Building Stock Observatory to ensure a better understanding of the energy performance of the building sector through comparable data.

The inventory shall contain at least the following data:

- (a) the floor area in m²;
- (b) the measured annual energy consumption of heat, cooling, electricity and hot water when those data are available;
- (c) the energy performance certificate of each building issued in accordance with Directive 2010/31/EU.

6. Member States may decide to apply an alternative approach to that set out in paragraphs 1 to 4 for the purpose of achieving, every year, an amount of energy savings in the buildings of public bodies which is at least equivalent to the amount required in paragraph 1.

For the purpose of applying that alternative approach, Member States shall:

- (a) ensure that, each year, a renovation passport is introduced, where applicable, for buildings representing at least 3 % of the total floor area of heated and/or cooled buildings that are owned by public bodies. For those buildings, the renovation to nearly zero-energy building shall be achieved at the latest by 2040;
- (b) estimate the energy savings that paragraphs 1 to 4 would generate by using appropriate standard values for the energy consumption of reference public bodies' buildings before and after renovation to be transformed into nearly zero-energy buildings as referred to in Directive 2010/31/EU.

Member States that decide to apply the alternative approach shall notify to the Commission, by 31 December 2023, their projected energy savings to achieve at least the equivalent of energy savings in the buildings covered by paragraph 1 by 31 December 2030.

Article 7

Public procurement

1. Member States shall ensure that contracting authorities and contracting entities, when concluding public contracts and concessions with a value equal to or greater than the thresholds laid down in Article 8 of Directive 2014/23/EU, Article 4 of Directive 2014/24/EU and Article 15 of Directive 2014/25/EU, purchase only products, services buildings and works with high energy-efficiency performance in accordance with the requirements referred to in Annex IV to this Directive, unless it is not technically feasible.

Member States shall also ensure that in concluding the public contracts and concessions with a value equal to or greater than the thresholds referred to in the first subparagraph, contracting authorities and contracting entities apply the energy efficiency first principle in accordance with Article 3, including for those public contracts and concessions for which no specific requirements are provided for in Annex IV.

2. The obligations referred to in paragraph 1 of this Article shall not apply if they undermine public security or impede the response to public health emergencies. The obligations referred to in paragraph 1 of this Article shall apply to the contracts of the armed forces only to the extent that their application does not cause any conflict with the nature and primary aim of the activities of the armed forces. The obligations shall not apply to contracts for the supply of military equipment as defined in Directive 2009/81/EC of the European Parliament and of the Council ⁽³⁹⁾.

3. Notwithstanding Article 29(4), Member States shall ensure that contracting authorities and contracting entities assess the feasibility of concluding long-term energy performance contracts that provide long-term energy savings when procuring service contracts with significant energy content.

4. Without prejudice to paragraph 1 of this Article, when purchasing a product package fully covered by a delegated act adopted under Regulation (EU) 2017/1369, Member States may require that the aggregate energy efficiency take priority over the energy efficiency of individual products within that package, by purchasing the product package that complies with the criterion of belonging to the highest available energy efficiency class.

5. Member States may require that contracting authorities and contracting entities, when concluding contracts as referred to in paragraph 1 of this Article, take into account, where appropriate, wider sustainability, social, environmental and circular economy aspects in procurement practices with a view to achieving the Union's decarbonisation and zero pollution objectives. Where appropriate, and in accordance with Annex IV, Member States shall require contracting authorities and contracting entities to take into account Union green public procurement criteria or available equivalent national criteria.

To ensure transparency in the application of energy efficiency requirements in the procurement process, Member States shall ensure that contracting authorities and contracting entities make publicly available information on the energy efficiency impact of contracts with a value equal to or greater than the thresholds referred to in paragraph 1 by publishing that information in the respective notices on Tenders Electronic Daily (TED), in accordance with Directives 2014/23/EU, 2014/24/EU and 2014/25/EU, and Commission Implementing Regulation (EU) 2019/1780 ⁽⁴⁰⁾. Contracting authorities may decide to require that tenderers disclose information on the life cycle global warming potential, the use of low carbon materials and the circularity of materials used for a new building and for a building to be renovated. Contracting authorities may make that information publicly available for the contracts, in particular for new buildings having a floor area larger than 2 000 m².

Member States shall support contracting authorities and contracting entities in the uptake of energy efficiency requirements, including at regional and local level, by providing clear rules and guidelines including methodologies on the assessment of life cycle costs and environment impacts and costs, setting up competence support centres, encouraging cooperation amongst contracting authorities, including across borders, and using aggregated procurement and digital procurement where possible.

⁽³⁹⁾ Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC (OJ L 216, 20.8.2009, p. 76).

⁽⁴⁰⁾ Commission Implementing Regulation (EU) 2019/1780 of 23 September 2019 establishing standard forms for the publication of notices in the field of public procurement and repealing Implementing Regulation (EU) 2015/1986 (eForms) (OJ L 272, 25.10.2019, p. 7)

6. Where appropriate, the Commission may provide further guidance to national authorities and procurement officials in the application of energy efficiency requirements in the procurement process. Such support may strengthen existing fora for the purpose of supporting Member States, such as by means of concerted action, and may assist them in taking the green public procurement criteria into account.

7. Member States shall establish the legal and regulatory provisions, and administrative practices, regarding public purchasing and annual budgeting and accounting, necessary to ensure that individual contracting authorities are not deterred from making investments in improving energy efficiency and from using energy performance contracting and third-party financing mechanisms on a long-term contractual basis.

8. Member States shall remove any regulatory or non-regulatory barriers to energy efficiency, in particular as regards legal and regulatory provisions, and administrative practices, regarding public purchasing and annual budgeting and accounting, with a view to ensuring that individual public bodies are not deterred from making investments in improving energy efficiency and from using energy performance contracting and third-party financing mechanisms on a long-term contractual basis.

Member States shall report to the Commission on the measures taken to address the barriers to uptake of energy efficiency improvements as part of their integrated national energy and climate progress reports submitted pursuant to Article 17 of Regulation (EU) 2018/1999.

CHAPTER III

EFFICIENCY IN ENERGY USE

Article 8

Energy savings obligation

1. Member States shall achieve cumulative end-use energy savings at least equivalent to:
 - (a) new savings each year from 1 January 2014 to 31 December 2020 of 1,5 % of annual energy sales to final customers by volume, averaged over the most recent three-year period preceding 1 January 2013. Sales of energy, by volume, used in transport may be excluded, in whole or in part, from that calculation;
 - (b) new savings each year from 1 January 2021 to 31 December 2030 of:
 - (i) 0,8 % of annual final energy consumption from 1 January 2021 to 31 December 2023, averaged over the most recent three-year period preceding 1 January 2019;
 - (ii) 1,3 % of annual final energy consumption from 1 January 2024 to 31 December 2025, averaged over the most recent three-year period preceding 1 January 2019;
 - (iii) 1,5 % of annual final energy consumption from 1 January 2026 to 31 December 2027, averaged over the most recent three-year period preceding 1 January 2019;
 - (iv) 1,9 % of annual final energy consumption from 1 January 2028 to 31 December 2030, averaged over the most recent three-year period preceding 1 January 2019.

By way of derogation from point (b)(i) of the first subparagraph, Cyprus and Malta shall achieve new savings each year from 1 January 2021 to 31 December 2023, equivalent to 0,24 % of annual final energy consumption, averaged over the most recent three-year period prior to 1 January 2019.

By way of derogation from points (b)(ii), (iii) and (iv) of the first subparagraph, Cyprus and Malta shall achieve new savings each year from 1 January 2024 to 31 December 2030 equivalent to 0,45 % of annual FEC, averaged over the most recent three-year period preceding 1 January 2019.

Member States shall decide how to phase the calculated quantity of new savings over each period referred to in points (a) and (b) of the first subparagraph, provided that the required total cumulative end-use energy savings have been achieved by the end of each obligation period.

Member States shall continue to achieve new annual savings in accordance with the savings rate provided for in point (b)(iv) of the first subparagraph for ten-year periods after 2030.

2. Member States shall achieve the amount of energy savings required under paragraph 1 of this Article either by establishing an energy efficiency obligation scheme as referred to in Article 9 or by adopting alternative policy measures as referred to in Article 10. Member States may combine an energy efficiency obligation scheme with alternative policy measures. Member States shall ensure that energy savings resulting from the policy measures referred to in Articles 9 and 10 and Article 30(14) are calculated in accordance with Annex V.

3. Member States shall implement energy efficiency obligation schemes, alternative policy measures, or a combination of both, or programmes or measures financed under a national energy efficiency fund, as a priority among, but not limited to, people affected by energy poverty, vulnerable customers, people in low-income households and, where applicable, people living in social housing. Member States shall ensure that policy measures implemented pursuant to this Article have no adverse effect on those persons. Where applicable, Member States shall make the best possible use of funding, including public funding, funding facilities established at Union level, and revenues from allowances pursuant to Article 24(3), point (b), with the aim of removing adverse effects and ensuring a just and inclusive energy transition.

For the purpose of achieving the energy savings required under paragraph 1 and without prejudice to Regulation (EU) 2019/943 and Directive (EU) 2019/944, Member States shall, for the purpose of designing such policy measures, consider and promote the role of renewable energy communities and citizen energy communities in the contribution to the implementation towards those policy measures.

Member States shall establish and achieve a share of the required amount of cumulative end-use energy savings among people affected by energy poverty, vulnerable customers, people in low-income households and, where applicable, people living in social housing. This share shall at least be equal to the proportion of households in energy poverty as assessed in their national energy and climate plans established in accordance with Article 3(3), point (d), of Regulation (EU) 2018/1999. Member States shall, in their assessment of the share of energy poverty in their national energy and climate plans, consider the following indicators:

- (a) the inability to keep the home adequately warm (Eurostat, SILC [ilc_mdcs01]);
- (b) the arrears on utility bills (Eurostat, SILC [ilc_mdcs07]);
- (c) the total population living in a dwelling with a leaking roof, damp walls, floors or foundation, or rot in window frames or floor (Eurostat, SILC [ilc_mdho01]);
- (d) at-risk-of-poverty rate (Eurostat, SILC and ECHP surveys [ilc_li02]) (cutoff point: 60 % of median equivalised income after social transfers).

If a Member State has not notified the share of households in energy poverty as assessed in their national energy and climate plan, the share of the required amount of cumulative end-use energy savings among people affected by energy poverty, vulnerable customers, people in low-income households and, where applicable, people living in social housing, shall be at least equal to the arithmetic average share of the indicators referred to in the third subparagraph for the year 2019 or, if not available for 2019, for the linear extrapolation of their values for the last three years that are available.

4. Member States shall include information about the indicators applied, the arithmetic average share and the outcome of policy measures established in accordance with paragraph 3 of this Article in the updates of their integrated national energy and climate plans submitted pursuant to Article 14(2) of Regulation (EU) 2018/1999, in their subsequent integrated national energy and climate plans notified pursuant to Article 3 and Articles 7 to 12 of that Regulation, and in the related national energy and climate progress reports submitted pursuant to Article 17 of that Regulation.

5. Member States may count energy savings that stem from policy measures, whether introduced by 31 December 2020 or after that date, provided that those measures result in new individual actions that are carried out after 31 December 2020. Energy savings achieved in any obligation period shall not count towards the amount of required energy savings for the previous obligation periods set out in paragraph 1.

6. Provided that Member States achieve at least their cumulative end-use energy savings obligation referred to in paragraph 1, first subparagraph, point (b)(i), they may calculate the required amount of energy savings referred to in that point by one or more of the following means:

- (a) applying an annual savings rate on energy sales to final customers or on final energy consumption, averaged over the most recent three-year period preceding 1 January 2019;
- (b) excluding, in whole or in part, energy used in transport from the calculation baseline;
- (c) making use of any of the options set out in paragraph 8.

7. Where Member States make use of any of the possibilities provided for in paragraph 6 regarding the required energy savings referred to in paragraph 1, first subparagraph, point (b)(i), they shall establish:

- (a) their own annual savings rate that will be applied in the calculation of their cumulative end-use energy savings, which shall ensure that the final amount of their net energy savings is no lower than those required under that point;
- (b) their own calculation baseline, which may exclude, in whole or in part, energy used in transport.

8. Subject to paragraph 9, each Member State may:

- (a) carry out the calculation required under paragraph 1, first subparagraph, point (a), using values of 1 % in 2014 and 2015, 1,25 % in 2016 and 2017, and 1,5 % in 2018, 2019 and 2020;
- (b) exclude from the calculation all or part of the sales of energy used, by volume, with respect to the obligation period referred to in paragraph 1, first subparagraph, point (a), or final energy consumed, with respect to the obligation period referred to in point (b)(i), of that subparagraph, by industrial activities listed in Annex I to Directive 2003/87/EC;
- (c) count towards the amount of required energy savings in paragraph 1, first subparagraph, points (a) and (b)(i), energy savings achieved in the energy transformation, distribution and transmission sectors, including efficient district heating and cooling infrastructure, as a result of implementing the requirements set out in Article 25(4), point (a), of Article 26(7), and Article 27(1), (5) to (9) and (11). Member States shall inform the Commission about their intended policy measures under this point for the period from 1 January 2021 to 31 December 2030 as part of their integrated national energy and climate plans notified pursuant to Article 3 and Articles 7 to 12. The impact of those measures shall be calculated in accordance with Annex V and included in those plans;
- (d) count towards the amount of required energy savings, energy savings resulting from individual actions newly implemented since 31 December 2008 that continue to have an impact in 2020 with respect to the obligation period referred to in paragraph 1, first subparagraph, point (a), and beyond 2020 with respect to the period referred to in point (b)(i), of that subparagraph, and which can be measured and verified;

- (e) count towards the amount of required energy savings, energy savings that stem from policy measures, provided that it can be demonstrated that those measures result in individual actions carried out from 1 January 2018 to 31 December 2020 which deliver savings after 31 December 2020;
 - (f) exclude from the calculation of the amount of required energy savings pursuant to paragraph 1, first subparagraph, points (a) and (b)(i), 30 % of the verifiable amount of energy generated on or in buildings for own use as a result of policy measures promoting new installation of renewable energy technologies;
 - (g) count towards the amount of required energy savings pursuant to paragraph 1, first subparagraph, points (a) and (b)(i), energy savings that exceed the energy savings required for the obligation period from 1 January 2014 to 31 December 2020, provided that those savings result from individual actions carried out under policy measures referred to in Articles 9 and 10, notified by Member States in their national energy efficiency action plans and reported in their progress reports in accordance with Article 26.
9. Member States shall apply and calculate the effect of the options chosen under paragraph 8 for the period referred to in paragraph 1, first subparagraph, points (a) and (b)(i), separately:
- (a) for the calculation of the amount of energy savings required for the obligation period referred to in paragraph 1, first subparagraph, point (a), Member States may make use of the options listed in paragraph 8, points (a) to (d). All the options chosen under paragraph 8 taken together shall amount to no more than 25 % of the amount of energy savings referred to in paragraph 1, first subparagraph, point (a);
 - (b) for the calculation of the amount of energy savings required for the obligation period referred to in paragraph 1, first subparagraph, point (b)(i), Member States may make use of the options listed in paragraph 8, points (b) to (g), provided that the individual actions referred to in paragraph 8, point (d), continue to have a verifiable and measurable impact after 31 December 2020. All the options chosen under paragraph 8 taken together shall not lead to a reduction of more than 35 % of the amount of energy savings calculated in accordance with paragraphs 6 and 7.

Regardless of whether Member States exclude, in whole or in part, energy used in transport from their calculation baseline or make use of any of the options listed in paragraph 8, they shall ensure that the calculated net amount of new savings to be achieved in final energy consumption during the obligation period referred to in paragraph 1, first subparagraph, point (b)(i), from 1 January 2021 to 31 December 2023 is not lower than the amount resulting from applying the annual savings rate referred to in that point.

10. Member States shall describe in the updates of their integrated national energy and climate plans submitted pursuant to Article 14(2) of Regulation (EU) 2018/1999, in their subsequent integrated national energy and climate plans notified pursuant to Article 3 and Articles 7 to 12 of Regulation (EU) 2018/1999 and in accordance with Annex III to Regulation (EU) 2018/1999, and respective progress reports the calculation of the amount of energy savings to be achieved over the period from 1 January 2021 to 31 December 2030 and shall, if relevant, explain how the annual savings rate and the calculation baseline were established, and how and to what extent the options referred to in paragraph 8 of this Article were applied.

11. Member States shall notify the Commission of the amount of the required energy savings referred to in paragraph 1, first subparagraph, point (b), and paragraph 3 of this Article, a description of the policy measures to be implemented to achieve the required total amount of the cumulative end-use energy savings and their calculation methodologies pursuant to Annex V to this Directive, as part of the updates of their integrated national energy and climate plans submitted pursuant to Article 14(2) of Regulation (EU) 2018/1999, and as part of their integrated national energy and climate plans notified pursuant to Article 3 and Articles 7 to 12 of Regulation (EU) 2018/1999. Member States shall use the reporting template provided to the Member States by the Commission.

12. Where on the basis of the assessment of the integrated national energy and climate progress reports pursuant to Article 29 of Regulation (EU) 2018/1999, or of the draft or final update of the latest notified integrated national energy and climate plan submitted pursuant to Article 14 of Regulation (EU) 2018/1999, or of the assessment of the subsequent draft and final integrated national energy and climate plans notified pursuant to Article 3 and Articles 7 to 12 of Regulation (EU) 2018/1999, the Commission concludes that policy measures do not ensure the achievement of the required amount of cumulative end-use energy savings by the end of the obligation period, the Commission may issue recommendations in accordance with Article 34 of Regulation (EU) 2018/1999 to the Member States whose policy measures it deems to be insufficient to ensure the fulfilment of their energy savings obligations.

13. Where a Member State has not achieved the required cumulative end-use energy savings by the end of each obligation period set out in paragraph 1, it shall achieve the outstanding energy savings in addition to the cumulative end-use energy savings required by the end of the following obligation period.

Alternatively, where a Member State has achieved cumulative end-use energy savings above the required level by the end of each obligation period set out in paragraph 1, it shall be entitled to carry the eligible amount of no more than 10 % of such surplus into the following obligation period without the target commitment being increased.

14. As part of their updates of national energy and climate plans submitted pursuant to Article 14(2) of Regulation (EU) 2018/1999, their relevant national energy and climate progress reports submitted pursuant to Article 17 of that Regulation, and their subsequent integrated national energy and climate plans notified pursuant to Article 3 and Articles 7 to 12 of that Regulation, Member States shall demonstrate including, where appropriate, with evidence and calculations:

- (a) that where there is an overlap in the impact of policy measures or individual actions, there is no double counting of energy savings;
- (b) how energy savings achieved pursuant to paragraph 1, first subparagraph, point (b), of this Article, contribute to the achievement of their national contribution pursuant to Article 4;
- (c) that policy measures are established for fulfilling their energy savings obligation, designed in compliance with this Article and that those policy measures are eligible and appropriate to ensure the achievement of the required amount of cumulative end-use energy savings by the end of each obligation period.

Article 9

Energy efficiency obligation schemes

1. Where Member States decide to fulfil their obligations to achieve the amount of savings required under Article 8(1) by way of an energy efficiency obligation scheme, they shall ensure that the obligated parties referred to in paragraph 3 of this Article operating in each Member State's territory achieve, without prejudice to Article 8(8) and (9), their cumulative end-use energy savings requirement as set out in Article 8(1).

Where applicable, Member States may decide that obligated parties fulfil those savings, in whole or in part, as a contribution to the national energy efficiency fund in accordance with Article 30(14).

2. Where Member States decide to fulfil their obligations to achieve the amount of savings required under Article 8(1) by way of an energy efficiency obligation scheme, they may appoint an implementing public authority to administer the scheme.

3. Member States shall designate, on the basis of objective and non-discriminatory criteria, obligated parties among transmission system operators, distribution system operators, energy distributors, retail energy sales companies and transport fuel distributors or transport fuel retailers operating in their territory. The amount of energy savings needed to fulfil the obligation shall be achieved by the obligated parties among final customers, designated by the Member State, independently of the calculation made pursuant to Article 8(1) or, if Member States so decide, through certified savings stemming from other parties as set out in paragraph 11, point (a), of this Article.

4. Where retail energy sales companies are designated as obligated parties under paragraph 3, Member States shall ensure that, in fulfilling their obligation, retail energy sales companies do not create any barriers that impede consumers from switching from one supplier to another.

5. Member States may require obligated parties to achieve a share of their energy savings obligation among people affected by energy poverty, vulnerable customers, people in low-income households and, where applicable, people living in social housing. Member States may also require obligated parties to achieve energy cost reduction targets, provided that they result in end use energy savings and are calculated in accordance with Annex V, and to achieve energy savings by promoting energy efficiency improvement measures, including financial support measures mitigating carbon price effects on SMEs and microenterprises.

6. Member States may require obligated parties to work with social services, regional authorities, local authorities or municipalities to promote energy efficiency improvement measures among people affected by energy poverty, vulnerable customers, people in low-income households and, where applicable, people living in social housing. This includes identifying and addressing the specific needs of particular groups at risk of energy poverty or more susceptible to its effects. To protect people affected by energy poverty, vulnerable customers and, where applicable, people living in social housing, Member States shall encourage obligated parties to carry out actions such as renovation of buildings, including social housing, replacement of appliances, financial support and incentives for energy efficiency improvement measures in accordance with national financing and support schemes, or energy audits. Member States shall ensure the eligibility of measures for individual units located in multi-apartment buildings.

7. When applying paragraphs 5 and 6, Member States shall require obligated parties to report on an annual basis on the energy savings achieved by the obligated parties from actions promoted among people affected by energy poverty, vulnerable customers, people in low-income households and, where applicable, people living in social housing, and shall require aggregated statistical information on their final customers, identifying changes in energy savings when compared to previously submitted information, and regarding technical and financial support provided.

8. Member States shall express the amount of energy savings required of each obligated party in terms of either primary energy consumption or final energy consumption. The method chosen to express the amount of energy savings required shall also be used to calculate the savings claimed by obligated parties. When converting the amount of energy savings, the net calorific values set out in Annex VI of Commission Implementing Regulation (EU) 2018/2066 ⁽⁴¹⁾ and the primary energy factor pursuant to Article 31 shall apply unless the use of other conversion factors can be justified.

9. Member States shall establish measurement, control and verification systems for carrying out documented verification on at least a statistically significant proportion and representative sample of the energy efficiency improvement measures put in place by the obligated parties. The measurement, control and verification shall be carried out independently of the obligated parties. Where an entity is an obligated party under a national energy efficiency obligation scheme under Article 9 and under the EU ETS for buildings and road transport in accordance with Directive 2003/87/EC, the monitoring and verification system shall ensure that the carbon price passed through when releasing fuel for consumption in accordance with Directive 2003/87/EC shall be taken into account in the calculation and reporting of energy savings of the entity's energy saving measures.

⁽⁴¹⁾ Commission Implementing Regulation (EU) 2018/2066 of 19 December 2018 on the monitoring and reporting of greenhouse gas emissions pursuant to Directive 2003/87/EC of the European Parliament and of the Council and amending Commission Regulation (EU) No 601/2012 (OJ L 334, 31.12.2018, p. 1).

10. Member States shall inform the Commission, as part of the integrated national energy and climate progress reports submitted pursuant to Article 17 of Regulation (EU) 2018/1999, on the measurement, control and verification systems put in place, including the methods used, the issues identified and how those issues were addressed.

11. Within the energy efficiency obligation scheme, Member States may authorise obligated parties to carry out the following:

- (a) count towards their obligation certified energy savings achieved by energy service providers or other third parties, including when obligated parties promote measures through other State-approved bodies or through public authorities that may involve formal partnerships and may be in combination with other sources of finance;
- (b) count savings obtained in a given year as if they had instead been obtained in any of the four previous or three following years as long as this is not beyond the end of the obligation periods set out in Article 8(1).

Where Member States so authorise, they shall ensure that the certification of energy savings referred to in point (a) of the first subparagraph follows an approval process that is put in place in the Member States, that is clear, transparent, and open to all market participants, and that aims to minimise the costs of certification.

Member States shall assess and, if appropriate, take measures to minimise the impact of the direct and indirect costs of energy efficiency obligation schemes on the competitiveness of energy-intensive industries exposed to international competition.

12. Member States shall, on an annual basis, publish the energy savings achieved by each obligated party, or each sub-category of obligated party, and in total under the scheme.

Article 10

Alternative policy measures

1. Where Member States decide to fulfil their obligations to achieve the savings required under Article 8(1) by way of alternative policy measures, they shall ensure, without prejudice to Article 8(8) and (9), that the energy savings required under Article 8(1) are achieved among final customers.

2. For all measures other than those relating to taxation, Member States shall put in place measurement, control and verification systems under which documented verification is carried out on at least a statistically significant proportion and representative sample of the energy efficiency improvement measures put in place by the participating or entrusted parties. The measurement, control and verification shall be carried out independently of the participating or entrusted parties.

3. Member States shall inform the Commission, as part of the integrated national energy and climate progress reports submitted pursuant to Article 17 of Regulation (EU) 2018/1999, on the measurement, control and verification systems put in place, including methods used, issues identified and how they were addressed.

4. When reporting a taxation measure, Member States shall demonstrate how the effectiveness of the price signal, such as tax rate and visibility over time, has been ensured in the design of the taxation measure. Where there is a decrease in the tax rate, Member States shall justify how the taxation measures still result in new energy savings.

Article 11

Energy management systems and energy audits

1. Member States shall ensure that enterprises with an average annual consumption higher than 85 TJ of energy over the previous three years, taking all energy carriers together, implement an energy management system. The energy management system shall be certified by an independent body, in accordance with the relevant European or international standards.

Member States shall ensure that the enterprises referred to in the first subparagraph have an energy management system in place at the latest by 11 October 2027.

2. Member States shall ensure that enterprises with an average annual consumption higher than 10 TJ of energy over the previous three years, taking all energy carriers together, which do not implement an energy management system are subject to an energy audit.

Such energy audits shall be either:

- (a) carried out in an independent and cost-effective manner by qualified or accredited experts, in accordance with Article 28; or
- (b) implemented and supervised by independent authorities under national legislation.

Member States shall ensure that the enterprises referred to in the first subparagraph carry out a first energy audit by 11 October 2026 and that subsequent energy audits are carried out at least every four years. Where such enterprises already carry out energy audits in accordance with the first subparagraph, they shall continue to do so at least every four years in accordance with this Directive.

The enterprises concerned shall draw up a concrete and feasible Action Plan on the basis of the recommendations arising from those energy audits. The Action Plan shall identify measures to implement each audit recommendation, where it is technically or economically feasible. The Action Plan shall be submitted to the management of the enterprise.

Member States shall ensure that the Action Plans and the recommendation implementation rate are published in the enterprise's annual report, and that they are made publicly available, subject to Union and national law protecting trade and business secrets and confidentiality.

3. Where, in any given year, an enterprise as referred to in paragraph 1 has an annual consumption of more than 85 TJ and where an enterprise as referred to in paragraph 2 has an annual consumption of more than 10 TJ, Member States shall ensure that that information is made available to the national authorities responsible for implementation of this Article. For that purpose, Member States may promote the use of a new or an existing platform to facilitate the collection of the required data at national level.

4. Member States may encourage the enterprises referred to in paragraphs 1 and 2 to provide information in their annual report about their annual energy consumption in kWh, their annual volume of water consumption in cubic metres and a comparison of their energy and water consumption with previous years.

5. Member States shall promote the availability to all final customers of high quality energy audits which are cost-effective and are:

- (a) carried out in an independent manner by qualified or accredited experts in accordance with qualification criteria; or
- (b) implemented and supervised by independent authorities under national legislation.

The energy audits referred to in the first subparagraph may be carried out by in-house experts or energy auditors, provided that the Member State concerned has put in place a scheme to ensure their quality, including, if appropriate, an annual random selection of at least a statistically significant percentage of all the energy audits carried out by such in-house experts or energy auditors.

For the purpose of ensuring the high quality of the energy audits and energy management systems, Member States shall establish transparent and non-discriminatory minimum criteria for energy audits in accordance with Annex VI and taking into consideration relevant European or international standards. Member States shall designate a competent authority or body to ensure that the timelines for conducting energy audits set out in paragraph 2 of this Article are complied with and the minimum criteria set out in Annex VI are correctly applied.

Energy audits shall not include clauses preventing the findings of the audit from being transferred to any qualified or accredited energy service provider, provided that the customer does not object.

6. Member States shall develop programmes with the aim of encouraging and providing technical support to SMEs that are not subject to paragraph 1 or 2 to undergo energy audits and to subsequently implement the recommendations arising from those audits.

On the basis of transparent and non-discriminatory criteria and without prejudice to Union State aid law, Member States may set up mechanisms, such as energy audit centres for SMEs and microenterprises, provided that such mechanisms do not compete with private auditors, to provide energy audits. They may also provide other support schemes for SMEs, including where such SMEs have concluded voluntary agreements, to cover the costs of energy audits and of the implementation of highly cost-effective recommendations arising from the energy audits, if the measures proposed in those recommendations are implemented.

7. Member States shall ensure that the programmes referred to in paragraph 6 include support to SMEs in quantifying the multiple benefits of energy efficiency measures within their operation, in the development of energy efficiency roadmaps and in the development of energy efficiency networks for SMEs, facilitated by independent experts.

Member States shall bring to the attention of SMEs, including through their respective representative intermediary organisations, concrete examples of how energy management systems could help their businesses. The Commission shall assist Member States by supporting the exchange of best practices in this domain.

8. Member States shall develop programmes to encourage enterprises that are not SMEs and that are not subject to paragraph 1 or 2 to undergo energy audits and to subsequently implement the recommendations arising from those audits.

9. Energy audits shall be considered to comply with paragraph 2 where they are:

- (a) carried out in an independent manner, on the basis of the minimum criteria set out in Annex VI;
- (b) implemented under voluntary agreements concluded between organisations of stakeholders and a body appointed and supervised by the Member State concerned, by another body to which the competent authorities have delegated the responsibility concerned or by the Commission.

Access of market participants offering energy services shall be based on transparent and non-discriminatory criteria.

10. Enterprises that implement an energy performance contract shall be exempt from the requirements laid down in paragraphs 1 and 2 of this Article, provided that the energy performance contract covers the necessary elements of the energy management system and that the contract complies with the requirements set out in Annex XV.

11. Enterprises that implement an environmental management system, certified by an independent body in accordance with the relevant European or international standards, shall be exempt from the requirements laid down in paragraphs 1 and 2 of this Article, provided that the environmental management system concerned includes an energy audit on the basis of the minimum criteria set out in Annex VI.

12. Energy audits may stand alone or be part of a broader environmental audit. Member States may require an assessment of the technical and economic feasibility of connection to an existing or planned district heating or cooling network to be part of the energy audit.

Without prejudice to Union State aid law, Member States may implement incentives and support schemes for the implementation of recommendations arising from energy audits and similar measures.

Article 12

Data centres

1. By 15 May 2024 and every year thereafter, Member States shall require owners and operators of data centres in their territory with a power demand of the installed information technology (IT) of at least 500kW, to make the information set out in Annex VII publicly available, except for information subject to Union and national law protecting trade and business secrets and confidentiality.
2. Paragraph 1 shall not apply to data centres used for, or providing their services exclusively with the final aim of, defence and civil protection.
3. The Commission shall establish a European database on data centres that includes information communicated by the obligated data centres in accordance with paragraph 1. The European database shall be publicly available on an aggregated level.
4. Member States shall encourage owners and operators of data centres in their territory with a power demand of the installed IT equal to or greater than 1 MW to take into account the best practices referred to in the most recent version of the European Code of Conduct on Data Centre Energy Efficiency.
5. By 15 May 2025, the Commission shall assess the available data on the energy efficiency of data centres submitted to it pursuant to paragraphs 1 and 3 and shall submit a report to the European Parliament and to the Council, accompanied, where appropriate, by legislative proposals containing further measures to improve energy efficiency, including establishing minimum performance standards and an assessment on the feasibility of transition towards a net-zero emission data centres sector, in close consultation with the relevant stakeholders. Such proposals may establish a timeframe within which existing data centres are to be required to meet minimum performance.

Article 13

Metering for natural gas

1. Member States shall ensure that, in so far as technically possible, financially reasonable, and proportionate to the potential energy savings, natural gas final customers are provided with competitively priced individual meters that accurately reflect the final customer's actual energy consumption and that provide information on actual time of use.

Such a competitively priced individual meter shall always be provided when:

- (a) an existing meter is replaced, unless this is technically impossible or not cost-effective in relation to the estimated potential savings in the long term;
- (b) a new connection is made in a new building or a building undergoes major renovations within the meaning of Directive 2010/31/EU.

2. Where, and to the extent that, Member States implement smart metering systems and roll out smart meters for natural gas in accordance with Directive 2009/73/EC:

- (a) they shall ensure that the metering systems provide to final customers information on actual time of use and that the objectives of energy efficiency and benefits for final customers are fully taken into account when establishing the minimum functionalities of the meters and the obligations imposed on market participants;

- (b) they shall ensure the security of the smart meters and data communication, and the privacy of final customers, in compliance with relevant Union data protection and privacy law;
- (c) they shall require that appropriate advice and information be given to customers at the time of installation of smart meters, in particular about their full potential with regard to meter reading management and the monitoring of energy consumption.

Article 14

Metering for heating, cooling and domestic hot water

1. Member States shall ensure that, for district heating, district cooling and domestic hot water, final customers are provided with competitively priced meters that accurately reflect their actual energy consumption.
2. Where heating, cooling or domestic hot water is supplied to a building from a central source that services multiple buildings or from a district heating or district cooling system, a meter shall be installed at the heat exchanger or point of delivery.

Article 15

Sub-metering and cost allocation for heating, cooling and domestic hot water

1. In multi-apartment and multi-purpose buildings with a central heating or central cooling source or supplied from a district heating or district cooling system, individual meters shall be installed to measure the consumption of heating, cooling or domestic hot water for each building unit, where technically feasible and cost effective in terms of being proportionate in relation to the potential energy savings.

Where the use of individual meters is not technically feasible or where it is not cost-efficient to measure heat consumption in each building unit, individual heat cost allocators shall be used to measure heat consumption at each radiator unless it is shown by the Member State in question that the installation of such heat cost allocators would not be cost-efficient. In those cases, alternative cost-efficient methods of heat consumption measurement may be considered. The general criteria, methodologies and procedures to determine technical non-feasibility and non-cost effectiveness shall be clearly set out and published by each Member State.

2. In new multi-apartment buildings and in residential parts of new multi-purpose buildings that are equipped with a central heating source for domestic hot water or are supplied from district heating systems, individual meters shall, notwithstanding paragraph 1, first subparagraph, be provided for domestic hot water.

3. Where multi-apartment or multi-purpose buildings are supplied from district heating or district cooling, or where own common heating or cooling systems for such buildings are prevalent, Member States shall ensure that they have in place transparent, publicly available national rules on the allocation of the cost of heating, cooling and domestic hot water consumption in such buildings to ensure transparency and accuracy of accounting for individual consumption. Where appropriate, such rules shall include guidelines on the manner in which to allocate cost for energy that is used for:

- (a) domestic hot water;
- (b) heat radiated from the building installation and for the purpose of heating the common areas, where staircases and corridors are equipped with radiators;
- (c) heating or cooling apartments.

*Article 16***Remote reading requirement**

1. For the purposes of Articles 14 and 15, newly installed meters and heat cost allocators shall be remotely readable devices. The conditions of technical feasibility and cost effectiveness set out in Article 15(1) shall apply.
2. Meters and heat cost allocators which are not remotely readable but which have already been installed shall be rendered remotely readable or replaced with remotely readable devices by 1 January 2027, save where the Member State in question shows that this is not cost-efficient.

*Article 17***Billing information for natural gas**

1. Where final customers do not have smart meters for natural gas as referred to in Directive 2009/73/EC, Member States shall ensure that billing information for natural gas is reliable, accurate and based on actual consumption, in accordance with Annex VIII, point 1.1, where that is technically possible and economically justified.

This obligation may be fulfilled by a system of regular self-reading by the final customers whereby they communicate readings from their meter to the energy supplier. Only when the final customer has not provided a meter reading for a given billing interval shall billing be based on estimated consumption or a flat rate.

2. Meters installed in accordance with Directive 2009/73/EC shall enable the provision of accurate billing information based on actual consumption. Member States shall ensure that final customers have the possibility of easy access to complementary information on historical consumption allowing detailed self-checks.

Complementary information on historical consumption shall include:

- (a) cumulative data for at least the three previous years or the period since the start of the supply contract if this is shorter;
- (b) detailed data according to the time of use for any day, week, month and year.

The data referred to in point (a) of the second subparagraph shall correspond to the intervals for which frequent billing information has been produced.

The data referred to in point (b) of the second subparagraph shall be made available to the final customer via the internet or the meter interface for the period of at least the previous 24 months or the period since the start of the supply contract if this is shorter.

3. Independently of whether smart meters have been installed, Member States:
 - (a) shall require that, to the extent that information on the energy billing and historical consumption of final customers is available, it be made available, at the request of the final customer, to an energy service provider designated by the final customer;
 - (b) shall ensure that final customers are offered the option of electronic billing information and bills and that they receive, on request, a clear and understandable explanation of how their bill was derived, especially where bills are not based on actual consumption;
 - (c) shall ensure that appropriate information is made available with the bill to provide final customers with a comprehensive account of current energy costs, in accordance with Annex VIII;

- (d) may lay down that, at the request of the final customer, the information contained in those bills shall not be considered to constitute a request for payment. In such cases, Member States shall ensure that suppliers of energy sources offer flexible arrangements for actual payments;
- (e) shall require that information and estimates for energy costs are provided to consumers on demand in a timely manner and in an easily understandable format enabling consumers to compare deals on a like-for-like basis.

Article 18

Billing and consumption information for heating, cooling and domestic hot water

1. Where meters or heat cost allocators are installed, Member States shall ensure that billing and consumption information is reliable, accurate and based on actual consumption or heat cost allocator readings, in accordance with Annex IX, points 1 and 2 for all final users.

That obligation may, where a Member State so provides, save in the case of sub-metered consumption based on heat cost allocators under Article 15, be fulfilled by a system of regular self-reading by the final customer or final user whereby they communicate readings from their meter. Only where the final customer or final user has not provided a meter reading for a given billing interval shall billing be based on estimated consumption or a flat rate.

2. Member States shall:

- (a) require that, if information on the energy billing and historical consumption or heat cost allocator readings of final users is available, it be made available upon request from the final user, to an energy service provider designated by the final user;
- (b) ensure that final customers are offered the option of electronic billing information and bills;
- (c) ensure that clear and comprehensible information is provided with the bill to all final users in accordance with Annex IX, point 3;
- (d) promote cybersecurity and ensure the privacy and data protection of final users in accordance with applicable Union law.

Member States may provide that, at the request of the final customer, the provision of billing information shall not be considered to constitute a request for payment. In such cases, Member States shall ensure that flexible arrangements for actual payment are offered.

3. Member States shall decide who is to be responsible for providing the information referred to in paragraphs 1 and 2 to final users without a direct or individual contract with an energy supplier.

Article 19

Cost of access to metering and billing information for natural gas

Member States shall ensure that final customers receive all their bills and billing information for energy consumption free of charge and that final customers have access to their consumption data in an appropriate manner and free of charge.

Article 20

Cost of access to metering and billing and consumption information for heating, cooling and domestic hot water

1. Member States shall ensure that final users receive all their bills and billing information for energy consumption free of charge and that final users have access to their consumption data in an appropriate manner and free of charge.

2. Notwithstanding paragraph 1 of this Article, the distribution of costs of billing information for the individual consumption of heating, cooling and domestic hot water in multi-apartment and multi-purpose buildings pursuant to Article 15 shall be carried out on a non-profit basis. Costs resulting from the assignment of that task to a third party, such as a service provider or the local energy supplier, covering the measuring, allocation and accounting for actual individual consumption in such buildings, may be passed onto the final users to the extent that such costs are reasonable.

3. In order to ensure reasonable costs for sub-metering services as referred to in paragraph 2, Member States may stimulate competition in that service sector by taking appropriate measures such as recommending or otherwise promoting the use of tendering or the use of interoperable devices and systems facilitating switching between service providers.

CHAPTER IV

CONSUMER INFORMATION AND EMPOWERMENT

Article 21

Basic contractual rights for heating, cooling and domestic hot water

1. Without prejudice to Union rules on consumer protection, in particular Directive 2011/83/EU of the European Parliament and of the Council ⁽⁴²⁾ and Council Directive 93/13/EEC ⁽⁴³⁾, Member States shall ensure that final customers and, where explicitly referred to, final users, are granted the rights provided for in paragraphs 2 to 9 of this Article.

2. Final customers shall have the right to a contract with their supplier that specifies:

- (a) the identity, address and contact details of the supplier;
- (b) the services provided and the service quality levels included;
- (c) the types of maintenance service included in the contract without additional charges;
- (d) the means by which up-to-date information on all applicable tariffs, maintenance charges and bundled products or services may be obtained;
- (e) the duration of the contract, the conditions for renewal and termination of the contract and services, including products or services that are bundled with those services, and whether terminating the contract without charge is permitted;
- (f) any compensation and the refund arrangements which apply if contracted service quality levels are not met, including inaccurate or delayed billing;
- (g) the method of initiating an out-of-court dispute-settlement procedure in accordance with Article 22;
- (h) information relating to consumer rights, including information on complaint handling and all of the information referred to in this paragraph, which is clearly communicated in the bill or on the enterprise's website and includes the contact details or link to the website of the single points of contact referred to in Article 22(3), point (e);

⁽⁴²⁾ Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (OJ L 304, 22.11.2011, p. 64).

⁽⁴³⁾ Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29).

- (i) the contact details enabling the customer to identify relevant one-stop shops as referred to in Article 22(3), point (a).

Suppliers' conditions shall be fair and shall be provided to final customers in advance. The information referred to in this paragraph shall be provided before the conclusion or confirmation of the contract. Where contracts are concluded through intermediaries, that information shall also be provided before the conclusion of the contract.

Final customers and final users shall be provided with a summary of the key contractual conditions, including prices and tariffs, in a comprehensible manner and in concise and simple language.

Final customers shall be provided with a copy of the contract and clear information, in a transparent manner, on applicable prices and tariffs and on standard terms and conditions in respect of access to and use of heating, cooling and domestic hot water services.

Member States shall decide who is to be responsible for providing the information referred to in this paragraph to final users without a direct or individual contract with a supplier, upon request, in an appropriate manner and free of charge.

3. Final customers shall be given adequate notice of any intention to modify contractual conditions. Suppliers shall notify their final customers, in a transparent and comprehensible manner, directly of any adjustment in the supply price and of the reasons and preconditions for the adjustment and its scope, at an appropriate time no later than two weeks, or no later than one month in the case of household customers, before the adjustment comes into effect. Final customers shall inform final users of the new conditions without delay.

4. Suppliers shall offer final customers a wide choice of payment methods. Such payment methods shall not unduly discriminate between customers. Any difference in charges related to payment methods or prepayment systems shall be objective, non-discriminatory and proportionate and shall not exceed the direct costs borne by the payee for the use of a specific payment method or a prepayment system, in accordance with Article 62 of Directive (EU) 2015/2366 of the European Parliament and of the Council ⁽⁴⁴⁾.

5. Pursuant to paragraph 4, household customers who have access to prepayment systems shall not be placed at a disadvantage by the prepayment systems.

6. Final customers and, where applicable, final users shall be offered fair and transparent general terms and conditions, which shall be provided in plain and unambiguous language and shall not include non-contractual barriers to the exercise of customers' rights, such as excessive contractual documentation. Final users shall be provided access to those general terms and conditions upon request. Final customers and final users shall be protected against unfair or misleading selling methods. Final customers with disabilities shall be provided all relevant information on their contract with their supplier in accessible formats.

7. Final customers and final users shall have the right to a good standard of service and complaint-handling by their suppliers. Suppliers shall handle complaints in a simple, fair and prompt manner.

8. Competent authorities shall ensure that the consumer protection measures laid down in this Directive are enforced. The competent authorities shall act independently from any market interests.

9. In the case of planned disconnection, the final customers concerned shall be provided with adequate information on alternative measures sufficiently in advance, no later than one month before the planned disconnection and at no extra cost.

⁽⁴⁴⁾ Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).

*Article 22***Information and awareness raising**

1. Member States, in cooperation with regional and local authorities, where applicable, shall ensure that information on available energy efficiency improvement measures, individual actions and financial and legal frameworks is transparent, accessible and widely disseminated to all relevant market actors, such as final customers, final users, consumer organisations, civil society representatives, renewable energy communities, citizen energy communities, local and regional authorities, energy agencies, social service providers, builders, architects, engineers, environmental and energy auditors, and installers of building elements as defined in Article 2, point (9), of Directive 2010/31/EU.

2. Member States shall take appropriate measures to promote and facilitate an efficient use of energy by final customers and final users. Those measures shall be part of a national strategy, such as the integrated national energy and climate plans provided for in Regulation (EU) 2018/1999, or the long-term renovation strategy established pursuant to Article 2a of Directive 2010/31/EU.

For the purposes of this Article, those measures shall include a range of instruments and policies to promote behavioural change such as:

- (a) fiscal incentives;
- (b) access to finance, vouchers, grants or subsidies;
- (c) publicly supported energy consumption assessments and targeted advisory services and support for household consumers, in particular people affected by energy poverty, vulnerable customers and, where applicable, people living in social housing;
- (d) targeted advisory services for SMEs and microenterprises;
- (e) information provision in accessible form to people with disabilities;
- (f) exemplary projects;
- (g) workplace activities;
- (h) training activities;
- (i) digital tools;
- (j) engagement strategies.

3. For the purposes of this Article, the measures referred to in paragraph 2 shall include the creation of a supportive framework for market actors such as those referred to in paragraph 1, in particular for:

- (a) the creation of one-stop shops or similar mechanisms for the provision of technical, administrative and financial advice and assistance on energy efficiency, such as energy checks for households, energy renovations of buildings, information on the replacement of old and inefficient heating systems with modern and more efficient appliances and the take-up of renewable energy and energy storage for buildings to final customers and final users, especially household and small non-household ones, including SMEs and microenterprises;
- (b) cooperation with private actors that provide services such as energy audits and energy consumption assessments, financing solutions and execution of energy renovations;
- (c) the communication of cost-effective and easy-to-achieve changes in energy use;
- (d) the dissemination of information on energy efficiency measures and financing instruments;

- (e) the provision of single points of contact, to provide final customers and final users with all necessary information concerning their rights, the applicable law and the dispute-settlement mechanisms available to them in the event of a dispute. Such single points of contact may be part of general consumer information points.

4. For the purpose of this Article, Member States shall in cooperation with competent authorities, and, where appropriate, private stakeholders establish dedicated one-stop shops or similar mechanisms for the provision of technical, administrative and financial advice for energy efficiency. Those facilities shall:

- (a) advise with streamlined information on technical and financial possibilities and solutions to households, SMEs, microenterprises, public bodies;
- (b) provide holistic support to all households, with a particular focus on households affected by energy poverty and on worst performing buildings, as well as to accredited companies and installers providing retrofit services, adapted to different housing typologies and geographical scope, and provide support covering the different stages of the retrofit project, including to facilitate the implementation of a minimum energy performance standard where such standard is provided for in a Union legislative act;
- (c) advise on energy consumption behaviour.

5. Dedicated one-stop shop facilities as referred to in paragraph 4 shall, where appropriate:

- (a) provide information about qualified energy efficiency professionals;
- (b) collect typology-aggregated data from energy efficiency projects, share experiences and make them publicly available;
- (c) connect potential projects with market players, in particular smaller-scale, local projects.

For the purposes of the first subparagraph, point (b), the Commission shall assist Member States in order to facilitate the sharing of, and enhance cross-border cooperation with regard to, best practices.

6. The one-stop shops referred to in paragraph 4 shall offer dedicated services for people affected by energy poverty, vulnerable customers and people in low-income households.

The Commission shall provide Member States with guidelines to develop those one-stop shops with the aim of creating a harmonised approach throughout the Union. The guidelines shall encourage cooperation among public bodies, energy agencies and community-led initiatives.

7. Member States shall establish appropriate conditions for market actors to provide adequate and targeted information and advice on energy efficiency to final customers, including people affected by energy poverty, vulnerable customers and, where applicable, people living in social housing, SMEs and microenterprises.

8. Member States shall ensure that final customers, final users, people affected by energy poverty, vulnerable customers and, where applicable, people living in social housing have access to simple, fair, transparent, independent, effective and efficient out-of-court mechanisms for the settlement of disputes concerning rights and obligations provided for in this Directive, through an independent mechanism such as an energy ombudsperson or a consumer body, or through a regulatory authority. Where the final customer is a consumer as defined in Article 4(1), point (a), of Directive 2013/11/EU of the European Parliament and of the Council ⁽⁴⁵⁾, such out-of-court dispute settlement mechanisms shall comply with the requirements set out therein. Out-of-court dispute settlement mechanisms already existing in Member States may be used for that purpose, provided they are equally effective.

⁽⁴⁵⁾ Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR) (OJ L 165, 18.6.2013, p. 63).

Where necessary, Member States shall ensure that alternative dispute resolution entities cooperate to provide simple, fair, transparent, independent, effective and efficient out-of-court dispute settlement mechanisms for any dispute that arises from products or services that are tied to, or bundled with, any product or service falling under the scope of this Directive.

The participation of enterprises in out-of-court dispute settlement mechanisms for household customers shall be mandatory unless the Member State demonstrates to the Commission that other mechanisms are equally effective.

9. Without prejudice to the basic principles of their laws on property and tenancy, Member States shall take the necessary measures to remove regulatory and non-regulatory barriers to energy efficiency as regards split incentives between owners and tenants, or among owners of a building or building unit, with a view to ensuring that those parties are not deterred from making efficiency-improving investments that they would otherwise have made by the fact that they will not individually obtain the full benefits or by the absence of rules for dividing the costs and benefits between them.

Measures to remove such barriers may include providing incentives, repealing or amending legal or regulatory provisions, adopting guidelines and interpretative communications, simplifying administrative procedures, including national rules and measures regulating decision-making processes in multi-owner properties, and the possibility to turn to third-party financing solutions. The measures may be combined with the provision of education, training and specific information and technical assistance on energy efficiency to market actors such as those referred to in paragraph 1.

Member States shall take appropriate measures to support a multilateral dialogue among relevant partners, such as local and regional authorities, the social partners, owners' and tenants' organisations, consumer organisations, energy distributors or retail energy sales companies, ESCOs, renewable energy communities, citizen energy communities, public authorities and agencies, with the aim of setting out proposals on jointly accepted measures, incentives and guidelines pertinent to split incentives between owners and tenants or among owners of a building or building unit.

Each Member State shall report such barriers and the measures taken in its long-term renovation strategy established pursuant to Article 2a of Directive 2010/31/EU and to Regulation (EU) 2018/1999.

10. The Commission shall encourage the exchange and wide dissemination of information on good energy efficiency practices and methodologies and provide technical assistance to mitigate split incentives in Member States.

Article 23

Partnerships for energy efficiency

1. By 11 October 2024, the Commission shall assess whether energy efficiency is covered by existing partnerships. If the assessment shows that energy efficiency is not sufficiently covered by existing partnerships, the Commission shall establish sector-specific energy efficiency partnerships at Union level, with sub-partnerships per missing sector, by bringing together key stakeholders, including the social partners, in sectors such as ICT, transport, finance and building, in an inclusive and representative manner.

If a partnership is established, the Commission shall appoint, where appropriate, a chair for each Union sector-specific energy efficiency partnership.

2. The partnerships referred to in paragraph 1 shall aim to facilitate climate and energy transition dialogues between the relevant actors and encourage sectors to draw up energy efficiency roadmaps in order to map available measures and technological options to achieve energy savings, prepare for renewable energy and decarbonise the sectors.

Such roadmaps would make a valuable contribution in assisting sectors in planning the necessary investments needed to reach the objectives of this Directive and of Regulation (EU) 2021/1119 as well as facilitate cross-border cooperation between actors to strengthen the internal market.

Article 24

Empowering and protecting vulnerable customers and alleviating energy poverty

1. Without prejudice to their national economic and social policies, and to their obligations under Union law, Member States shall take appropriate measures to empower and protect people affected by energy poverty, vulnerable customers, people in low-income households and, where applicable, people living in social housing.

In defining the concept of vulnerable customers pursuant to Article 3(3) of Directive 2009/73/EC and Article 28(1) of Directive (EU) 2019/944, Member States shall take into account final users.

2. Without prejudice to their national economic and social policies, and to their obligations under Union law, Member States shall implement energy efficiency improvement measures and related consumer protection or information measures, in particular those set out in Article 8(3) and Article 22 of this Directive, as a priority among people affected by energy poverty, vulnerable customers, people in low-income households and, where applicable, people living in social housing to alleviate energy poverty. Monitoring and reporting of those measures shall be undertaken in the framework of the existing reporting requirements set out in Article 24 of Regulation (EU) 2018/1999.

3. To support people affected by energy poverty, vulnerable customers, people in low-income households and, where applicable, people living in social housing, Member States shall, where applicable:

- (a) implement energy efficiency improvement measures to mitigate distributional effects from other policies and measures, such as taxation measures implemented in accordance with Article 10 of this Directive, or the application of emissions trading in the buildings and transport sector in accordance with Directive 2003/87/EC;
- (b) make the best possible use of public funding available at Union and national level, including, where applicable, the financial contribution that Member States receive from the Social Climate Fund pursuant to Articles 9 and 14 of Regulation (EU) 2023/955, and revenues from allowance auctions from emissions trading pursuant to the EU ETS in accordance with Directive 2003/87/EC, for investments into energy efficiency improvement measures as priority actions;
- (c) carry out early, forward-looking investments in energy efficiency improvement measures before distributional impacts from other policies and measures show their effect;
- (d) foster technical assistance and the roll-out of enabling funding and financial tools, such as on-bill schemes, local loan-loss reserve, guarantee funds, funds targeting deep renovations and renovations with minimum energy gains;
- (e) foster technical assistance for social actors to promote vulnerable customer's active engagement in the energy market, and positive changes in their energy consumption behaviour;
- (f) ensure access to finance, grants or subsidies bound to minimum energy gains and thus facilitate access to affordable bank loans or dedicated credit lines.

4. Member States shall establish a network of experts from various sectors such as the health, building and social sectors, or entrust an existing network, to develop strategies to support local and national decision makers in implementing energy efficiency improvement measures, technical assistance and financial tools aiming to alleviate energy poverty. Member States shall strive to ensure that the composition of the network of experts ensures gender balance and reflects the perspectives of all people.

Member States may entrust the network of experts to offer advice on:

- (a) national definitions, indicators and criteria of energy poverty, energy poor and vulnerable customers, including final users;
- (b) the development or improvement of relevant indicators and data sets, pertinent to the issue of energy poverty, that should be used and reported upon;
- (c) methods and measures to ensure affordability of living costs, the promotion of housing cost neutrality, or ways to ensure that public funding invested in energy efficiency improvement measures benefit both owners and tenants of buildings and building units, in particular regarding people affected by energy poverty, vulnerable customers, people in low-income households, and, where applicable, people living in social housing;
- (d) measures to prevent or remedy situations in which particular groups are more affected or more at risk of being affected by energy poverty or are more susceptible to the adverse impacts of energy poverty such as on the basis of their income, gender, health condition or membership of a minority group, and demographics.

CHAPTER V

EFFICIENCY IN ENERGY SUPPLY

Article 25

Heating and cooling assessment and planning

1. As part of its integrated national energy and climate plan and its updates pursuant to Regulation (EU) 2018/1999, each Member State shall submit to the Commission a comprehensive heating and cooling assessment. That comprehensive assessment shall contain the information set out in Annex X to this Directive and shall be accompanied by the assessment carried out pursuant to Article 15(7) of Directive (EU) 2018/2001.

2. Member States shall ensure that stakeholders affected by the comprehensive assessment referred to in paragraph 1 are given the opportunity to participate in the preparation of heating and cooling plans, the comprehensive assessment and the policies and measures, whilst ensuring that the competent authorities do not disclose or publish trade secrets or business secrets that have been identified as such.

3. For the purpose of the comprehensive assessment referred to in paragraph 1, Member States shall carry out a cost-benefit analysis covering their territory on the basis of climate conditions, economic feasibility and technical suitability. The cost-benefit analysis shall be capable of facilitating the identification of the most resource- and cost-efficient solutions to meeting heating and cooling needs, taking into account the energy efficiency first principle. That cost-benefit analysis may be part of an environmental assessment under Directive 2001/42/EC of the European Parliament and of the Council ⁽⁴⁶⁾.

Member States shall designate the competent authorities responsible for carrying out the cost-benefit analyses, provide the detailed methodologies and assumptions in accordance with Annex XI and establish and make public the procedures for the economic analysis.

4. Where the comprehensive assessment referred to in paragraph 1 of this Article and the analysis referred to in paragraph 3 of this Article identify a potential for the application of high-efficiency cogeneration and/or efficient district heating and cooling from waste heat, whose benefits exceed the costs, Member States shall take adequate measures for efficient district heating and cooling infrastructure to be developed, to encourage the development of installations for the utilisation of waste heat, including in the industrial sector, and/or to accommodate the development of high-efficiency cogeneration and the use of heating and cooling from waste heat and renewable energy sources in accordance with paragraph 1 of this Article and with Article 26(7) and (9).

⁽⁴⁶⁾ Directive 2001/42/EC of the European Parliament and of the Council of 27 June 2001 on the assessment of the effects of certain plans and programmes on the environment (OJ L 197, 21.7.2001, p. 30).

Where the comprehensive assessment referred to in paragraph 1 of this Article and the analysis referred to in paragraph 3 of this Article do not identify a potential whose benefits exceed the costs, including the administrative costs of carrying out the cost-benefit analysis referred to in Article 26(7), the Member State concerned, together with the local and regional authorities, where applicable, may exempt installations from the requirements laid down in paragraphs 1 and 3 of this Article.

5. Member States shall adopt policies and measures which ensure that the potential identified in the comprehensive assessments carried out pursuant to paragraph 1 of this Article is realised. Those policies and measures shall include at least the elements set out in Annex X. Each Member State shall notify those policies and measures as part of the update of its integrated national energy and climate plans submitted pursuant to Article 14(2) of Regulation (EU) 2018/1999, its subsequent integrated national energy and climate plan notified pursuant to Article 3 and Articles 7 to 12 of that Regulation, and the relevant national energy and climate progress reports submitted pursuant to that Regulation.

6. Member States shall ensure that regional and local authorities prepare local heating and cooling plans at least in municipalities having a total population higher than 45 000. Those plans should at least:

- (a) be based on the information and data provided in the comprehensive assessments carried out pursuant to paragraph 1 and provide an estimate and mapping of the potential for increasing energy efficiency, including via low-temperature district heating readiness, high efficiency cogeneration, waste heat recovery, and renewable energy in heating and cooling in that particular area;
- (b) be compliant with the energy efficiency first principle;
- (c) include a strategy for the use of the identified potential pursuant to point (a);
- (d) be prepared with the involvement of all relevant regional or local stakeholders and ensure the participation of general public, including operators of local energy infrastructure;
- (e) take into account the relevant existing energy infrastructure;
- (f) consider the common needs of local communities and multiple local or regional administrative units or regions;
- (g) assess the role of energy communities and other consumer-led initiatives that can actively contribute to the implementation of local heating and cooling projects;
- (h) include an analysis of heating and cooling appliances and systems in local building stocks, taking into account the area-specific potentials for energy efficiency measures and addressing the worst performing buildings and the needs of vulnerable households;
- (i) assess how to finance the implementation of policies and measures and identify financial mechanisms allowing consumers to shift to renewable heating and cooling;
- (j) include a trajectory to achieve the goals of the plans in line with climate neutrality and the monitoring of the progress of the implementation of policies and measures identified;
- (k) aim to replace old and inefficient heating and cooling appliances in public bodies with highly efficient alternatives with the aim of phasing out fossil fuels;
- (l) assess potential synergies with the plans of neighbouring regional or local authorities to encourage joint investments and cost efficiency.

Member States shall ensure that all relevant parties, including public and relevant private stakeholders, are given the opportunity to participate in the preparation of heating and cooling plans, the comprehensive assessment referred to in paragraph 1 and the policies and measures referred to in paragraph 5.

For that purpose, Member States shall develop recommendations supporting the regional and local authorities to implement policies and measures in energy efficient and renewable energy based heating and cooling at regional and local level utilising the potential identified. Member States shall support regional and local authorities to the utmost extent possible by any means, including financial support and technical support schemes. Member States shall ensure that heating and cooling plans are aligned with other local climate, energy and environment planning requirements in order to avoid administrative burden for local and regional authorities and to encourage the effective implementation of the plans.

Local heating and cooling plans may be carried out jointly by a group of several neighbouring local authorities provided that the geographical and administrative context, as well as the heating and cooling infrastructure, is appropriate.

Local heating and cooling plans shall be assessed by a competent authority and, if necessary, followed by appropriate implementation measures.

Article 26

Heating and cooling supply

1. In order to ensure more efficient consumption of primary energy and to increase the share of renewable energy in heating and cooling supply going into the network, an efficient district heating and cooling system shall meet the following criteria:

- (a) until 31 December 2027, a system using at least 50 % renewable energy, 50 % waste heat, 75 % cogenerated heat or 50 % of a combination of such energy and heat;
- (b) from 1 January 2028, a system using at least 50 % renewable energy, 50 % waste heat, 50 % renewable energy and waste heat, 80 % of high-efficiency cogenerated heat or at least a combination of such thermal energy going into the network where the share of renewable energy is at least 5 % and the total share of renewable energy, waste heat or high-efficiency cogenerated heat is at least 50 %;
- (c) from 1 January 2035, a system using at least 50 % renewable energy, 50 % waste heat or 50 % renewable energy and waste heat, or a system where the total share of renewable energy, waste heat or high-efficiency cogenerated heat is at least 80 % and in addition the total share of renewable energy or waste heat is at least 35 %;
- (d) from 1 January 2040, a system using at least 75 % renewable energy, 75 % waste heat or 75 % renewable energy and waste heat, or a system using at least 95 % renewable energy, waste heat and high-efficiency cogenerated heat and in addition the total share of renewable energy or waste heat is at least 35 %;
- (e) from 1 January 2045, a system using at least 75 % renewable energy, 75 % waste heat or 75 % renewable energy and waste heat;
- (f) from 1 January 2050, a system using only renewable energy, only waste heat, or only a combination of renewable energy and waste heat.

2. Member States may also choose, as an alternative to the criteria set out in paragraph 1 of this Article, sustainability performance criteria based on the amount of GHG emissions from the district heating and cooling system per unit of heat or cold delivered to the customers, taking into consideration measures implemented to fulfil the obligation pursuant to Article 24(4) of Directive (EU) 2018/2001. When choosing those criteria, an efficient district heating and cooling system shall have the following maximum amount of GHG emissions per unit of heat or cold delivered to the customers:

- (a) until 31 December 2025: 200 grams/kWh;
- (b) from 1 January 2026: 150 grams/kWh;
- (c) from 1 January 2035: 100 grams/kWh;
- (d) from 1 January 2045: 50 grams/kWh;
- (e) from 1 January 2050: 0 grams/kWh.

3. Member States may choose to apply the criteria of GHG emissions per unit of heat or cold for any given period referred to in paragraph 2, points (a) to (e), of this Article. If they choose to do so, they shall notify the Commission by 11 January 2024 for the period referred to in paragraph 2, point (a), of this Article and at least six months before the beginning of the relevant periods referred to in paragraph 2, points (b) to (e), of this Article. Such a notification shall include the measures implemented to fulfil the obligation pursuant to Article 24(4) of Directive (EU) 2018/2001 if they have not already been notified in the latest update of their national energy and climate plan.

4. In order for a district heating and cooling system to qualify as efficient, Member States shall ensure that where it is built or its supply units are substantially refurbished, the district heating or cooling system meet the criteria set out in paragraph 1 or 2 applicable at the time when it starts or continues its operation after the refurbishment. In addition, Member States shall ensure that when a district heating and cooling system is built or its supply units are substantially refurbished:

- (a) there is no increase in the use of fossil fuels other than natural gas in existing heat sources compared to the annual consumption averaged over the previous three calendar years of full operation before refurbishment; and
- (b) any new heat sources in that system do not use fossil fuels, except natural gas, if built or substantially refurbished until 2030.

5. Member States shall ensure that as from 1 January 2025, and every five years thereafter, operators of all existing district heating and cooling systems with a total heat and cold output exceeding 5 MW and which do not meet the criteria set out in paragraph 1, points (b) to (e), prepare a plan to ensure more efficient consumption of primary energy, to reduce distribution losses and to increase the share of renewable energy in heating and cooling supply. The plan shall include measures to meet the criteria set out in paragraph 1, points (b) to (e), and shall require approval by the competent authority.

6. Member States shall ensure that data centres with a total rated energy input exceeding 1 MW utilise the waste heat or other waste heat recovery applications unless they can show that it is not technically or economically feasible in accordance with the assessment referred to in paragraph 7.

7. In order to assess the economic feasibility of increasing energy efficiency of heat and cooling supply, Member States shall ensure that an installation level cost-benefit analysis in accordance with Annex XI is carried out where the following installations are newly planned or substantially refurbished:

- (a) a thermal electricity generation installation with an average annual total energy input exceeding 10 MW, in order to assess the cost and benefits of providing for the operation of the installation as a high-efficiency cogeneration installation;
- (b) an industrial installation with an average annual total energy input exceeding 8 MW in order to assess utilisation of the waste heat on-site and off-site;
- (c) a service facility with an annual average total energy input exceeding 7 MW, such as wastewater treatment facilities and LNG facilities, in order to assess utilisation of waste heat on-site and off-site;
- (d) a data centre with a total rated energy input exceeding 1 MW level in order to assess the cost and benefit analysis, including, but not limited to, technical feasibility, cost-efficiency and the impact on energy efficiency and local heat demand, including seasonal variation, of utilising the waste heat to satisfy economically justified demand, and of the connection of that installation to a district heating network or an efficient/RES-based district cooling system or other waste heat recovery applications.

The analysis referred to in the first subparagraph, point (d), shall consider cooling system solutions that allow removing or capturing the waste heat at useful temperature level with minimal ancillary energy inputs.

Member States shall aim to remove barriers for the utilisation of waste heat and provide support for the uptake of waste heat where the installations are newly planned or refurbished.

The fitting of equipment to capture carbon dioxide produced by a combustion installation with a view to it being geologically stored as provided for in Directive 2009/31/EC shall not be considered as refurbishment for the purpose of points (b) and (c) of this paragraph.

Member States shall require the cost-benefit analysis to be carried out in cooperation with the companies responsible for the operation of the facility.

8. Member States may exempt from paragraph 7:

- (a) peak load and back-up electricity generating installations which are planned to operate under 1 500 operating hours per year as a rolling average over a period of five years, based on a verification procedure established by the Member States ensuring that this exemption criterion is met;
- (b) installations that need to be located close to a geological storage site approved under Directive 2009/31/EC;
- (c) data centres whose waste heat is or will be used in a district heating network or directly for space heating, domestic hot water preparation or other uses in the building or group of buildings or facilities where it is located.

Member States may also lay down thresholds, expressed in terms of the amount of available useful waste heat, the demand for heat or the distances between industrial installations and district heating networks, for exempting individual installations from paragraph 7, points (c) and (d).

Member States shall notify exemptions adopted under this paragraph to the Commission.

9. Member States shall adopt authorisation criteria as referred to in Article 8 of Directive (EU) 2019/944, or equivalent permit criteria, in order to:

- (a) take into account the outcome of the comprehensive assessment referred to in Article 25(1);
- (b) ensure that the requirements laid down in paragraph 7 are fulfilled;
- (c) take into account the outcome of the cost-benefit analysis referred to in paragraph 7.

10. Member States may exempt individual installations from being required, by the authorisation or equivalent permit criteria referred to in paragraph 9, to implement options whose benefits exceed their costs, if there are imperative reasons of law, ownership or finance for doing so. In those cases the Member State concerned shall submit a reasoned decision to the Commission within three months of the date of taking that decision. The Commission may issue an opinion on the decision within three months of its receipt.

11. Paragraphs 7, 8, 9 and 10 of this Article shall apply to installations covered by Directive 2010/75/EU without prejudice to the requirements laid down in that Directive.

12. Member States shall collect information on cost-benefit analyses carried out in accordance with paragraph 7, points (a) to (d). That information should contain at least the data on available heat supply amounts and heat parameters, number of planned operating hours every year and geographical location of the sites. Those data shall be published with due respect for their potential sensitivity.

13. On the basis of the harmonised efficiency reference values referred to in Annex III, point (d), Member States shall ensure that the origin of electricity produced from high-efficiency cogeneration can be guaranteed according to objective, transparent and non-discriminatory criteria laid down by each Member State. They shall ensure that that guarantee of origin complies with the requirements laid down in, and contains at least the information specified in, Annex XII. Member States shall mutually recognise their guarantees of origin, exclusively as proof of the information referred to in this

paragraph. Any refusal to recognise a guarantee of origin as such proof, in particular for reasons relating to the prevention of fraud, shall be based on objective, transparent and non-discriminatory criteria. Member States shall notify the Commission of such refusal and set out the reasons for it. In the event of a refusal to recognise a guarantee of origin, the Commission may adopt a decision to compel the refusing party to recognise it, in particular with regard to objective, transparent and non-discriminatory criteria on which such recognition is based.

14. Member States shall ensure that any available support for cogeneration is subject to the electricity produced originating from high-efficiency cogeneration and the waste heat being effectively used to achieve primary energy savings. Public support to cogeneration and district heating generation and networks shall be subject to State aid rules, where applicable.

Article 27

Energy transformation, transmission and distribution

1. National energy regulatory authorities shall apply the energy efficiency first principle, in accordance with Article 3 of this Directive, in carrying out the regulatory tasks provided for in Directives 2009/73/EC and (EU) 2019/944 regarding their decisions on the operation of the gas and electricity infrastructure, including their decisions on network tariffs. In addition to the energy efficiency first principle, national energy regulatory authorities may take into account cost efficiency, system efficiency and security of supply, and market integration, while safeguarding the Union's climate targets and sustainability, as set out in Article 18 of Regulation (EU) 2019/943 and in Article 13 of Regulation (EC) No 715/2009.

2. Member States shall ensure that gas and electricity transmission and distribution system operators apply the energy efficiency first principle, in accordance with Article 3 of this Directive, in their network planning, network development and investment decisions. National regulatory authorities or other designated national authorities shall verify that methodologies used by transmission system operators and distribution system operators assess alternatives in the cost-benefit analysis and take into account the wider benefits of energy efficiency solutions, demand-side flexibility and investment into assets that contribute to climate change mitigation. National regulatory authorities and other designated authorities shall also verify the implementation of the energy efficiency first principle by the transmission system operators or distribution system operators when approving, verifying or monitoring their projects and network development plans pursuant to Article 22 of Directive 2009/73/EC and to Article 32(3) and Article 51 of Directive (EU) 2019/944. National regulatory authorities may provide methodologies and guidance on how to assess alternatives in the cost-benefit analysis in close cooperation with the transmission system operators and distribution system operators, which can share key technical expertise.

3. Member States shall ensure that transmission and distribution system operators monitor and quantify the overall volume of network losses and, where it is technically and financially feasible, optimise networks and improve network efficiency. Transmission and distribution system operators shall report those measures and expected energy savings through the reduction of network losses to the national energy regulatory authority. Member States shall ensure that transmission and distribution system operators assess energy efficiency improvement measures with regard to their existing gas or electricity transmission or distribution systems and improve energy efficiency in infrastructure design and operation, especially in terms of smart grid deployment. Member States shall encourage transmission and distribution system operators to develop innovative solutions to improve the energy efficiency of existing and future systems through incentive-based regulations in accordance with the tariff principles set out in Article 18 of Regulation (EU) 2019/943 and Article 13 of Regulation (EC) No 715/2009.

4. National energy regulatory authorities shall include a specific section on the progress achieved in energy efficiency improvements regarding the operation of the gas and electricity infrastructure in the annual report drawn up pursuant to Article 41 of Directive 2009/73/EC and pursuant to Article 59(1), point (i), of Directive (EU) 2019/944. In those reports, national energy regulatory authorities shall provide an assessment of the overall efficiency in the operation of the gas and electricity infrastructure, the measures carried out by transmission and distribution system operators and, where applicable, provide recommendations for energy efficiency improvements, including cost-efficient alternatives that reduce peak loads and overall electricity use.

5. For electricity, Member States shall ensure that network regulation and network tariffs fulfil the criteria set out in Annex XIII, taking into account network codes and guidelines developed pursuant to Regulation (EU) 2019/943 and the obligation set out in Article 59(7), point (a), of Directive (EU) 2019/944 to allow for necessary investments in the networks to be carried out in a manner ensuring the viability of the networks.
6. Member States may permit components of schemes and tariff structures with a social aim for net-bound energy transmission and distribution, provided that any disruptive effects on the transmission and distribution system are kept to the minimum necessary and are not disproportionate to the social aim.
7. National regulatory authorities shall ensure the removal of those incentives in transmission and distribution tariffs that are detrimental to the energy efficiency of the generation, transmission, distribution and supply of electricity and gas. Member States shall ensure efficiency in infrastructure design and the operation of the existing infrastructure, in accordance with Regulation (EU) 2019/943, and that tariffs allow for demand response.
8. Transmission system operators and distribution system operators shall comply with Annex XIV.
9. Where appropriate, national regulatory authorities may require transmission system operators and distribution system operators to encourage high-efficiency cogeneration to be located close to areas of heat demand by reducing the connection and use-of-system charges.
10. Member States may allow producers of electricity from high-efficiency cogeneration wishing to be connected to the grid to issue a call for tender for the connection work.
11. When reporting under Directive 2010/75/EU, and without prejudice to Article 9(2) of that Directive, Member States shall consider including information on energy efficiency levels of installations undertaking the combustion of fuels with total rated thermal input of 50 MW or more in the light of the relevant best available techniques developed in accordance with Directive 2010/75/EU.

CHAPTER VI

HORIZONTAL PROVISIONS

Article 28

Availability of qualification, accreditation and certification schemes

1. Member States shall set up a network ensuring the appropriate level of competences for energy efficiency-related professions that corresponds to market needs. Member States, in close cooperation with the social partners, shall ensure that certification or equivalent qualification schemes, including, where necessary, suitable training programmes, are available for energy efficiency-related professions including providers of energy services, providers of energy audits, energy managers, independent experts, installers of building elements as referred to in Directive 2010/31/EU, and providers of integrated renovation works, and are reliable and contribute to national energy efficiency objectives and the overall Union decarbonisation objectives.

Member States shall ensure that providers of certification or equivalent qualification schemes, including, where necessary, suitable training programmes are accredited in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council ⁽⁴⁷⁾ or approved in line with converging national legislation or standards.

⁽⁴⁷⁾ Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

2. Member States shall promote participation in certification, training and education programmes to ensure the appropriate level of competences for energy efficiency professions that correspond to market needs.
3. By 11 October 2024, the Commission shall:
 - (a) in cooperation with a group of experts nominated by Member States, set up a framework for or design a campaign to attract more people to energy efficiency professions while ensuring respect for the principle of non-discrimination;
 - (b) assess the viability of setting up a single point of access platform, making use of existing initiatives where possible, to provide support to the Member States in setting up their measures to ensure the appropriate level of qualified professionals needed to keep up with the pace of progress in energy efficiency to reach the Union's climate and energy targets. The platform would gather experts from Member States, the social partners, education institutions, academia and other relevant stakeholders to foster and promote best practices of qualification schemes and training programmes to ensure more energy efficiency professionals and to re-skill or up-skill existing professionals in order to meet market needs.
4. Member States shall ensure that national certification, or equivalent qualification schemes, including, where necessary, training programmes, take into account existing European or international standards on energy efficiency.
5. Member States shall make publicly available the certification, equivalent qualification schemes or suitable training programmes referred to in paragraph 1, and shall cooperate among themselves and with the Commission on comparisons between, and recognition of, the schemes.

Member States shall take appropriate measures to make consumers aware of the availability of the schemes in accordance with Article 29(1).

6. By 31 December 2024 and at least every four years thereafter, Member States shall assess whether the schemes ensure the necessary level of competences and equal access to all individuals in accordance with the principle of non-discrimination for energy services providers, energy auditors, energy managers, independent experts, installers of building elements as referred to in Directive 2010/31/EU, and providers of integrated renovation works. Member States shall also assess the gap between available and in demand professionals. Member States shall make the assessment and recommendations thereof publicly available and submit them through the e-platform established in accordance with Article 28 of Regulation (EU) 2018/1999.

Article 29

Energy services

1. Member States shall promote the energy services market and access to it for SMEs by disseminating clear and easily accessible information on:
 - (a) available energy service contracts and clauses that should be included in such contracts to guarantee energy savings and final customers' rights;
 - (b) financial instruments, incentives, grants, revolving funds, guarantees, insurance schemes, and loans to support energy efficiency service projects;
 - (c) available energy services providers, such as ESCOs, that are qualified or certified and their qualifications or certifications in accordance with Article 28;
 - (d) available monitoring and verification methodologies and quality control schemes.
2. Member States shall encourage the development of quality labels, inter alia, by trade associations, based on European or international standards where relevant.

3. Member States shall make publicly available and regularly update a list of available energy service providers that are qualified or certified and their qualifications or certifications in accordance with Article 28, or provide an interface where energy service providers can provide that information.

4. Member States shall promote and ensure, where technically and economically feasible, the use of energy performance contracting for renovations of large buildings that are owned by public bodies. For renovations of large non-residential buildings with a total useful floor area above 750 m², Member States shall ensure that public bodies assess the feasibility of using energy performance contracting and other performance-based energy services.

Member States may encourage public bodies to combine energy performance contracting with expanded energy services, including demand response and storage, in order to ensure energy savings and maintain the results obtained over time through continuous monitoring, effective operation and maintenance.

5. Member States shall support the public sector in taking up energy service offers, in particular for building refurbishment, by:

- (a) providing model contracts for energy performance contracting which include at least the items listed in Annex XV and take into account the existing European or international standards, available tendering guidelines and the Eurostat guide to the statistical treatment of energy performance contracts in government accounts;
- (b) providing information on best practices for energy performance contracting, including, if available, a cost-benefit analysis using a life-cycle approach;
- (c) promoting and making publicly available a database of implemented and ongoing energy performance contracting projects that includes the projected and achieved energy savings.

6. Member States shall support the proper functioning of the energy services market, by taking the following measures:

- (a) identifying and publicising one or more points of contact where final customers can obtain the information referred to in paragraph 1;
- (b) removing the regulatory and non-regulatory barriers that impede the uptake of energy performance contracting and other energy efficiency service models for the identification or implementation of energy saving measures, or both;
- (c) setting up and promoting the role of advisory bodies and independent market intermediaries including one-stop shops or similar support mechanisms to stimulate market development on the demand and supply sides, and making information about those support mechanisms publicly available and accessible to market actors.

7. For the purpose of supporting the proper functioning of the energy services market, Member States may establish an individual mechanism or designate an ombudsperson to ensure the efficient handling of complaints and out-of-court settlement of disputes arising from energy service and energy performance contracts.

8. Member States shall ensure that energy distributors, distribution system operators and retail energy sales companies refrain from any activities that may impede the demand for and delivery of energy services or energy efficiency improvement measures, or hinder the development of markets for such services or measures, including foreclosing the market for competitors or abusing dominant positions.

Article 30

National energy efficiency fund, financing and technical support

1. Without prejudice to Articles 107 and 108 TFEU, Member States shall facilitate the establishment of financing facilities, or the use of existing ones, for energy efficiency improvement measures to maximise the benefits of multiple streams of financing and the combination of grants, financial instruments and technical assistance.

2. The Commission shall, where appropriate, directly or via financial institutions, assist Member States in setting up financing facilities and project development assistance facilities at national, regional or local level with the aim of increasing investments in energy efficiency in different sectors and of protecting and empowering people affected by energy poverty, vulnerable customers, people in low-income households and, where applicable, people living in social housing, including by integrating an equality perspective so that no one is left behind.

3. Member States shall adopt measures that promote energy efficiency lending products, such as green mortgages and green loans, secured and unsecured, and ensure that they are offered widely and in a non-discriminatory manner by financial institutions and, are visible and accessible to consumers. Member States shall adopt measures to facilitate the implementation of on-bill and on-tax financing schemes, taking into account the Commission guidance provided in accordance with paragraph 10. Member States shall ensure that banks and other financial institutions receive information on opportunities to participate in the financing of energy efficiency improvement measures, including through the creation of public-private partnerships. Member States shall encourage the setting up of loan guarantee facilities for energy efficiency investment.

4. Without prejudice to Articles 107 and 108 TFEU, Member States shall promote the establishment of financial support schemes to increase the uptake of energy efficiency improvement measures for the substantial refurbishment of individual and district heating and cooling systems.

5. Member States shall promote the establishment of local expertise and technical assistance, where appropriate through existing networks and facilities, to advise on best practices with regard to achieving the decarbonisation of local district heating and cooling, such as access to dedicated financial support.

6. The Commission shall facilitate the exchange of best practices between the competent national or regional authorities or bodies, including through annual meetings of the regulatory bodies, public databases with information on the implementation of measures by Member States, and cross-country comparisons.

7. In order to mobilise private financing for energy efficiency measures and energy renovation and to contribute to the achievement the Union's energy efficiency targets and of the national contributions pursuant to Article 4 of this Directive and of the objectives in Directive 2010/31/EU, the Commission shall conduct a dialogue with both public and private financial institutions, as well as relevant specific sectors in order to map out needs and possible actions it can take.

8. The actions referred to in paragraph 7 shall include the following elements:

- (a) mobilising capital investment into energy efficiency by considering the wider impacts of energy savings;
- (b) facilitating the implementation of dedicated energy efficiency financial instruments and financing schemes at scale to be set up by financial institutions;
- (c) ensuring better energy and finance performance data by:
 - (i) examining further how energy efficiency investments improve underlying asset values;
 - (ii) supporting studies to assess the monetisation of the non-energy benefits of energy efficiency investments.

9. For the purpose of mobilising private financing of energy efficiency measures and energy renovation, Member States shall, when implementing this Directive:

- (a) consider ways to make better use of energy management systems and energy audits under Article 11 to influence decision-making;

- (b) make optimal use of the possibilities and tools available in the Union budget and proposed in the smart finance for smart buildings initiative and in Commission communication of 14 October 2020 on 'A Renovation Wave for Europe – greening our buildings, creating jobs, improving lives'.

10. By 31 December 2024, the Commission shall provide guidance for Member States and market actors on how to unlock private investment.

The guidance shall have the purpose of helping Member States and market actors to develop and implement their energy efficiency investments, including in the various Union programmes, and shall propose adequate financial mechanisms and innovative financing solutions, with a combination of grants, financial instruments and project development assistance, to scale up existing initiatives and use the Union programmes as a catalyst to leverage and trigger private financing.

11. Member States may set up a national energy efficiency fund. The purpose of this fund shall be to implement energy efficiency measures to support Member States in meeting their national energy efficiency contributions and their indicative trajectories referred to in Article 4(2). The national energy efficiency fund may be established as a dedicated fund within an already existing national facility promoting capital investments. The national energy efficiency fund may be financed with revenues from the allowance auctions pursuant to the EU ETS on buildings and transport sectors.

12. Where Member States set up national energy efficiency funds, as referred to in paragraph 11 of this Article, they shall establish financing instruments, including public guarantees, to increase the uptake of private investments in energy efficiency and of the energy efficiency lending products and innovative schemes referred to in paragraph 3 of this Article. Pursuant to Article 8(3) and Article 24, the national energy efficiency fund shall support the implementation of measures as a priority among people affected by energy poverty, vulnerable customers, people in low-income households and, where applicable, people living in social housing. That support shall include financing for energy efficiency measures for SMEs in order to leverage and trigger private financing for SMEs.

13. Member States may allow public bodies to fulfil the obligations set out in Article 6(1) by means of annual contributions to the national energy efficiency fund equivalent to the amount of the investments required to achieve those obligations.

14. Member States may provide that obligated parties can fulfil their obligations set out in Article 8(1) and (4) by contributing every year to the national energy efficiency fund an amount equal to the investments required to achieve those obligations.

15. Member States may use their revenues from annual emission allocations under Decision No 406/2009/EC for the development of innovative financing for energy efficiency improvements.

16. The Commission shall assess the effectiveness and efficiency of energy efficiency public funding support at Union and national level and the Member States' capacity to increase the uptake of private investments in energy efficiency, while also taking into account public financing needs expressed in the national energy and climate plans. The Commission shall evaluate whether an energy efficiency mechanism at Union level, with the objective of providing a Union guarantee, technical assistance and associated grants to enable the implementation of financial instruments, and financing and support schemes at national level, could support in a cost-effective way the achievement of the Union energy efficiency and climate targets, and, if appropriate, propose the establishment of such a mechanism.

To that end, the Commission shall submit by 30 March 2024 a report to the European Parliament and to the Council, accompanied, where appropriate, by legislative proposals.

17. Member States shall report to the Commission by 15 March 2025 and every two years thereafter, as part of their integrated national energy and climate progress reports submitted pursuant to Article 17 and in accordance with Article 21 of Regulation (EU) 2018/1999, the following data:

- (a) the volume of public investments on energy efficiency and the average leverage factor achieved by public funding supporting energy efficiency measures;
- (b) the volume of energy efficiency lending products, distinguishing between different products;
- (c) where relevant, national financing programmes put in place to increase uptake of energy efficiency and best practices, and innovative financing schemes for energy efficiency.

To facilitate the preparation of the report referred to in the first subparagraph of this paragraph, the Commission shall integrate the requirements set out in that subparagraph in the common template laid down in the implementing acts adopted pursuant to Article 17(4) of Regulation (EU) 2018/1999.

18. For the purpose of fulfilling the obligation referred to in paragraph 17, point (b), and without prejudice to additional national measures, Member States shall take into consideration the existing disclosure obligations for financial institutions, including:

- (a) the disclosure rules for credit institutions under Commission Delegated Regulation (EU) 2021/2178 ⁽⁴⁸⁾;
- (b) the ESG risks disclosure requirements for credit institutions in accordance with Article 449a of Regulation (EU) No 575/2013 of the European Parliament and of the Council ⁽⁴⁹⁾.

To facilitate the collection and aggregation of data on volume of energy efficiency lending product for the purpose of fulfilling the obligation referred to in paragraph 17, point (b), the Commission shall by 15 March 2024 provide guidance to Member States on the arrangements for accessing, collecting and aggregating data on the volume of energy efficiency lending products at national level.

Article 31

Conversion factors and primary energy factors

1. For the purpose of comparison of energy savings and conversion to a comparable unit, the net calorific values in Annex VI of Regulation (EU) 2018/2066 and the primary energy factors set out in paragraph 2 of this Article shall apply unless the use of other values or factors can be justified.
2. A primary energy factor shall be applicable when energy savings are calculated in primary energy terms using a bottom-up approach based on final energy consumption.
3. For savings in kWh electricity, Member States shall apply a coefficient in order to accurately calculate the resulting primary energy consumption savings. Member States shall apply a default coefficient of 1,9 unless they use their discretion to define a different coefficient based upon justified national circumstances.
4. For savings in kWh of other energy carriers, Member States shall apply a coefficient in order to accurately calculate the resulting primary energy consumption savings.
5. Where Member States establish their own coefficient to a default value provided pursuant to this Directive, Member States shall establish that coefficient through a transparent methodology on the basis of national, regional or local circumstances affecting primary energy consumption. The circumstances shall be substantiated, verifiable and based on objective and non-discriminatory criteria.

⁽⁴⁸⁾ Commission Delegated Regulation (EU) 2021/2178 of 6 July 2021 supplementing Regulation (EU) 2020/852 of the European Parliament and of the Council by specifying the content and presentation of information to be disclosed by undertakings subject to Articles 19a or 29a of Directive 2013/34/EU concerning environmentally sustainable economic activities, and specifying the methodology to comply with that disclosure obligation (OJ L 443, 10.12.2021, p. 9).

⁽⁴⁹⁾ Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

6. Where establishing an own coefficient, Member States shall take into account the energy mix included in the update of their integrated national energy and climate plans submitted pursuant to Article 14(2) of Regulation (EU) 2018/1999 and their subsequent integrated national energy and climate plans notified to the Commission pursuant to Article 3 and Articles 7 to 12 of that Regulation. If they deviate from the default value, Member States shall notify the coefficient that they use to the Commission along with the calculation methodology and underlying data in those updates and subsequent plans.

7. By 25 December 2026 and every four years thereafter, the Commission shall revise the default coefficients on the basis of observed data. Those revisions shall be carried out taking into account its effects on Union law such as Directive 2009/125/EC and Regulation (EU) 2017/1369.

CHAPTER VII

FINAL PROVISIONS

Article 32

Penalties

Member States shall lay down the rules on penalties applicable to infringements of national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall by 11 October 2025 notify the Commission of those rules and of those measures and shall notify it without delay of any subsequent amendment affecting them.

Article 33

Delegated acts

1. The Commission is empowered to adopt delegated acts in accordance with Article 34 to review the harmonised efficiency reference values laid down in Regulation (EU) 2015/2402.

2. The Commission is empowered to adopt delegated acts in accordance with Article 34 to amend this Directive by adapting to technical progress the values, calculation methods, default primary energy coefficients and the requirements referred to in Article 31 and in Annexes II, III, V, VIII to XII, and XIV.

3. The Commission is empowered to adopt delegated acts in accordance with Article 34 to supplement this Directive by establishing, after having consulted the relevant stakeholders, a common Union scheme for rating the sustainability of data centres located in its territory. The Commission shall adopt the first such delegated act by 31 December 2023. The common Union scheme shall establish the definition of data centre sustainability indicators and shall set out the key performance indicators and the methodology to measure them.

Article 34

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 33 shall be conferred on the Commission for a period of five years from 10 October 2023. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

3. The delegation of power referred to in Article 33 may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Article 33 shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 35

Review and monitoring of implementation

1. In the context of its State of the Energy Union report submitted pursuant to Article 35 of Regulation (EU) 2018/1999, the Commission shall report on the functioning of the carbon market in accordance with Article 35(1) and Article 35(2), point (c), of that Regulation, taking into consideration the effects of the implementation of this Directive.

2. By 31 October 2025 and every four years thereafter, the Commission shall evaluate the existing measures to achieve energy efficiency increase and decarbonisation in heating and cooling. The evaluation shall take into account all of the following:

- (a) energy efficiency and GHG emissions trends in heating and cooling, including in district heating and cooling;
- (b) interlinkages between measures taken;
- (c) changes in energy efficiency and greenhouse gas emissions in the heating and cooling;
- (d) existing and planned energy efficiency policies and measures and greenhouse gas reduction policies and measures at Union and national level;
- (e) measures which Member States provided in their comprehensive assessments pursuant to Article 25(1) of this Directive and notified in accordance with Article 17(1) of Regulation (EU) 2018/1999.

By 31 October 2025 and every four years thereafter, the Commission shall submit a report to the European Parliament and to the Council on that evaluation and, if appropriate, propose measures to ensure the achievement of the Union's climate and energy targets.

3. Member States shall submit to the Commission before 30 April each year statistics on national electricity and heat production from high and low efficiency cogeneration, in accordance with the general principles set out in Annex II, in relation to total heat and electricity production. They shall also submit annual statistics on cogeneration heat and electricity capacities and fuels for cogeneration, and on district heating and cooling production and capacities, in relation to total heat and electricity production and capacities. Member States shall submit statistics on primary energy savings achieved by the application of cogeneration in accordance with the methodology set out in Annex III.

4. By 1 January 2021, the Commission shall submit a report to the European Parliament and to the Council, on the basis of an assessment of the potential for energy efficiency in conversion, transformation, transmission, transportation and storage of energy, accompanied, where appropriate, by legislative proposals.

5. By 31 December 2021, the Commission shall, subject to any changes to the provisions relating to retail markets in Directive 2009/73/EC, carry out an assessment, and submit a report to the European Parliament and to the Council, on the provisions related to metering, billing and consumer information for natural gas, with the aim of aligning them, where appropriate, with the relevant provisions for electricity in Directive (EU) 2019/944, in order to strengthen consumer protection and enable final customers to receive more frequent, clear and up-to-date information about their natural gas consumption and to regulate their energy use. As soon as possible after the submission of that report, the Commission shall, where appropriate, adopt legislative proposals.

6. By 31 October 2022, the Commission shall assess whether the Union has achieved its 2020 headline targets on energy efficiency.

7. By 28 February 2027 and every five years thereafter, the Commission shall evaluate the implementation of this Directive and submit a report to the European Parliament and to the Council.

That evaluation shall include:

- (a) an assessment of the general effectiveness of this Directive and the need to further adjust the Union's energy efficiency policy in accordance with the objectives of the Paris Agreement and in light of economic and innovation developments;
- (b) a detailed assessment of the aggregated macroeconomic impact of this Directive, with an emphasis on the effects on the Union's energy security, energy prices, minimising energy poverty, economic growth, competitiveness, job creation, mobility cost and household purchasing power;
- (c) the Union's 2030 headline targets on energy efficiency set out in Article 4(1) with a view to revising those targets upwards in the event of substantial cost reductions resulting from economic or technological developments, or where needed to meet the Union's decarbonisation targets for 2040 or 2050, or its international commitments for decarbonisation;
- (d) whether Member States are to continue to achieve new annual savings in accordance with Article 8(1), first subparagraph, point (b)(iv), for a ten-year periods after 2030;
- (e) whether Member States are to continue to ensure that at least 3 % of the total floor area of heated and/or cooled buildings that are owned by public bodies is renovated each year in accordance with Article 6(1) with a view to revising the renovation rate in that Article;
- (f) whether Member States are to continue to achieve a share of energy savings among people affected by energy poverty, vulnerable customers and, where applicable, people living in social housing, pursuant to Article 8(3) for the ten-year periods after 2030;
- (g) whether Member States are to continue to achieve a reduction of final energy consumption in accordance with Article 5(1);
- (h) the impacts of this Directive on supporting economic growth, increasing industrial output, the deployment of renewables or advanced efforts to climate neutrality.

The evaluation shall also cover the effects on efforts to electrify the economy and the introduction of hydrogen, including whether any change to the treatment of clean renewable energy sources might be justified, and shall propose, where appropriate, solutions to any potentially identified adverse effect.

That report shall be accompanied by a detailed assessment of whether there is a need to amend this Directive in the interests of regulatory simplification and, where appropriate, by proposals for further measures.

8. By 31 October 2032, the Commission shall assess whether the Union has achieved its 2030 headline targets on energy efficiency.

Article 36

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with Articles 1, 2 and 3, Article 4(1) to (4), Article 4(5), first, second, fourth, fifth and sixth subparagraphs, Article 4(6) and (7), Articles 5 to 11, Article 12(2) to (5), Articles 21 to 25, Article 26(1), (2) and (4) to (14), Article 27, Article 28(1) to (5), Articles 29 to 32 and Annexes I, III to VII, X, XI and XV by 11 October 2025.

Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with Article 4(5), third subparagraph, Article 12(1), Article 26(3) and Article 28(6) by the dates referred to therein. They shall immediately communicate the text of those measures to the Commission.

When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. They shall also include a statement that references in existing laws, regulations and administrative provisions to the Directive repealed by this Directive shall be construed as references to this Directive. Member States shall determine how such reference is to be made and how that statement is to be formulated.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 37

Amendment to Regulation (EU) 2023/955

In Article 2 of Regulation (EU) 2023/955, point (1) is replaced by the following:

‘(1) “energy poverty” means energy poverty as defined in Article 2, point (52), of Directive (EU) 2023/1791 of the European Parliament and of the Council (*).

(*) Directive (EU) 2023/1791 of the European Parliament and of the Council of 13 September 2023 on energy efficiency and amending Regulation (EU) 2023/955 (OJ L 231, 20.9.2023, p. 1).’.

Article 38

Repeal

Directive 2012/27/EU, as amended by the acts listed in Part A of Annex XVI is repealed with effect from 12 October 2025, without prejudice to the obligations of the Member States relating to the time-limits for the transposition into national law of the Directives set out in Part B of Annex XVI.

References to the repealed Directive shall be construed as references to this Directive and shall be read in accordance with the correlation table in Annex XVII.

*Article 39***Entry into force and application**

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Articles 13, 14, 15, 16, 17, 18, 19 and 20 and Annexes II, VIII, IX, XII, XIII and XIV shall apply from 12 October 2025.

Article 37 shall apply from 30 June 2024.

*Article 40***Addressees**

This Directive is addressed to the Member States.

Done at Strasbourg, 13 September 2023.

For the European Parliament

The President

R. METSOLA

For the Council

The President

J. M. ALBARES BUENO

ANNEX I

NATIONAL CONTRIBUTIONS TO THE UNION'S ENERGY EFFICIENCY TARGETS IN 2030 IN FINAL ENERGY CONSUMPTION AND/OR PRIMARY ENERGY CONSUMPTION

1. The level of national contributions is calculated on the basis of the indicative formula:

$$FEC_{C2030} = C_{EU} (1 - \text{Target}) FEC_{B2030}$$

$$PEC_{C2030} = C_{EU} (1 - \text{Target}) PEC_{B2030}$$

Where C_{EU} is a correction factor, Target is the level of national-specific ambition and FEC_{B2030} PEC_{B2030} is the 2020 EU Reference Scenario used as a baseline for 2030.

2. The following indicative formula represents the objective criteria reflecting the factors listed in Article 4(3), points (d) (i) to (iv), each used for defining the level of national-specific ambition in % (Target) and having the same weight in the formula (0,25):
 - (a) early action dependent contribution ($F_{\text{early-action}}$);
 - (b) GDP-per-capita dependent contribution (F_{wealth});
 - (c) energy intensity dependent contribution ($F_{\text{intensity}}$);
 - (d) cost-effective energy savings potential contribution ($F_{\text{potential}}$).
3. $F_{\text{early-action}}$ shall be calculated for each Member State as the product of its amount of energy savings and the improvement in the energy intensity that each Member State achieved. The amount of energy savings for each Member State shall be calculated on the basis of the reduction of energy consumption (in toe) to the Union's reduction of energy consumption between the three-year average for the period 2007-2009 and the three-year average for the period 2017-2019. The improvement in the energy intensity for each Member State shall be calculated on the basis of the reduction of energy intensity (in toe/EUR) to the Union's reduction of energy intensity between the three-year average for the period 2007-2009 and the three-year average for the period 2017-2019.
4. F_{wealth} shall be calculated for each Member State on the basis of its three-year average Eurostat's real GDP per capita index to the Union's three-year average over the 2017-2019 period, expressed in Purchasing power parities (PPPs).
5. $F_{\text{intensity}}$ shall be calculated for each Member State on the basis of its three-year average final energy intensity (FEC or PEC per real GDP in PPPs) index to the Union's three-year average over 2017-2019 period.
6. $F_{\text{potential}}$ shall be calculated for each Member State on the basis of the final or primary energy savings under the PRIMES MIX 55 % scenario for 2030. The savings are expressed in relation to 2020 EU Reference Scenario projections for 2030.
7. For each criteria provided in point 2(a) to (d), a lower and upper limit shall be applied. The level of ambition for factors F_{wealth} $F_{\text{intensity}}$ and $F_{\text{potential}}$ shall be capped at 50 % and 150 % of the Union average level of ambition under a given factor. The level of ambition for factor $F_{\text{early-action}}$ shall be capped at 50 % and 100 % of the Union average level of ambition.
8. The source of the input data used to calculate the factors is Eurostat unless stated otherwise.

9. F_{total} shall be calculated as the weighted sum of all four factors ($F_{\text{early-action}}$, F_{wealth} , $F_{\text{intensity}}$ and $F_{\text{potential}}$). The target shall be then calculated as the product of the total factor F_{total} and the Union target.
 10. The Commission shall calculate a primary and final energy correction factor C_{EU} , which shall be applied to adjust the sum of the formula results for all national contributions to the respective Union targets in 2030. The factor C_{EU} is identical for all Member States.
-

ANNEX II

GENERAL PRINCIPLES FOR THE CALCULATION OF ELECTRICITY FROM COGENERATION

Part I

General principles

Values used for calculation of electricity from cogeneration shall be determined on the basis of the expected or actual operation of the unit under normal conditions of use. For micro-cogeneration units the calculation may be based on certified values.

- (1) Electricity production from cogeneration shall be considered equal to total annual electricity production of the unit measured at the outlet of the main generators if the following conditions are met:
 - (a) in cogeneration units of types (2), (4), (5), (6), (7) and (8) as referred to in Part II with an annual overall efficiency set by Member States at a level of at least 75 %;
 - (b) in cogeneration units of types (1) and (3) as referred to in Part II with an annual overall efficiency set by Member States at a level of at least 80 %.
- (2) In cogeneration units with an annual overall efficiency below the value referred to in point (1)(a), namely the cogeneration units of types (2), (4), (5), (6), (7), and (8) as referred to in Part II, or with an annual overall efficiency below the value referred to in point (1)(b), namely the cogeneration units of types (1) and (3) as referred to in Part II, electricity from cogeneration is calculated according to the following formula:

$$E_{\text{CHP}} = H_{\text{CHP}} * C$$

where:

E_{CHP} is the amount of electricity from cogeneration;

C is the power-to-heat ratio;

H_{CHP} is the amount of useful heat from cogeneration (calculated for this purpose as total heat production minus any heat produced in separate boilers or by live steam extraction from the steam generator before the turbine).

The calculation of electricity from cogeneration shall be based on the actual power-to-heat ratio. If the actual power-to-heat ratio of a cogeneration unit is not known, the following default values may be used, in particular for statistical purposes, for units of types (1), (2), (3), (4) and (5) as referred to in Part II provided that the calculated cogeneration electricity is less or equal to total electricity production of the unit:

Type of the unit	Default power to heat ratio, C
Combined cycle gas turbine with heat recovery	0,95
Steam back pressure turbine	0,45
Steam condensing extraction turbine	0,45
Gas turbine with heat recovery	0,55
Internal combustion engine	0,75

If Member States introduce default values for power-to-heat ratios for units of types (6), (7), (8), (9), (10) and (11) as referred to in Part II, such default values shall be published and shall be notified to the Commission.

- (3) If a share of the energy content of the fuel input to the cogeneration process is recovered in chemicals and recycled, that share can be subtracted from the fuel input before calculating the overall efficiency used in points (1) and (2).

- (4) Member States may determine the power-to-heat ratio as the ratio of electricity to useful heat when operating in cogeneration mode at a lower capacity using operational data of the specific unit.
- (5) Member States may use reporting periods other than annual reporting periods for the purpose of the calculations in accordance with points (1) and (2).

Part II

Cogeneration technologies covered by this Directive

- (1) Combined cycle gas turbine with heat recovery
- (2) Steam back pressure turbine
- (3) Steam condensing extraction turbine
- (4) Gas turbine with heat recovery
- (5) Internal combustion engine
- (6) Microturbines
- (7) Stirling engines
- (8) Fuel cells
- (9) Steam engines
- (10) Organic Rankine cycles
- (11) Any other type of technology or combination comprising cogeneration.

When implementing and applying the general principles for the calculation of electricity from cogeneration, Member States shall use the detailed Guidelines established by Commission Decision 2008/952/EC ⁽¹⁾.

⁽¹⁾ Commission Decision 2008/952/EC of 19 November 2008 establishing detailed guidelines for the implementation and application of Annex II to Directive 2004/8/EC of the European Parliament and of the Council (OJ L 338, 17.12.2008, p. 55).

ANNEX III

METHODOLOGY FOR DETERMINING THE EFFICIENCY OF THE COGENERATION PROCESS

Values used for calculation of efficiency of cogeneration and primary energy savings shall be determined on the basis of the expected or actual operation of the unit under normal conditions of use.

(a) High-efficiency cogeneration

For the purpose of this Directive, high-efficiency cogeneration shall fulfil the following criteria:

- cogeneration production from cogeneration units shall provide primary energy savings calculated in accordance with point (b) of at least 10 % compared with the references for separate production of heat and electricity;
- production from small-scale and micro-cogeneration units providing primary energy savings may qualify as high-efficiency cogeneration;
- for cogeneration units that are built or substantially refurbished after the transposition of this Annex, direct emissions of the carbon dioxide from cogeneration production that is fuelled with fossil fuels, are less than 270 gCO₂ per 1 kWh of energy output from the combined generation (including heating/cooling, power and mechanical energy);
- cogeneration units in operation before 10 October 2023, may derogate from this requirement until 1 January 2034 provided that they have a plan to reduce progressively the emissions to meet the threshold of less than 270 gCO₂ per 1 kWh by 1 January 2034 and that they have notified this plan to relevant operators and competent authorities.

When a cogeneration unit is built or substantially refurbished, Member States shall ensure that there is no increase in the use of fossil fuels other than natural gas in existing heat sources compared to the annual consumption averaged over the previous three calendar years of full operation before refurbishment, and that any new heat sources in that system do not use fossil fuels other than natural gas.

(b) Calculation of primary energy savings

The amount of primary energy savings provided by cogeneration production defined in accordance with Annex II shall be calculated on the basis of the following formula:

$$PES = \left(1 - \frac{1}{\frac{CHPH\eta}{RefH\eta} + \frac{CHPE\eta}{RefE\eta}} \right) \times 100\%$$

Where:

PES is primary energy savings.

CHP H η is the heat efficiency of the cogeneration production defined as annual useful heat output divided by the fuel input used to produce the sum of useful heat output and electricity from cogeneration.

Ref H η is the efficiency reference value for separate heat production.

CHP E η is the electrical efficiency of the cogeneration production defined as annual electricity from cogeneration divided by the fuel input used to produce the sum of useful heat output and electricity from cogeneration. Where a cogeneration unit generates mechanical energy, the annual electricity from cogeneration may be increased by an additional element representing the amount of electricity which is equivalent to that of mechanical energy. This additional element does not create a right to issue guarantees of origin in accordance with Article 26(13).

Ref E η is the efficiency reference value for separate electricity production.

(c) Calculations of energy savings using alternative calculation

Member States may calculate primary energy savings from a production of heat and electricity and mechanical energy as indicated below without applying Annex II to exclude the non-cogenerated heat and electricity parts of the same process. Such a production can be regarded as high-efficiency cogeneration provided that it fulfils the efficiency criteria set out in point (a) of this Annex and, for cogeneration units with an electrical capacity larger than 25 MW, the overall efficiency is above 70 %. However, specification of the quantity of electricity from cogeneration produced in such a production, for issuing a guarantee of origin and for statistical purposes, shall be determined in accordance with Annex II.

If primary energy savings for a process are calculated using alternative calculation as indicated above the primary energy savings shall be calculated using the formula in point (b) of this Annex replacing: 'CHP $H\eta$ ' with ' $H\eta$ ' and 'CHP $E\eta$ ' with ' $E\eta$ ', where:

$H\eta$ means the heat efficiency of the process, defined as the annual heat output divided by the fuel input used to produce the sum of heat output and electricity output.

$E\eta$ means the electricity efficiency of the process, defined as the annual electricity output divided by the fuel input used to produce the sum of heat output and electricity output. Where a cogeneration unit generates mechanical energy, the annual electricity from cogeneration may be increased by an additional element representing the amount of electricity which is equivalent to that of mechanical energy. This additional element will not create a right to issue guarantees of origin in accordance with Article 26(13).

Member States may use reporting periods other than annual reporting periods for the purpose of the calculations in accordance with points (b) and (c) of this Annex.

For micro-cogeneration units the calculation of primary energy savings may be based on certified data.

(d) Efficiency reference values for separate production of heat and electricity

The harmonised efficiency reference values shall consist of a matrix of values differentiated by relevant factors, including year of construction and types of fuel, and shall be based on a well-documented analysis taking into account, inter alia, data from operational use under realistic conditions, fuel mix and climate conditions as well as applied cogeneration technologies.

The efficiency reference values for separate production of heat and electricity in accordance with the formula set out in point (b) shall establish the operating efficiency of the separate heat and electricity production that cogeneration is intended to substitute.

The efficiency reference values shall be calculated according to the following principles:

- (i) for cogeneration units the comparison with separate electricity production shall be based on the principle that the same fuel categories are compared;
 - (ii) each cogeneration unit shall be compared with the best available and economically justifiable technology for separate production of heat and electricity on the market in the year of construction of the cogeneration unit;
 - (iii) the efficiency reference values for cogeneration units older than 10 years shall be fixed on the reference values of units of 10 years;
 - (iv) the efficiency reference values for separate electricity production and heat production shall reflect the climatic differences between Member States.
-

ANNEX IV

ENERGY EFFICIENCY REQUIREMENTS FOR PUBLIC PROCUREMENT

In award procedures for public contracts and concessions, contracting authorities and contracting entities that purchase products, services, buildings and works, shall:

- (a) where a product is covered by a delegated act adopted under Regulation (EU) 2017/1369, Directive 2010/30/EU or by a related Commission implementing act, purchase only the products that comply with the criterion laid down in Article 7(2) of that Regulation;
- (b) where a product not covered under point (a) is covered by an implementing measure under Directive 2009/125/EC, purchase only products that comply with energy efficiency benchmarks specified in that implementing measure;
- (c) where a product or a service is covered by the Union green public procurement criteria or available equivalent national criteria, with relevance to energy efficiency of the product or service, make best efforts to purchase only products and services that respect at least the technical specifications set at 'core' level in the relevant Union green public procurement criteria or available equivalent national criteria including among others for data centres, server rooms and cloud services, road lighting and traffic signals, computers, monitors tablets and smartphones;
- (d) purchase only tyres that comply with the criterion of having the highest fuel energy efficiency class, as defined in Regulation (EU) 2020/740, which shall not prevent public bodies from purchasing tyres with the highest wet grip class or external rolling noise class where justified by safety or public health reasons;
- (e) require in their tenders for service contracts that service providers use, for the purposes of providing the services in question, only products that comply with points (a), (b) and (d), when providing the services in question. This requirement shall apply only to new products purchased by service providers partially or wholly for the purpose of providing the service in question;
- (f) purchase, or make new rental agreements for, buildings that comply at least with nearly zero-energy level, without prejudice to Article 6 of this Directive, unless the purpose of the purchase is:
 - (i) to undertake deep renovation or demolition;
 - (ii) in the case of public bodies, to re-sell the building without using it for the public body's own purposes; or
 - (iii) to preserve it as a building officially protected as part of a designated environment, or because of its special architectural or historic merit.

Compliance with the requirements laid down in point (f) of this Annex shall be verified by means of the energy performance certificates referred to in Article 11 of Directive 2010/31/EU.

ANNEX V

COMMON METHODS AND PRINCIPLES FOR CALCULATING THE IMPACT OF ENERGY EFFICIENCY OBLIGATION
SCHEMES OR OTHER POLICY MEASURES UNDER ARTICLES 8, 9 AND 10 AND ARTICLE 30(14)

1. Methods for calculating energy savings other than those arising from taxation measures for the purposes of Articles 8, 9 and 10 and Article 30(14).

Obligated, participating or entrusted parties, or implementing public authorities, may use the following methods for calculating energy savings:

- (a) deemed savings, by reference to the results of previous independently monitored energy improvements in similar installations. The generic approach is termed '*ex ante*';
- (b) metered savings, whereby the savings from the installation of a measure, or package of measures, are determined by recording the actual reduction in energy use, taking due account of factors such as additionality, occupancy, production levels and the weather which may affect consumption. The generic approach is termed '*ex post*';
- (c) scaled savings, whereby engineering estimates of savings are used. This approach may be used only where establishing robust measured data for a specific installation is difficult or disproportionately expensive, for example replacing a compressor or electric motor with a different kWh rating from that for which independent information about savings has been measured, or where those estimates are carried out on the basis of nationally established methodologies and benchmarks by qualified or accredited experts that are independent of the obligated, participating or entrusted parties involved;
- (d) when calculating the energy savings for the purpose of Article 8(3) that can be counted to fulfil the obligation in that Article, Member States may estimate the energy savings of people affected by energy poverty, vulnerable customers, people in low-income households and, where applicable, people living in social housing on the basis of engineering estimates using standardised occupancy and thermal comfort conditions or parameters, such as parameters defined in national building regulations. The way comfort is considered for actions in buildings should be reported by the Member States to the Commission together with explanations of their calculation methodology.
- (e) surveyed savings, where consumers' response to advice, information campaigns, labelling or certification schemes or smart metering is determined. This approach shall be used only for savings resulting from changes in consumer behaviour. It shall not be used for savings resulting from the installation of physical measures.

2. In determining the energy savings for an energy efficiency measure for the purposes of Articles 8, 9 and 10 and Article 30(14), the following principles apply:

- (a) Member States shall demonstrate that one of the objectives of the policy measure, whether new or existing, is the achievement of end-use energy savings pursuant to Article 8(1) and shall provide evidence and their documentation showing that the energy savings are caused by a policy measure, including voluntary agreements;
- (b) the savings shall be shown to be additional to those that would have occurred in any event without the activity of the obligated, participating or entrusted parties, or implementing public authorities. To determine the savings that can be claimed as additional, Member States shall have regard to how energy use and demand would evolve in the absence of the policy measure in question by taking into account at least the following factors: energy consumption trends, changes in consumer behaviour, technological progress and changes caused by other measures implemented at Union and national level;

- (c) savings resulting from the implementation of mandatory Union law shall be considered to be savings that would have occurred in any event, and thus shall not be claimed as energy savings for the purpose of Article 8(1). By way of derogation from that requirement, savings related to the renovation of existing buildings, including the savings resulting from the implementation of minimum energy performance standards in buildings in accordance with Directive 2010/31/EU, may be claimed as energy savings for the purpose of Article 8(1), provided that the materiality criterion referred to in point 3(h) of this Annex is ensured. Measures promoting energy efficiency improvements in the public sector pursuant to Article 5 and Article 6 may be eligible to be taken into account for the fulfilment of energy savings required under Article 8(1), provided that they result in verifiable and measurable or estimable end-use energy savings. The calculation of energy savings shall comply with this Annex;
- (d) end-use energy savings resulting from the implementation of energy efficiency improvement measures taken pursuant to emergency regulations under Article 122 TFEU may be claimed for the purpose of Article 8(1), provided that they result in verifiable and measurable or estimable end-use energy savings, with the exception of those energy savings resulting from rationing or curtailment measures;
- (e) measures taken pursuant to Regulation (EU) 2018/842 can be considered material, but Member States have to show that they result in verifiable and measurable or estimable end-use energy savings. The calculation of energy savings shall comply with this Annex;
- (f) Member States shall count only end use energy savings from policy measures in sectors or installations covered by Chapter IVa of Directive 2003/87/EC if they result from the implementation of Article 9 or 10 of this Directive and which go beyond the requirements laid down in Directive 2003/87/EC or beyond the implementation of actions linked to the allocation of free allowances under that Directive. Member States shall demonstrate that the policy measures result in verifiable and measurable or estimable end-use energy savings. The calculation of energy savings shall comply with this Annex. If an entity is an obligated party under a national energy efficiency obligation scheme under Article 9 of this Directive and under the EU ETS for buildings and road transport under Chapter IVa of Directive 2003/87/EC, the monitoring and verification system shall ensure that the carbon price passed through when releasing fuel for consumption under that Chapter is taken into account when calculating and reporting the energy savings of its energy saving measures;
- (g) credit may be given, provided that it is only given for savings exceeding the following levels:
 - (i) Union emission performance standards for new passenger cars and new light commercial vehicles following the implementation of Regulation (EU) 2019/631 of the European Parliament and of the Council ⁽¹⁾; Member States must provide reasons, their assumptions and their calculation methodology to show additionality to the Union's new vehicle CO₂ requirements;
 - (ii) Union requirements relating to the removal from the market of certain energy related products following the implementation of implementing measures under Directive 2009/125/EC. Member States shall provide evidence, their assumptions and their calculation methodology to show additionality;
- (h) policies with the purpose of encouraging higher levels of energy efficiency of products, equipment, transport systems, vehicles and fuels, buildings and building elements, processes or markets shall be permitted, except for policy measures:
 - (i) regarding the use of direct combustion of fossil fuel technologies that are newly implemented as from 1 January 2026; and
 - (ii) subsidising the use of direct combustion of fossil fuel technologies in residential buildings as from 1 January 2026.

⁽¹⁾ Regulation (EU) 2019/631 of the European Parliament and of the Council of 17 April 2019 setting CO₂ emission performance standards for new passenger cars and for new light commercial vehicles, and repealing Regulations (EC) No 443/2009 and (EU) No 510/2011 (OJ L 111, 25.4.2019, p. 13).

- (i) energy savings as a result of policy measures newly implemented as from 1 January 2024 regarding the use of direct fossil fuel combustion in products, equipment, transport systems, vehicles, buildings or works shall not count towards the fulfilment of energy savings obligation pursuant to Article 8(1)(b). In the case of policy measures promoting combinations of technologies, the share of energy savings related to the fossil fuel combustion technology are not eligible as from 1 January 2024.
- (j) by way of derogation from point (i), for the period 1 January 2024 to 31 December 2030, energy savings from direct fossil fuel combustion technologies improving the energy efficiency in energy intense enterprises in the industry sector may be counted as energy savings only for the purpose of Article 8(1), points (b) and (c), until 31 December 2030, provided that:
 - (i) the enterprise has carried out an energy audit pursuant to Article 11(2) and an implementation plan including:
 - an overview of all cost-effective energy efficiency measures with a payback period of five years or less, on the basis of simple pay-back period methodologies provided by the Member State,
 - a timeframe for the implementation of all recommended energy efficiency measures with a payback period of five years or fewer,
 - a calculation of expected energy savings resulting from the energy efficiency measures recommended, and
 - energy efficiency measures related to the use of direct fossil fuel combustion technologies with the relevant information needed for:
 - proving that the measure identified does not increase the amount of energy needed or the capacity of an installation,
 - justifying that the uptake of sustainable, non-fossil fuel technologies is technically not feasible,
 - showing that the direct fossil fuel combustion technology complies with the most up-to-date corresponding Union emission performance legislation and prevents technology lock-in effects by ensuring future compatibility with climate-neutral alternative non-fossil fuels and technologies.
 - (ii) the continuation of the use of direct fossil fuel technologies is an energy efficiency measure to decrease energy consumption with a payback period of five years or less, on the basis of simple pay-back period methodologies provided by the Member State, recommended as result of an energy audit pursuant to Article 11(2) and included in the implementation plan;
 - (iii) the use of direct fossil fuel technologies complies with the most up-to-date corresponding Union emission performance legislation, does not lead to technology lock-in effects and ensures future compatibility with climate-neutral alternative fuels and technologies;
 - (iv) the use of direct fossil fuel technologies in the enterprise does not lead to an increased energy consumption or increase the capacity of the installation in that enterprise;
 - (v) evidence is provided that no alternative, sustainable non-fossil fuel solution was technically feasible;
 - (vi) the use of direct fossil fuel technologies result in verifiable and measurable or estimable end-use energy savings calculated in accordance with this Annex;
 - (vii) evidence is published on a website or is made publicly available for all interested citizens;

- (k) measures promoting the installation of small-scale renewable energy technologies on or in buildings may be eligible to be taken into account for the fulfilment of energy savings required under Article 8(1), provided that they result in verifiable and measurable or estimable end-use energy savings. The calculation of energy savings shall comply with this Annex;
 - (l) measures promoting the installation of solar thermal technologies may be eligible to be taken into account for the fulfilment of energy savings required under Article 8(1) provided that they result in verifiable and measurable or estimable end-use energy savings. The heat produced by solar thermal technologies from solar radiation can be excluded from their end-use energy consumption;
 - (m) for policies that accelerate the uptake of more efficient products and vehicles, except those newly implemented as from 1 January 2024 regarding the use of direct fossil fuel combustion, full credit may be claimed, provided that it is shown that such uptake takes place before the expiry of the average expected lifetime of the product or vehicle, or before the product or vehicle would usually be replaced, and the savings are claimed only for the period until the end of the average expected lifetime of the product or vehicle to be replaced;
 - (n) in promoting the uptake of energy efficiency measures, Member States shall, where relevant, ensure that quality standards for products, services and installation of measures are maintained or introduced where such standards do not exist;
 - (o) to account for climatic variations between regions, Member States may choose to adjust the savings to a standard value or to accord different energy savings in accordance with temperature variations between regions;
 - (p) the calculation of energy savings shall take into account the lifetime of the measures and the rate at which the savings decline over time. That calculation shall count the savings each individual action will achieve during the period from its date of implementation to the end of each obligation period. Alternatively, Member States may adopt another method that is estimated to achieve at least the same total quantity of savings. When using another method, Member States shall ensure that the total amount of energy savings calculated using that method does not exceed the amount of energy savings that would have been the result of their calculation when counting the savings each individual action will achieve during the period from its date of implementation to 2030. Member States shall describe in detail in their integrated national energy and climate plans notified pursuant to Article 3 and Articles 7 to 12 of Regulation (EU) 2018/1999 that other method and the provisions made to ensure that the binding calculation requirement is met.
3. Member States shall ensure that the following requirements for policy measures taken pursuant to Article 10 and Article 30(14) are met:
- (a) policy measures and individual actions produce verifiable end-use energy savings;
 - (b) the responsibility of each participating party, entrusted party or implementing public authority, as relevant, is clearly defined;
 - (c) the energy savings that are achieved or are to be achieved are determined in a transparent manner;
 - (d) the amount of energy savings required or to be achieved by the policy measure is expressed in either primary energy consumption or final energy consumption, using the net calorific values or primary energy factors referred to in Article 31;
 - (e) an annual report on the energy savings achieved by entrusted parties, participating parties and implementing public authorities be provided and made publicly available, as well as data on the annual trend of energy savings;
 - (f) monitoring of the results and taking appropriate measures if progress is not satisfactory;
 - (g) the energy savings from an individual action are not claimed by more than one party;

- (h) the activities of the participating party, entrusted party or implementing public authority are shown to be material to the achievement of the energy savings claimed;
- (i) the activities of the participating party, entrusted party or implementing public authority have no adverse effects on people affected by energy poverty, vulnerable customers and, where applicable, people living in social housing.

4. In determining the energy savings from taxation-related policy measures introduced under Article 10, the following principles shall apply:

- (a) credit shall be given only for energy savings from taxation measures exceeding the minimum levels of taxation applicable to fuels as required in Council Directive 2003/96/EC ⁽²⁾ or 2006/112/EC ⁽³⁾;
- (b) short-run price elasticities for the calculation of the impact of the energy taxation measures shall represent the responsiveness of energy demand to price changes, and shall be estimated on the basis of recent and representative official data sources, which are applicable for the Member State, and, where applicable, on the basis of accompanying studies from an independent institute. If a different price elasticity than short-run elasticities is used, Member States shall explain how energy efficiency improvements due to the implementation of other Union legislation have been included in the baseline used to estimate the energy savings, or how a double-counting of energy savings from other Union legislation has been avoided;
- (c) the energy savings from accompanying taxation policy instruments, including fiscal incentives or payment to a fund, shall be accounted separately;
- (d) short-run elasticity estimates should be used to assess the energy savings from taxation measures to avoid overlap with Union law and other policy measures;
- (e) Member States shall determine distributional effects of taxation and equivalent measures on people affected by energy poverty, vulnerable customers and, where applicable, people living in social housing, and show the effects of the mitigation measures implemented in accordance with Article 24(1), (2) and (3);
- (f) Member States shall provide evidence, including calculation methodologies, that where there is an overlap in the impact of energy or carbon taxation measures or emissions trading in accordance with Directive 2003/87/EC, there is no double counting of energy savings.

5. Notification of methodology

Member States shall, in accordance with Regulation (EU) 2018/1999, notify to the Commission their proposed detailed methodology for the operation of the energy efficiency obligation schemes and alternative measures referred to in Articles 9 and 10, and Article 30(14) of this Directive. Except in the case of taxation, such notification shall include information on:

- (a) the level of the energy savings required under Article 8(1), first subparagraph, or savings expected to be achieved over the whole period from 1 January 2021 to 31 December 2030;
- (b) how the calculated quantity of new energy savings required under Article 8(1), first subparagraph, or energy savings expected to be achieved will be phased over the obligation period;
- (c) the obligated, participating or entrusted parties, or implementing public authorities;
- (d) target sectors;
- (e) policy measures and individual actions, including the expected total amount of cumulative energy savings for each measure;

⁽²⁾ Council Directive 2003/96/EC of 27 October 2003 restructuring the Community framework for the taxation of energy products and electricity (OJ L 283, 31.10.2003, p. 51).

⁽³⁾ Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax (OJ L 347, 11.12.2006, p. 1).

- (f) policy measures or programmes or measures financed under a national energy efficiency fund implemented as a priority among people affected by energy poverty, vulnerable customers and, where applicable, people living in social housing;
 - (g) the share and the amount of energy savings to be achieved among people affected by energy poverty, vulnerable customers and, where applicable, people living in social housing;
 - (h) where applicable, the indicators applied, the arithmetic average share and the outcome of policy measures established pursuant to Article 8(3);
 - (i) where applicable, impacts and adverse effects of policy measures implemented pursuant to Article 8(3) on people affected by energy poverty, vulnerable customers and, where applicable, people living in social housing;
 - (j) the duration of the obligation period for the energy efficiency obligation scheme;
 - (k) where applicable, the amount of energy savings or cost reduction targets to be achieved by obligated parties among people affected by energy poverty, vulnerable customers and, where applicable, people living in social housing;
 - (l) the actions provided for by the policy measure;
 - (m) the calculation methodology, including how additionality and materiality have been determined and which methodologies and benchmarks are used for deemed and scaled savings, and, where applicable, the net calorific values and conversion factors used;
 - (n) the lifetimes of measures, and how they are calculated or what they are based upon;
 - (o) the approach taken to address climatic variations within the Member State;
 - (p) the monitoring and verification systems for measures under Articles 9 and 10 and how their independence from the obligated, participating or entrusted parties is ensured;
 - (q) in the case of taxation:
 - (i) the target sectors and segment of taxpayers;
 - (ii) the implementing public authority;
 - (iii) the savings expected to be achieved;
 - (iv) the duration of the taxation measure;
 - (v) the calculation methodology, including the price elasticities used and how they have been established and
 - (vi) how overlaps with EU ETS in accordance with Directive 2003/87/EC have been avoided and the risk of double counting has been abolished.
-

ANNEX VI

MINIMUM CRITERIA FOR ENERGY AUDITS INCLUDING THOSE CARRIED OUT AS PART OF ENERGY MANAGEMENT SYSTEMS

The energy audits referred to in Article 11 shall:

- (a) be based on up-to-date, measured, traceable operational data on energy consumption and (for electricity) load profiles;
- (b) comprise a detailed review of the energy consumption profile of buildings or groups of buildings, industrial operations or installations, including transportation;
- (c) identify energy efficiency measures to decrease energy consumption;
- (d) identify the potential for cost-effective use or production of renewable energy;
- (e) build, whenever possible, on life-cycle cost analysis instead of simple payback periods in order to take account of long-term savings, residual values of long-term investments and discount rates;
- (f) be proportionate, and sufficiently representative to permit the drawing of a reliable picture of overall energy performance and the reliable identification of the most significant opportunities for improvement.

Energy audits shall allow detailed and validated calculations for the proposed measures so as to provide clear information on potential savings.

The data used in energy audits shall be storable for historical analysis and tracking performance.

ANNEX VII

MINIMUM REQUIREMENTS FOR MONITORING AND PUBLISHING THE ENERGY PERFORMANCE OF DATA CENTRES

The following minimum information shall be monitored and published with regard to the energy performance of data centres referred to in Article 12:

- (a) the name of the data centre, the name of the owner and operators of the data centre, the date on which the data centre started its operations and the municipality where the data centre is based;
 - (b) the floor area of the data centre, the installed power, the annual incoming and outgoing data traffic, and the amount of data stored and processed within the data centre;
 - (c) the performance, during the last full calendar year, of the data centre in accordance with key performance indicators about, inter alia, energy consumption, power utilisation, temperature set points, waste heat utilisation, water usage and use of renewable energy, using as a basis, where applicable, the CEN/CENELEC EN 50600-4 'Information technology – Data centre facilities and infrastructures', until the entry into force of the delegated act adopted pursuant to Article 33(3).
-

ANNEX VIII

MINIMUM REQUIREMENTS FOR BILLING AND BILLING INFORMATION BASED ON ACTUAL CONSUMPTION OF NATURAL GAS

1. Minimum requirements for billing

1.1. Billing based on actual consumption

In order to enable final customers to regulate their own energy consumption, billing should take place on the basis of actual consumption at least once a year, and billing information should be made available at least on a quarterly basis, on request or where the consumers have opted to receive electronic billing or else twice a year. Gas used only for cooking purposes may be exempt from this requirement.

1.2. Minimum information contained in the bill

Member States shall ensure that, where appropriate, the following information is made available to final customers in clear and understandable terms in or with their bills, contracts, transactions, and receipts at distribution stations:

- (a) current actual prices and actual consumption of energy;
- (b) comparisons of the final customer's current energy consumption with consumption for the same period in the previous year, preferably in graphic form;
- (c) contact information for final customers' organisations, energy agencies or similar bodies, including website addresses from which information may be obtained on available energy efficiency improvement measures, comparative end-user profiles and objective technical specifications for energy-using equipment.

In addition, wherever possible and useful, Member States shall ensure that comparisons with an average normalised or benchmarked final customer in the same user category are made available to final customers in clear and understandable terms, in, with or signposted to within, their bills, contracts, transactions, and receipts at distribution stations.

1.3. Advice on energy efficiency accompanying bills and other feedback to final customers

When sending contracts and contract changes, and in the bills customers receive or through websites addressing individual customers, energy distributors, distribution system operators and retail energy sales companies shall inform their customers in a clear and understandable manner of contact information for independent consumer advice centres, energy agencies or similar institutions, including their internet addresses, where they can obtain advice on available energy efficiency measures, benchmark profiles for their energy consumption and technical specifications of energy using appliances that can serve to reduce the consumption of those appliances.

ANNEX IX

MINIMUM REQUIREMENTS FOR BILLING AND CONSUMPTION INFORMATION FOR HEATING, COOLING AND DOMESTIC HOT WATER

1. Billing based on actual consumption or heat cost allocator readings

In order to enable final users to regulate their own energy consumption, billing shall take place on the basis of actual consumption or heat cost allocator readings at least once per year.

2. Minimum frequency of billing or consumption information

Until 31 December 2021, where remotely readable meters or heat cost allocators have been installed, billing or consumption information based on actual consumption or heat cost allocator readings shall be provided to final users at least on a quarterly basis upon request or where final customers have opted to receive electronic billing, or else twice a year.

From 1 January 2022, where remotely readable meters or heat cost allocators have been installed, billing or consumption information based on actual consumption or heat cost allocator readings shall be provided to final users at least on a monthly basis. It may also be made available via the internet and be updated as frequently as allowed by the measurement devices and systems used. Heating and cooling may be exempted from that requirement outside the heating or cooling seasons.

3. Minimum information contained in the bill

Member States shall ensure that the following information is made available to final users in clear and comprehensible terms in or with their bills where those are based on actual consumption or heat cost allocator readings:

- (a) current actual prices and actual consumption of energy or total heat cost and heat cost allocator readings;
- (b) the fuel mix used and the related annual GHG emissions, including for final users supplied by district heating or district cooling, and a description of the different taxes, levies and tariffs applied;
- (c) comparisons of the final users' current energy consumption with consumption for the same period in the previous year, in graphic form and climate corrected for heating and cooling;
- (d) contact information for final customers' organisations, energy agencies or similar bodies, including website addresses, from which information on available energy efficiency improvement measures, comparative end-user profiles and objective technical specifications for energy-using equipment may be obtained;
- (e) information about related complaints procedures, ombudsman services or alternative dispute resolution mechanisms, as applicable in the Member States;
- (f) comparisons with an average normalised or benchmarked final user in the same user category. In the case of electronic bills, such comparisons may instead be made available online and signposted to within the bills.

Member States may limit the scope of the requirement to provide information about GHG emissions pursuant to point (b) of the first subparagraph to include only supplies from district heating systems with a total rated thermal input exceeding 20 MW.

Bills that are not based on actual consumption or heat cost allocator readings shall contain a clear and comprehensible explanation of how the amount set out in the bill was calculated, and at least the information referred to in points (d) and (e).

ANNEX X

POTENTIAL FOR EFFICIENCY IN HEATING AND COOLING

The comprehensive assessment of national heating and cooling potentials referred to in Article 25(1) shall include and shall be based on the following:

Part I

OVERVIEW OF HEATING AND COOLING

1. heating and cooling demand in terms of assessed useful energy ⁽¹⁾ and quantified final energy consumption in GWh per year ⁽²⁾ by sector:
 - (a) residential;
 - (b) services;
 - (c) industry;
 - (d) any other sector that individually consumes more than 5 % of total national useful heating and cooling demand;
2. the identification, or, in the case of point (a)(i), the identification or estimation, of current heating and cooling supply:
 - (a) by technology, in GWh per year ⁽³⁾, within the sectors referred to in point 1 where possible, distinguishing between energy derived from fossil and renewable sources:
 - (i) provided on-site in residential and service sites by:
 - heat only boilers;
 - high-efficiency heat and power cogeneration;
 - heat pumps;
 - other on-site technologies and sources;
 - (ii) provided on-site in non-service and non-residential sites by:
 - heat only boilers;
 - high-efficiency heat and power cogeneration;
 - heat pumps;
 - other on-site technologies and sources;
 - (iii) provided off-site by:
 - high-efficiency heat and power cogeneration;
 - waste heat;
 - other off-site technologies and sources;
 - (b) the identification of installations that generate waste heat or cold and their potential heating or cooling supply, in GWh per year:
 - (i) thermal power generation installations that can supply or can be retrofitted to supply waste heat with a total thermal input exceeding 50 MW;
 - (ii) heat and power cogeneration installations using technologies referred to in Part II of Annex II with a total thermal input exceeding 20 MW;
 - (iii) waste incineration plants;

⁽¹⁾ The amount of thermal energy needed to satisfy the heating and cooling demand of end-users.

⁽²⁾ The most recent data available should be used.

⁽³⁾ The most recent data available should be used.

- (iv) renewable energy installations with a total thermal input exceeding 20 MW other than the installations specified under points (i) and (ii) generating heating or cooling using the energy from renewable sources;
 - (v) industrial installations with a total thermal input exceeding 20 MW which can provide waste heat;
 - (c) reported share of energy from renewable sources and from waste heat or cold in the final energy consumption of the district heating and cooling ⁽⁴⁾ sector over the past 5 years, in accordance with Directive (EU) 2018/2001;
3. aggregated data on cogeneration units in existing district heating and cooling networks in five capacity ranges covering:
- (a) primary energy consumption;
 - (b) overall efficiency;
 - (c) primary energy savings;
 - (d) CO₂ emission factors;
4. aggregated data on existing district heating and cooling networks supplied from cogeneration in five capacity ranges covering:
- (a) overall primary energy consumption;
 - (b) primary energy consumption of cogeneration units;
 - (c) share of cogeneration in district heating or cooling supply;
 - (d) district heating system losses;
 - (e) district cooling system losses;
 - (f) connection density;
 - (g) shares of systems per different operating temperature groups;
5. a map covering the entire national territory, which, while preserving commercially sensitive information, identifies:
- (a) heating and cooling demand areas following from the analysis of point 1, while using consistent criteria for focusing on energy dense areas in municipalities and conurbations;
 - (b) existing heating and cooling supply points identified under point 2(b) and district heating transmission installations;
 - (c) planned heating and cooling supply points of the type described under point 2(b) and identified new areas for the district heating and cooling;
6. a forecast of trends in the demand for heating and cooling to maintain a perspective of the next 30 years in GWh and taking into account, in particular, projections for the next 10 years, the change in demand in buildings and different sectors of the industry, and the impact of policies and strategies related to the demand management, such as long-term building renovation strategies under Directive (EU) 2018/844 of the European Parliament and of the Council ⁽⁵⁾;

⁽⁴⁾ The identification of 'renewable cooling' shall, after the methodology for calculating the quantity of renewable energy used for cooling and district cooling is established in accordance with Article 35 of Directive (EU) 2018/2001, be carried out in accordance with that Directive. Until then it shall be carried out according to an appropriate national methodology.

⁽⁵⁾ Directive (EU) 2018/844 of the European Parliament and of the Council of 30 May 2018 amending Directive 2010/31/EU on the energy performance of buildings and Directive 2012/27/EU on energy efficiency (OJ L 156, 19.6.2018, p. 75).

Part II

OBJECTIVES, STRATEGIES AND POLICY MEASURES

7. planned contribution of the Member State to its national objectives, targets and contributions for the five dimensions of the Energy Union, as laid out in Article 3(2), point (b), of Regulation (EU) 2018/1999, delivered through efficiency in heating and cooling, in particular related to Article 4, point (b), points 1 to 4 and to Article 15 (4), point (b) of that Regulation, identifying which of those elements is additional compared to the integrated national energy and climate plan notified pursuant to Article 3 and Articles 7 to 12 of that Regulation;
8. a general overview of the existing policies and measures as described in the most recent report submitted in accordance with Articles 3, 20 and 21 and Article 27(a) of Regulation (EU) 2018/1999;

Part III

ANALYSIS OF THE ECONOMIC POTENTIAL FOR EFFICIENCY IN HEATING AND COOLING

9. an analysis of the economic potential ⁽⁶⁾ of different technologies for heating and cooling shall be carried out for the entire national territory by using the cost-benefit analysis referred to in Article 25(3) and shall identify alternative scenarios for more efficient and renewable heating and cooling technologies, distinguishing between energy derived from fossil and renewable sources where applicable.

The following technologies should be considered:

- (a) industrial waste heat and cold;
- (b) waste incineration;
- (c) high efficiency cogeneration;
- (d) renewable energy sources, such as geothermal, solar thermal and biomass, other than those used for high efficiency cogeneration;
- (e) heat pumps;
- (f) reducing heat and cold losses from existing district networks;
- (g) district heating and cooling;

10. the analysis of economic potential shall include the following steps and considerations:

- (a) Considerations:
 - (i) the cost-benefit analysis for the purposes of Article 25(3) shall include an economic analysis that takes into consideration socioeconomic and environmental factors ⁽⁷⁾, and a financial analysis performed to assess projects from the investors' point of view, both economic and financial analyses using the net present value as a criterion for the assessment;
 - (ii) the baseline scenario should serve as a reference point and take into account existing policies at the time of compiling this comprehensive assessment ⁽⁸⁾, and be linked to data collected under Part I and Part II, point 6 of this Annex;

⁽⁶⁾ The analysis of the economic potential should present the volume of energy (in GWh) that can be generated per year by each technology analysed. The limitations and interrelations within the energy system should also be taken into account. The analysis may make use of models based on assumptions representing the operation of common types of technologies or systems.

⁽⁷⁾ Including the assessment referred to in Article 15 (7) of Directive (EU) 2018/2001.

⁽⁸⁾ The cut-off date for taking into account policies for the baseline scenario is the end of the year preceding to the year by the end of which the comprehensive assessment is due. That is to say, policies enacted within a year prior to the deadline for submission of the comprehensive assessment do not need to be taken into account.

(iii) alternative scenarios to the baseline shall take into account energy efficiency and the renewable energy objectives of Regulation (EU) 2018/1999, each scenario presenting the following elements compared to the baseline scenario:

- economic potential of technologies examined using the net present value as criterion;
- GHG emission reductions;
- primary energy savings in GWh per year;
- impact on the share of renewables in the national energy mix.

Scenarios that are not feasible due to technical reasons, financial reasons or national regulation may be excluded at an early stage of the cost-benefit analysis, if justified on the basis of careful, explicit and well-documented considerations.

The assessment and decision-making should take into account costs and energy savings from the increased flexibility in energy supply and from a more optimal operation of the electricity networks, including avoided costs and savings from reduced infrastructure investment, in the analysed scenarios.

(b) Costs and benefits

The costs and benefits referred to in point (a) shall include at least the following costs and benefits:

(i) costs:

- capital costs of plants and equipment;
- capital costs of the associated energy networks;
- variable and fixed operating costs;
- energy costs;
- environmental, health and safety costs, to the extent possible;
- labour market costs, energy security and competitiveness, to the extent possible.

(ii) benefits:

- value of output to the consumer (heating, cooling and electricity);
- external benefits such as environmental, greenhouse gas emissions and health and safety benefits, to the extent possible;
- labour market effects, energy security and competitiveness, to the extent possible.

(c) Relevant scenarios to the baseline:

All relevant scenarios to the baseline shall be considered, including the role of efficient individual heating and cooling. The cost-benefit analysis may cover either a project assessment or a group of projects for a broader local, regional or national assessment in order to establish the most cost-effective and beneficial heating or cooling solution against a baseline for a given geographical area for the purpose of planning.

(d) Boundaries and integrated approach:

- (i) the geographical boundary shall cover a suitable, well-defined geographical area;
- (ii) the cost-benefit analyses shall take into account all relevant centralised or decentralised supply resources available within the system and geographical boundary, including technologies considered under Part III, point 9, of this Annex, and heating and cooling demand trends and characteristics.

(e) Assumptions:

- (i) Member States shall provide assumptions, for the purpose of the cost-benefit analyses, on the prices of major input and output factors and the discount rate;

- (ii) the discount rate used in the economic analysis to calculate net present value shall be chosen according to European or national guidelines;
- (iii) Member States shall use national, European or international energy price development forecasts, if appropriate, in their national, regional or local context;
- (iv) the prices used in the economic analysis shall reflect socio-economic costs and benefits. External costs, such as environmental and health effects, should be included to the extent possible, namely when a market price exists or when it is already included in European or national regulation.
- (f) Sensitivity analysis: a sensitivity analysis shall be included to assess the costs and benefits of a project or group of projects and be based on variable factors having a significant impact on the outcome of the calculations, such as different energy prices, levels of demand, discount rates and other.

Part IV

POTENTIAL NEW STRATEGIES AND POLICY MEASURES

11. an overview of new legislative and non-legislative policy measures ⁽⁹⁾ to realise the economic potential identified in accordance with points 9 and 10, together with a forecast of:
 - (a) greenhouse gas emission reductions;
 - (b) primary energy savings in GWh per year;
 - (c) impact on the share of high-efficiency cogeneration;
 - (d) impact on the share of renewables in the national energy mix and in the heating and cooling sector;
 - (e) links to national financial programming and cost savings for the public budget and market participants;
 - (f) estimated public support measures, if any, with their annual budget and identification of the potential aid element.

⁽⁹⁾ This overview shall include financing measures and programmes that may be adopted over the period of the comprehensive assessment, not prejudging a separate notification of the public support schemes for a State aid assessment.

ANNEX XI

COST-BENEFIT ANALYSES

Cost-benefit analyses shall provide information for the purpose of the measures referred to in Article 25(3) and Article 26(7):

If an electricity-only installation or an installation without heat recovery is planned, a comparison shall be made between the planned installations or the planned refurbishment and an equivalent installation producing the same amount of electricity or process heat, but recovering the waste heat and supplying heat through high-efficiency cogeneration or district heating and cooling networks, or both.

Within a given geographical boundary the assessment shall take into account the planned installation and any appropriate existing or potential heat or cooling demand points that could be supplied from it, taking into account rational possibilities, for example, technical feasibility and distance.

The system boundary shall be set to include the planned installation and the heat and cooling loads, such as building(s) and industrial process. Within this system boundary the total cost of providing heat and power shall be determined for both cases and compared.

Heat or cooling loads shall include existing heat or cooling loads, such as an industrial installation or an existing district heating or cooling system, and also, in urban areas, the heat or cooling load and costs that would exist if a group of buildings or part of a city were provided with or connected into a new district heating or cooling network, or both.

Cost-benefit analyses shall be based on a description of the planned installation and the comparison installation(s), covering electrical and thermal capacity, as applicable, fuel type, planned usage and the number of planned operating hours every year, location and electricity and thermal demand.

An assessment of waste heat utilisation shall take into consideration current technologies. The assessment shall take into consideration the direct use of waste heat or its upgrading to higher temperature levels, or both. In the case of waste heat recovery on-site, at least the use of heat exchangers, heat pumps, and heat to power technologies shall be assessed. In the case of waste heat recovery off-site, at least industrial installations, agriculture sites and district heating networks shall be assessed as potential demand points.

For the purpose of the comparison, the thermal energy demand and the types of heating and cooling used by the nearby heat or cooling demand points shall be taken into account. The comparison shall cover infrastructure related costs for the planned and comparison installation.

Cost-benefit analyses for the purposes of Article 26(7) shall include an economic analysis covering a financial analysis reflecting actual cash flow transactions from investing in and operating individual installations.

Projects with positive cost-benefit outcome are those where the sum of discounted benefits in the economic and financial analysis exceeds the sum of discounted costs (cost-benefit surplus).

Member States shall set guiding principles for the methodology, assumptions and time horizon for the economic analysis.

Member States may require that the companies responsible for the operation of thermal electric generation installations, industrial companies, district heating and cooling networks, or other parties influenced by the defined system boundary and geographical boundary, contribute data for use in assessing the costs and benefits of an individual installation.

ANNEX XII

GUARANTEE OF ORIGIN FOR ELECTRICITY PRODUCED FROM HIGH-EFFICIENCY COGENERATION

- (1) Member States shall take measures to ensure that:
- (a) the guarantee of origin of the electricity produced from high-efficiency cogeneration:
 - enables producers to demonstrate that the electricity they sell is produced from high-efficiency cogeneration and is issued to that effect in response to a request from the producer;
 - is accurate, reliable and fraud-resistant;
 - is issued, transferred and cancelled electronically;
 - (b) the same unit of energy from high-efficiency cogeneration is taken into account only once.
- (2) The guarantee of origin referred to in Article 26(13) shall contain at least the following information:
- (a) the identity, location, type and capacity (thermal and electrical) of the installation where the energy was produced;
 - (b) the dates and places of production;
 - (c) the lower calorific value of the fuel source from which the electricity was produced;
 - (d) the quantity and the use of the heat generated together with the electricity;
 - (e) the quantity of electricity from high-efficiency cogeneration in accordance with Annex III that the guarantee of origin represents;
 - (f) the primary energy savings calculated in accordance with Annex III on the basis of the harmonised efficiency reference values indicated in Annex III, point (d);
 - (g) the nominal electric and thermal efficiency of the plant;
 - (h) whether and to what extent the installation has benefited from investment support;
 - (i) whether and to what extent the unit of energy has benefited in any other way from a national support scheme, and the type of support scheme;
 - (j) the date on which the installation became operational; and
 - (k) the date and country of issue and a unique identification number.

The guarantee of origin shall be of the standard size of 1 MWh. It shall relate to the net electricity output measured at the station boundary and exported to the grid.

ANNEX XIII

ENERGY EFFICIENCY CRITERIA FOR ENERGY NETWORK REGULATION AND FOR ELECTRICITY NETWORK TARIFFS

1. Network tariffs shall be transparent and non-discriminatory, and shall comply with Article 18 of Regulation (EU) 2019/943 and be cost-reflective of cost-savings in networks achieved from demand-side and demand- response measures and distributed generation, including savings from lowering the cost of delivery or of network investment and a more optimal operation of the network.
 2. Network regulation and tariffs shall not prevent network operators or energy retailers making available system services for demand response measures, demand management and distributed generation on organised electricity markets, including over-the-counter markets and electricity exchanges for trading energy, capacity, balancing and ancillary services in all timeframes, including forward, day-ahead and intra-day markets, in particular:
 - (a) the shifting of the load from peak to off-peak times by final customers taking into account the availability of renewable energy, energy from cogeneration and distributed generation;
 - (b) energy savings from demand response of distributed consumers by independent aggregators;
 - (c) demand reduction from energy efficiency measures undertaken by energy service providers, including ESCOs;
 - (d) the connection and dispatch of generation sources at lower voltage levels;
 - (e) the connection of generation sources from closer location to the consumption; and
 - (f) the storage of energy.
 3. Network or retail tariffs may support dynamic pricing for demand response measures by final customers, such as:
 - (a) time-of-use tariffs;
 - (b) critical peak pricing;
 - (c) real time pricing; and
 - (d) peak time rebates.
-

ANNEX XIV

ENERGY EFFICIENCY REQUIREMENTS FOR TRANSMISSION SYSTEM OPERATORS AND DISTRIBUTION SYSTEM OPERATORS

Transmission system operators and distribution system operators shall:

- (a) set up and make public their standard rules relating to the bearing and sharing of costs of technical adaptations, such as grid connections, grid reinforcements and the introduction of new grids, improved operation of the grid and rules on the non-discriminatory implementation of the grid codes, which are necessary in order to integrate new producers feeding electricity produced from high-efficiency cogeneration into the interconnected grid;
- (b) provide any new producer of electricity produced from high-efficiency cogeneration wishing to be connected to the system with the comprehensive and necessary information required, including:
 - (i) a comprehensive and detailed estimate of the costs associated with the connection;
 - (ii) a reasonable and precise timetable for receiving and processing the request for grid connection;
 - (iii) a reasonable indicative timetable for any proposed grid connection. The overall process to become connected to the grid should be no longer than 24 months, bearing in mind what is reasonably practicable and non-discriminatory;
- (c) provide standardised and simplified procedures for the connection of distributed high-efficiency cogeneration producers to facilitate their connection to the grid.

The standard rules referred to in point (a) of the first paragraph shall be based on objective, transparent and non-discriminatory criteria taking particular account of all the costs and benefits associated with the connection of those producers to the grid. They may provide for different types of connection.

ANNEX XV

MINIMUM ITEMS TO BE INCLUDED IN ENERGY PERFORMANCE CONTRACTS OR IN THE ASSOCIATED TENDER SPECIFICATIONS

- Findings and recommendations set out in analyses and energy audits carried out before the contract has been concluded that cover energy use of the building with a view to implementing energy efficiency improvement measures.
 - A clear and transparent list of the efficiency measures to be implemented or the efficiency results to be obtained.
 - Guaranteed savings to be achieved by implementing the measures of the contract.
 - The duration and milestones of the contract, terms and period of notice.
 - A clear and transparent list of the obligations of each contracting party.
 - Reference date(s) to establish achieved savings.
 - A clear and transparent list of steps to be performed to implement a measure or package of measures and, where relevant, associated costs.
 - An obligation to fully implement the measures in the contract and documentation of all changes made during the project.
 - Regulations specifying the inclusion of equivalent requirements in any subcontracting with third parties.
 - A clear and transparent display of the financial implications of the project and the distribution of the share of both parties in the monetary savings achieved, namely the remuneration of the service provider.
 - A clear and transparent provisions on measurement and verification of the guaranteed savings achieved, quality checks and guarantees.
 - Provisions clarifying the procedure to deal with changing framework conditions that affect the content and the outcome of the contract, namely changing energy prices and the use intensity of an installation.
 - Detailed information on the obligations of each contracting party and of the penalties for their breach.
-

ANNEX XVI

Part A

Repealed Directive with list of the successive amendments thereto (referred to in Article 39)

Directive 2012/27/EU of the European Parliament and of the Council
(OJ L 315, 14.11.2012, p. 1)

Council Directive 2013/12/EU
(OJ L 141, 28.5.2013, p. 28)

Directive (EU) 2018/844 of the European Parliament and of the Council
(OJ L 156, 19.6.2018, p. 75) only Article 2

Directive (EU) 2018/2002 of the European Parliament and of the Council
(OJ L 328, 21.12.2018, p. 210)

Regulation (EU) 2018/1999 of the European Parliament and of the Council
(OJ L 328, 21.12.2018, p. 1) only Article 54

Decision (EU) 2019/504 of the European Parliament and of the Council
(OJ L 85I, 27.3.2019, p. 66) only Article 1

Commission Delegated Regulation (EU) 2019/826
(OJ L 137, 23.5.2019, p. 3)

Directive (EU) 2019/944 of the European Parliament and of the Council
(OJ L 158, 14.6.2019, p. 125) only Article 70

Part B

Time-limits for transposition into national law (referred to in Article 39)

Directive	Time-limit for transposition
2012/27/EU	5 June 2014
(EU) 2018/844	10 March 2020
(EU) 2018/2002	25 June 2020, with the exception of points 5 to 10 of Article 1 and points 3 and 4 of the Annex 25 October 2020 as regards points 5 to 10 of Article 1 and points 3 and 4 of the Annex
(EU) 2019/944	31 December 2019 as regards point (5)(a) of Article 70 25 October 2020 as regards point (4) of Article 70 31 December 2020 as regards points (1) to (3), (5)(b) and (6) of Article 70

ANNEX XVII

Correlation Table

Directive 2012/27/EU	This Directive
Article 1	Article 1
Article 2, introductory wording	Article 2, introductory wording
Article 2, point 1	Article 2, point 1
-	Article 2, points 2, 3 and 4
Article 2, point 2	Article 2, point 5
Article 2, point 3	Article 2, point 6
-	Article 2, point 7
Article 2, point 4	Article 2, point 8
Article 2, point 5	Article 2, point 9
Article 2, point 6	Article 2, point 10
Article 2, point 7	Article 2, point 11
Article 2, point 8	Article 2, point 12
Article 2, point 9	-
Article 2, point 10	Article 2, point 13
-	Article 2, points 14 and 15
Article 2, point 11	Article 2, point 16
Article 2, point 12	Article 2, point 17
Article 2, point 13	Article 2, point 18
Article 2, point 14	Article 2, point 19
Article 2, point 15	Article 2, point 20
Article 2, point 16	Article 2, point 21
Article 2, point 17	Article 2, point 22
Article 2, point 18	Article 2, point 23
Article 2, point 19	Article 2, point 24
Article 2, point 20	Article 2, point 25
Article 2, point 21	Article 2, point 26
Article 2, point 22	Article 2, point 27
Article 2, point 23	Article 2, point 28
Article 2, point 24	Article 2, point 29
-	Article 2, point 30
-	Article 2, point 31
Article 2, point 25	Article 2, point 32
Article 2, point 26	-
Article 2, point 27	Article 2, point 33
Article 2, point 28	Article 2, point 34
Article 2, point 29	Article 2, point 35

Directive 2012/27/EU	This Directive
Article 2, point 30	Article 2, point 36
Article 2, point 31	Article 2, point 37
Article 2, point 32	Article 2, point 38
Article 2, point 33	Article 2, point 39
Article 2, point 34	Article 2, point 40
Article 2, point 35	Article 2, point 41
Article 2, point 36	Article 2, point 42
Article 2, point 37	Article 2, point 43
Article 2, point 38	Article 2, point 44
Article 2, point 39	Article 2, point 45
Article 2, point 40	-
Article 2, point 41	Article 2, point 46
Article 2, point 42	Article 2, point 47
Article 2, point 43	Article 2, point 48
-	Article 2, point 49
Article 2, point 44	Article 2, point 50
Article 2, point 45	Article 2, point 51
-	Article 2, points 52, 53, 54, 55 and 56
-	Article 3
-	Article 4(1)
Article 3(1), first subparagraph	Article 4(2), first subparagraph Article 4(2), second subparagraph
Article 3(1), second subparagraph, introductory wording	Article 4(3), first subparagraph, introductory wording
Article 3(1), second subparagraph, points (a) and (b)	Article 4(3), first subparagraph, points (a) and (b)
Article 3(1), second subparagraph, point (c)	-
Article 3(1), second subparagraph, point (d)	Article 4(3), first subparagraph, point (c)
Article 3(1), third subparagraph, introductory wording	-
-	Article 4(3), first subparagraph, point (d), introductory wording
-	Article 4(3), first subparagraph, points (d)(i), (ii) and (iii)
Article 3(1), third subparagraph, point (a)	Article 4(3), first subparagraph, point (d)(iv)
-	Article 4(3), first subparagraph, point (e), introductory wording
Article 3(1), third subparagraph, point (b)	Article 4(3), first subparagraph, point (e)(i)

Directive 2012/27/EU	This Directive
Article 3(1), third subparagraph, point (c)	Article 4(3), first subparagraph, point (e)(ii)
Article 3(1), third subparagraph, point (d)	Article 4(3), first subparagraph, point (e)(iii)
Article 3(1), third subparagraph, point (e)	-
-	Article 4(3), first subparagraph, point (e)(iv)
Article 3(2) and (3)	-
Article 3(4)	Article 35(6)
Article 3(5) and (6)	-
-	Article 4(4)
-	Article 4(5)
	Article 4(6)
	Article 4(7)
-	Article 5
Article 5(1), first subparagraph	Article 6(1), first subparagraph
Article 5(1), second subparagraph	Article 6(1), fifth subparagraph
-	Article 6(1), second and third subparagraph
Article 5(1), third subparagraph	Article 6(1), fourth subparagraph
Article 5(1), fourth and fifth subparagraph	-
Article 5(2)	Article 6(2)
-	Article 6(2), second subparagraph
Article 5(3)	Article 6(3)
Article 5(4)	Article 6(4)
Article 5(5)	Article 6(5)
Article 5(5), first subparagraph, point (b)	Article 6(5), second subparagraph, point (c)
-	Article 6(5), second subparagraph, point (b)
Article 5(6)	Article 6(6)
-	Article 6(6), second subparagraph, point (a)
Article 5(6), second subparagraph	Article 6(6), second subparagraph, point (b)
Article 5(6), third subparagraph	Article 6(6), third subparagraph
Article 5(7)	-
Article 6(1), first subparagraph	Article 7(1), first subparagraph
Article 6(1), second subparagraph	Article 7(1), first subparagraph
	Article 7(1), second subparagraph
	-
Article 6(2), (3) and (4)	Article 7(2), (3) and (4)
-	Article 7(5), (6), (7) and (8)
-	
Article 7(1), introductory wording, point (a) and (b)	Article 8(1), introductory wording, point (a) and (b)

Directive 2012/27/EU	This Directive
-	Article 8(1), point (c)
Article 7(1), second subparagraph	Article 8(5)
Article 7(1), third subparagraph	Article 8(1), fifth subparagraph
Article 7(1), fourth subparagraph	Article 8(1), fourth subparagraph
-	Article 8 (3) and (4)
Article 7(2)	Article 8(6)
Article 7(3)	Article 8(7)
Article 7(4)	Article 8(8)
Article 7(5)	Article 8(9)
Article 7(6)	Article 8(10)
Article 7(7)	-
Article 7(8)	-
Article 7(9)	-
Article 7(10)	Article 8(2)
Article 7(11)	-
	Article 8(11), (12) and (13)
Article 7(12)	Article 8(14)
Article 7a (1)	Article 9(1)
Article 7a(2)	Article 9(3)
Article 7a(3)	Article 9(4)
-	Article 9(2)
-	Article 9(5), (6) and (7)
Article 7a (4) and (5)	Article 9(8) and (9)
-	Article 9(10)
Article 7a (6) and (7)	Article 9(11) and (12)
Article 7b (1) and (2)	Article 10(1) and (2)
-	Article 10(3) and (4)
-	Article 11(1) and (2)
-	Article 11(3) and (4)
Article 8(1) and (2)	Article 11(5), (6) and (7)
Article 8(3) and (4)	-
-	Article 11(8)
Article 8(5)	Article 11(9)
-	Article 11(10)
Article 8(6)	Article 11(11)
Article 8(7)	Article 11(12)
-	Article 12

Directive 2012/27/EU	This Directive
Article 9	Article 13
Article 9a	Article 14
Article 9b	Article 15
Article 9c	Article 16
Article 10	Article 17
Article 10a	Article 18
Article 11	Article 19
Article 12	Article 20
-	Article 21
-	Article 22(1)
Article 12(1)	Article 22(2)
Article 12(2), introductory wording and point (a), points (i) to (v)	Article 22(2), second subparagraph, points (a) to (g) Article 22(2), second subparagraph, point (h)
Article 12(2), point (b)	Article 22(3), third subparagraph
-	Article 22(3), third subparagraph, points (a) and (b)
Article 12(2), point (b), points (i) and (ii)	Article 22(3), third subparagraph, points (c) and (d)
-	Article 22(3), third subparagraph, point (e)
-	Article 22 (4) to (9)
-	Article 23
-	Article 24
Article 13	Article 32
Article 14(1)	Article 25(1)
-	Article 25(2)
Article 14(2)	Article 25(5)
Article 14(3)	Article 25(3), first subparagraph
-	Article 25(3), second subparagraph
Article 14(4)	Article 25(4)
-	Article 25(6)
-	Article 26(1), (2), (3), (4), (5) and (6)
Article 14(5), introductory wording and point (a)	Article 26(7), introductory wording and point (a)
Article 14(5), points (b), (c) and (d)	-
-	Article 26(7), points (b), (c) and (d) and second subparagraph
Article 14(5), second and third subparagraphs	Article 26(7), third and fourth subparagraphs
Article 14(6), point (a)	Article 26(8), point (a)

Directive 2012/27/EU	This Directive
Article 14(6), point (b)	-
Article 14(6), point (c)	Article 26(8), point (b)
-	Article 26(8), point (c)
Article 14(6), second and third subparagraphs	Article 26(8), second and third subparagraphs
Article 14(7), (8) and (9)	Article 26(9), (10) and (11)
-	Article 26(12)
Article 14(10) and (11)	Article 26(13) and (14)
Article 15(1), first subparagraph	Article 27(1)
Article 15(1), second and third subparagraphs	-
-	Article 27(2), (3) and (4)
Article 15(1), fourth subparagraph	Article 27(5)
Article 15(2) and (2a)	-
Article 15(3), (4) and (5), first subparagraph	Article 27(6), (7) and (8)
Article 15(5), second subparagraph	-
Article 15(6), first subparagraph	-
Article 15(6), second subparagraph	Article 27(9)
Article 15(7)	Article 27(10)
Article 15(9), first subparagraph	Article 27(11)
Article 15(9), second subparagraph	-
Article 16(1) and (2)	-
-	Article 28(1), (2), (3) and (5)
Article 16(3)	Article 28(4)
Article 17(1), first subparagraph	-
Article 17(1), second subparagraph	Article 30(3)
Article 17(2)	Article 22(7)
Article 17(3)	-
Article 17(4)	-
Article 17(5)	Article 22(10)
Article 18(1), introductory wording	Article 29(1), introductory wording
Article 18(1), point (a), points (i) and (ii)	Article 29(1), points (a) and (b)
-	Article 29(1), points (c) and (d)
Article 18(1), point (b)	Article 29(2)
Article 18(1), point (c)	Article 29(3)
-	Article 29(4)
Article 18(1), point (d), points (i) and (ii)	Article 29(5), points (a) and (b)

Directive 2012/27/EU	This Directive
-	Article 29(5), point (c)
Article 18(2), points (a) and (b)	Article 29(6), points (a) and (b)
Article 18(2), point (c) and (d)	-
-	Article 29(6), point (c)
-	Article 29(7)
Article 18(3)	Article 29(8)
Article 19(1), point (a)	Article 22(5), first subparagraph
Article 19(1), point (b)	Article 7(7), first subparagraph
Article 19(1), second subparagraph	Article 22(9), second subparagraph
Article 19(2)	-
Article 20(1) and (2)	Article 30(1) and (2)
-	Article 30(3), (4), (5),
Article 20(3), (3a), (3b) and (3c)	Article 30(6), (7), (8) and (9)
Article 20(3d)	Article 30(10), first subparagraph
-	Article 30(10), second subparagraph
Article 20(4), (5), (6) and (7)	Article 30(11), (13), (14) and (15)
-	Article 30(12)
-	Article 30(16)
-	Article 30(17) and (18)
Article 21	Article 31(1)
Annex IV, footnote 3	Article 31(2), (3) and (4)
-	Article 31(5)
Annex IV, footnote 3	Article 31(6) and (7)
Article 22(1) and (2)	Article 33(1) and (2)
-	Article 33(3)
Article 23	Article 34
Article 24(4a), (5) and (6)	Article 35(1), (2) and (3)
Article 24(7), (8), (9), (10), (12)	-
Article 24(13) and (14)	Article 35(4) and (5)
Article 24(15), introductory wording	Article 35(7), introductory wording
Article 24(15), point (a)	-
Article 24(15), point (b)	Article 35(7), point (a)
-	Article 35(7), point (b), (c), (d), (e), (f), (g) and (h)
-	Article 35(7), second subparagraph
Article 24(8)	Article 35(7), third subparagraph
Article 25	-
Article 26	-

Directive 2012/27/EU	This Directive
Article 28	Article 36
-	Article 37
Article 27, first paragraph	Article 38, first paragraph
Article 27, second paragraph	-
Article 27, third paragraph	Article 38, second paragraph
Article 28(1), first subparagraph	Article 36(1), first subparagraph
Article 28(1), second subparagraph	-
Article 28(1), third and fourth subparagraphs	Article 36(1), second subparagraph
Article 28(2)	Article 36(2)
Article 29	Article 39
-	Article 39, second paragraph
-	Article 39, third paragraph
Article 30	Article 40
-	Annex I
Annex I	Annex II
Annex II	Annex III
Annex III	Annex IV
Annex IV	-
Annex V	Annex V
Annex VI	Annex VI
-	Annex VII
Annex VII	Annex VIII
Annex VIIa	Annex IX
Annex VIII	Annex X
Annex IX	Annex XI
Annex X	Annex XII
Annex XI	Annex XIII
Annex XII	Annex XIV
Annex XIII	Annex XV
Annex XV	-
-	Annex XVI
-	Annex XVII

II

(Non-legislative acts)

REGULATIONS

COMMISSION IMPLEMENTING REGULATION (EU) 2023/1792

of 13 September 2023

approving Union amendment to the specification for a Protected Designation of Origin or a Protected Geographical Indication ('Ribera del Guadiana' (PDO))

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Commission Delegated Regulation (EU) 2019/33 of 17 October 2018 supplementing Regulation (EU) No 1308/2013 of the European Parliament and of the Council as regards applications for protection of designations of origin, geographical indications and traditional terms in the wine sector, the objection procedure, restrictions of use, amendments to product specifications, cancellation of protection, and labelling and presentation ⁽¹⁾, and in particular Article 15(2) thereof,

Whereas:

- (1) The Commission has examined the application for the approval of Union amendment to the product specification for the Protected Designation of Origin 'Ribera del Guadiana', forwarded by Spain in accordance with Article 105 of Regulation (EU) No 1308/2013 of the European Parliament and of the Council ⁽²⁾ in conjunction with Article 15 of Delegated Regulation (EU) 2019/33.
- (2) The Commission has published the application for the approval of the Union amendment to the product specification in the *Official Journal of the European Union* ⁽³⁾, as required by Article 97(3) of Regulation (EU) No 1308/2013.
- (3) No statement of objection has been received by the Commission under Article 98 of Regulation (EU) No 1308/2013.
- (4) The Union amendment to the product specification should therefore be approved in accordance with Article 99 of Regulation (EU) No 1308/2013 in conjunction with Article 15(2) of Delegated Regulation (EU) 2019/33,

HAS ADOPTED THIS REGULATION:

Article 1

The amendment to the product specification published in the *Official Journal of the European Union* regarding the name 'Ribera del Guadiana' (PDO) are hereby approved.

⁽¹⁾ OJ L 9, 11.1.2019, p. 2.

⁽²⁾ Regulation (EU) No 1308/2013 of the European Parliament and of the Council of 17 December 2013 establishing a common organisation of the markets in agricultural products and repealing Council Regulations (EEC) No 922/72, (EEC) No 234/79, (EC) No 1037/2001 and (EC) No 1234/2007 (OJ L 347, 20.12.2013, p. 671).

⁽³⁾ OJ C 215, 19.6.2023, p. 25.

Article 2

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 13 September 2023.

*For the Commission,
On behalf of the President,
Janusz WOJCIECHOWSKI
Member of the Commission*

DECISIONS

DECISION (EU) 2023/1793 OF THE REPRESENTATIVES OF THE GOVERNMENTS OF THE MEMBER STATES

of 15 September 2023

appointing two Judges to the General Court

THE REPRESENTATIVES OF THE GOVERNMENTS OF THE MEMBER STATES OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Article 19 thereof,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 254 and 255 thereof,

Whereas:

- (1) The terms of office of 23 Judges of the General Court expired on 31 August 2019.
- (2) In that context, Mr Saulius Lukas KALĖDA has been nominated for the post of Judge of the General Court for a term of office ending on 31 August 2025.
- (3) In addition, under Articles 5 and 7 of Protocol No 3 on the Statute of the Court of Justice of the European Union, and following the resignation of Mr Sten FRIMODT NIELSEN, a Judge should be appointed to the General Court for the remainder of Mr Sten FRIMODT NIELSEN's term of office, which runs until 31 August 2028.
- (4) Ms Louise SPANGSBERG GRØNFELDT has been nominated for the vacant post.
- (5) The panel set up under Article 255 of the Treaty on the Functioning of the European Union has given a favourable opinion on the suitability of those candidates to perform the duties of Judge of the General Court,

HAVE ADOPTED THIS DECISION:

Article 1

Mr Saulius Lukas KALĖDA is hereby appointed Judge of the General Court for the period from the date of entry into force of this Decision to 31 August 2025.

Article 2

Ms Louise SPANGSBERG GRØNFELDT is hereby appointed Judge of the General Court for the period from the date of entry into force of this Decision to 31 August 2028.

Article 3

This Decision shall enter into force on the date of its publication in the *Official Journal of the European Union*.

Done at Brussels, 15 September 2023.

The President
M. ALONSO ALONSO

COUNCIL DECISION (EU) 2023/1794**of 18 September 2023****establishing the position to be taken on behalf of the European Union within the Committee on Government Procurement on the adoption of its rules of procedure for the selection of the Chairperson****(Text with EEA relevance)**

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 207(4), first subparagraph, in conjunction with Article 218(9) thereof,

Having regard to the proposal from the European Commission,

Whereas:

- (1) The Agreement on Government Procurement is a plurilateral agreement, within the framework of the World Trade Organization, which aims to mutually open government procurement markets among its Parties. The revised version of that Agreement entered into force on 6 April 2014 ('the Revised GPA').
- (2) Article XXI:1 of the Revised GPA establishes a Committee on Government Procurement ('the Committee') for the purpose of affording Parties the opportunity to consult on any matter relating to the operation of the Revised GPA or the furtherance of its objectives.
- (3) Article XXI:1 of the Revised GPA provides that the Committee is to elect its own Chairperson.
- (4) The draft rules of procedure for the selection of the Chairperson were distributed by the Committee on 12 May 2023.
- (5) It is appropriate to establish the position to be taken on the Union's behalf within the Committee on the adoption of its rules of procedure as those rules will be binding on the Union.
- (6) The draft rules of procedure for the selection of the Chairperson, distributed by the Committee on 12 May 2023, should therefore be adopted in order to regulate the functioning of the Committee,

HAS ADOPTED THIS DECISION:

Article 1

The position to be taken on behalf of the European Union within the Committee on Government Procurement established by the Agreement on Government Procurement shall be to support the adoption of its rules of procedure for the selection of the Chairperson.

The text of those rules of procedure is attached to this Decision.

Article 2

This Decision shall enter into force on the date of its adoption.

Done at Brussels, 18 September 2023.

For the Council
The President
L. PLANAS PUCHADES

**Rules of Procedure for the selection of the Chairperson of the WTO Committee on Government
Procurement (the 'Committee')**

- (1) The Parties shall select a Chairperson from among their representatives to the Committee on Government Procurement on a yearly basis.
 - (2) The Parties may decide to extend the term of the Chairperson, drawing on Chairperson's work plan for the following year.
 - (3) A candidate shall be selected as Chairperson on the basis of the candidate's capacity, experience, availability and competencies to undertake the attendant responsibilities. The Chairperson will serve in a personal capacity.
 - (4) The outgoing Chairperson shall hold consultations to facilitate the selection. If there is no Chairperson, the Parties may appoint, by consensus, an interim Chairperson or invite the Party that provided the previous Chairperson to hold such consultations.
 - (5) Prior to or during the course of the consultations, the candidate(s) for the position of the Chairperson shall be given an opportunity to present proposed plans to the Parties for the period of chairing the Committee.
 - (6) The appointment shall take place at the first regular Committee meeting of the year. If the office of Chairperson becomes vacant in the middle of a year, the Parties shall aim to find a replacement within the shortest possible delay.
 - (7) The appointment shall take effect at the end of the meeting provided in the preceding paragraph. If there is no Chairperson at that time, it shall take effect immediately.
 - (8) The Chairperson shall hold office until the end of the first regular meeting of the following calendar year, unless the Chairperson is no longer able to serve or resigns at an earlier time.
 - (9) If the Parties are unable to reach consensus on the selection of a Chairperson, so that the Committee is prevented from fulfilling its obligation to meet at least once a year, the Committee may appoint, by consensus, an interim Chairperson from among the candidates, or alternatively invite the Party that provided the previous Chairperson, to temporarily facilitate the meetings of the Committee until such time as a Chairperson can be appointed.
 - (10) The Parties may decide to complement these rules of procedure further. The rules of procedure may be reviewed within five years of their adoption.
-

COMMISSION IMPLEMENTING DECISION EU 2023/1795**of 10 July 2023****pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework***(notified under document C(2023)4745)***(Text with EEA relevance)**

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ⁽¹⁾, and in particular Article 45(3) thereof,

Whereas:

1. INTRODUCTION

- (1) Regulation (EU) 2016/679 ⁽²⁾ sets out the rules for the transfer of personal data from controllers or processors in the Union to third countries and international organisations to the extent that such transfers fall within its scope of application. The rules on international data transfers are laid down in Chapter V of that Regulation. While the flow of personal data to and from countries outside the European Union is essential for the expansion of cross-border trade and international cooperation, the level of protection afforded to personal data in the Union must not be undermined by transfers to third countries or international organisations ⁽³⁾.
- (2) Pursuant to Article 45(3) of Regulation (EU) 2016/679, the Commission may decide, by means of an implementing act, that a third country, a territory or one or more specified sectors within a third country, ensure(s) an adequate level of protection. Under this condition, transfers of personal data to a third country may take place without the need to obtain any further authorisation, as provided for in Article 45(1) and recital 103 of Regulation (EU) 2016/679.
- (3) As specified in Article 45(2) of Regulation (EU) 2016/679, the adoption of an adequacy decision has to be based on a comprehensive analysis of the third country's legal order, covering both the rules applicable to data importers and the limitations and safeguards as regards access to personal data by public authorities. In its assessment, the Commission has to determine whether the third country in question guarantees a level of protection 'essentially equivalent' to that ensured within the Union (recital 104 of Regulation (EU) 2016/679). Whether this is the case is to be assessed against Union legislation, notably Regulation (EU) 2016/679, as well as the case law of the Court of Justice of the European Union (the Court of Justice) ⁽⁴⁾.

⁽¹⁾ OJ L 119, 4.5.2016, p. 1.

⁽²⁾ For ease of reference, a list of abbreviations used in this Decision is included in Annex VIII.

⁽³⁾ See recital 101 of Regulation (EU) 2016/679.

⁽⁴⁾ See, most recently, Case C-311/18, *Facebook Ireland and Schrems (Schrems II)* ECLI:EU:C:2020:559.

- (4) As clarified by the Court of Justice in its judgment of 6 October 2015 in Case C-362/14, *Maximilian Schrems v Data Protection Commissioner* ⁽⁵⁾ (*Schrems*), this does not require finding an identical level of protection. In particular, the means to which the third country in question has recourse for protecting personal data may differ from the ones employed in the Union, as long as they prove, in practice, effective for ensuring an adequate level of protection ⁽⁶⁾. The adequacy standard therefore does not require a point-to-point replication of Union rules. Rather, the test is whether, through the substance of privacy rights and their effective implementation, supervision and enforcement, the foreign system as a whole delivers the required level of protection ⁽⁷⁾. Furthermore, according to that judgment, when applying this standard, the Commission should notably assess whether the legal framework of the third country in question provides rules intended to limit interferences with the fundamental rights of the persons whose data is transferred from the Union, which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security, and provides effective legal protection against interferences of that kind ⁽⁸⁾. The 'Adequacy Referential' of the European Data Protection Board, which seeks to further clarify this standard, also provides guidance in this regard ⁽⁹⁾.
- (5) The applicable standard with respect to such interference with the fundamental rights to privacy and data protection was further clarified by the Court of Justice in its judgment of 16 July 2020 in Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems* (*Schrems II*), which invalidated Commission Implementing Decision (EU) 2016/1250 ⁽¹⁰⁾ on a previous transatlantic data flow framework, the EU-U.S. Privacy Shield (Privacy Shield). The Court of Justice considered that the limitations to the protection of personal data arising from U.S. domestic law on the access and use by U.S. public authorities of data transferred from the Union to the United States for national security purposes were not circumscribed in a way that satisfies requirements that are essentially equivalent to those under Union law, as regards the necessity and proportionality of such interferences with the right to data protection ⁽¹¹⁾. The Court of Justice also considered that no cause of action was available before a body which offers the persons whose data was transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter on the right to an effective remedy ⁽¹²⁾.
- (6) Following the *Schrems II* judgment, the Commission entered into talks with the U.S. government with a view to a possible new adequacy decision that would meet the requirements of Article 45(2) of Regulation (EU) 2016/679 as interpreted by the Court of Justice. As a result of these discussions, the United States on 7 October 2022 adopted Executive Order 14086 'Enhancing Safeguards for US Signals Intelligence Activities' (EO 14086), which is complemented by a Regulation on the Data Protection Review Court issued by the U.S. Attorney General (AG Regulation) ⁽¹³⁾. In addition, the framework that applies to commercial entities processing data transferred from the Union under the present Decision – the 'EU-U.S. Data Privacy Framework' (EU-U.S. DPF or DPF) – has been updated.
- (7) The Commission has carefully analysed U.S. law and practice, including EO 14086 and the AG Regulation. Based on the findings set out in recitals 9-200, the Commission concludes that the United States ensures an adequate level of protection for personal data transferred under the EU-U.S. DPF from a controller or a processor in the Union ⁽¹⁴⁾ to certified organisations in the United States.

⁽⁵⁾ Case C-362/14, *Maximilian Schrems v. Data Protection Commissioner* (*Schrems*), ECLI:EU:C:2015:650, paragraph 73.

⁽⁶⁾ *Schrems*, paragraph 74.

⁽⁷⁾ See Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, COM(2017)7 of 10.1.2017, section 3.1, pp. 6-7.

⁽⁸⁾ *Schrems*, paragraph 88-89.

⁽⁹⁾ European Data Protection Board, Adequacy Referential, WP 254 rev. 01, available at the following link: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

⁽¹⁰⁾ Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (OJ L 207, 1.8.2016, p. 1).

⁽¹¹⁾ *Schrems II*, paragraph 185.

⁽¹²⁾ *Schrems II*, paragraph 197.

⁽¹³⁾ 28 CFR Part 302.

⁽¹⁴⁾ This Decision has EEA relevance. The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Joint Committee Decision incorporating Regulation (EU) 2016/679 into Annex XI to the EEA Agreement was adopted by the EEA Joint Committee on 6 July 2018 and entered into force on 20 July 2018. The Regulation is thus covered by that agreement. For the purposes of the decision, references to the EU and EU Member States should thus be understood as also covering the EEA States.

- (8) This Decision has the effect that personal data transfers from controllers and processors in the Union ⁽¹⁵⁾ to certified organisations in the United States may take place without the need to obtain any further authorisation. It does not affect the direct application of Regulation (EU) 2016/679 to such organisations where the conditions regarding the territorial scope of that Regulation, laid down in its Article 3, are fulfilled.

2. THE EU-U.S. DATA PRIVACY FRAMEWORK

2.1. Personal and material scope

2.1.1. *Certified organisations*

- (9) The EU-U.S. DPF is based on a system of certification by which U.S. organisations commit to a set of privacy principles - the 'EU-U.S. Data Privacy Framework Principles', including the Supplemental Principles (together: the Principles) - issued by the U.S. Department of Commerce (DoC) and contained in Annex I to this Decision ⁽¹⁶⁾. To be eligible for certification under the EU-U.S. DPF, an organisation must be subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC) or the U.S. Department of Transportation (DoT) ⁽¹⁷⁾. The Principles apply immediately upon certification. As explained in more detail in recitals 48-52, EU-U.S. DPF organisations are required to re-certify their adherence to the Principles on an annual basis ⁽¹⁸⁾.

2.1.2. *Definition of personal data and concepts of controller and 'agent'*

- (10) The protection afforded under the EU-U.S. DPF applies to any personal data transferred from the Union to organisations in the U.S. that have certified their adherence to the Principles with the DoC, with the exception of data that is collected for publication, broadcast or other forms of public communication of journalistic material and information in previously published material disseminated from media archives ⁽¹⁹⁾. Such information can therefore not be transferred on the basis of the EU-U.S. DPF.
- (11) The Principles define personal data/personal information in the same way as Regulation (EU) 2016/679, i.e. as "data about an identified or identifiable individual that are within the scope of the GDPR received by an organization in the United States from the EU, and recorded in any form" ⁽²⁰⁾. Accordingly, they also cover pseudonymised (or "key-coded") research data (including where the key is not shared with the receiving U.S. organisation) ⁽²¹⁾. Similarly, the notion of processing is defined as "any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination and erasure or destruction" ⁽²²⁾.
- (12) The EU-U.S. DPF applies to organisations in the U.S. that qualify as controllers (i.e. as a person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data) ⁽²³⁾ or processors (i.e. agents acting on behalf of a controller) ⁽²⁴⁾. U.S. processors must be contractually bound to act only on instructions from the EU controller and assist the latter in responding to individuals exercising their rights under

⁽¹⁵⁾ This Decision does not affect the requirements of Regulation (EU) 2016/679 that apply to the entities (controllers and processors) in the Union transferring the data, for instance on purpose limitation, data minimisation, transparency and data security (see also Article 44 of Regulation (EU) 2016/679).

⁽¹⁶⁾ See in this respect *Schrems*, paragraph 81, in which the Court of Justice confirmed that a system of self-certification can ensure an adequate level of protection.

⁽¹⁷⁾ Annex I, Section I.2. The FTC has broad jurisdiction over commercial activities, with some exceptions, e.g. with respect to banks, airlines, the business of insurance and common carrier activities of telecommunications service providers (although the decision of the U.S. Court of Appeals for the Ninth Circuit of 26 February 2018 in *FTC v. AT&T* has confirmed that the FTC has jurisdiction over non-common carrier activities of such entities). See also Annex IV, footnote 2. The DoT is competent to enforce compliance by airlines and ticket agents (for air transportation), see Annex V, under section A.

⁽¹⁸⁾ Annex I, Section III.6.

⁽¹⁹⁾ Annex I, Section III.2.

⁽²⁰⁾ Annex I, Section I.8.a.

⁽²¹⁾ Annex I, Section III.14.g.

⁽²²⁾ Annex I, Section I.8.b.

⁽²³⁾ Annex I, Section I.8.c.

⁽²⁴⁾ See e.g. Annex I, Section II.2.b and Section II.3.b and 7.d, which make clear that agents act on behalf of a controller, subject to the latter's instructions and under specific contractual obligations.

the Principles ⁽²⁵⁾. In addition, in the case of sub-processing, a processor must conclude a contract with the sub-processor guaranteeing the same level of protection as provided by the Principles and take steps to ensure its proper implementation ⁽²⁶⁾.

2.2. EU-U.S. Data Privacy Framework Principles

2.2.1. *Purpose limitation and choice*

- (13) Personal data should be processed lawfully and fairly. It should be collected for a specific purpose and subsequently used only insofar as this is not incompatible with the purpose of processing.
- (14) Under the EU-U.S. DPF, this is ensured through different Principles. Firstly, under the *Data Integrity and Purpose Limitation Principle*, similarly as under Article 5(1)(b) of Regulation (EU) 2016/679, an organisation may not process personal data in a way that is incompatible with the purpose for which it was originally collected or subsequently authorised by the data subject ⁽²⁷⁾.
- (15) Secondly, before using personal data for a new (changed) purpose that is materially different but still compatible with the original purpose, or disclosing it to a third party, the organisation must provide data subjects with the opportunity to object (opt-out), in accordance with the *Choice Principle* ⁽²⁸⁾, through a clear, conspicuous and readily available mechanism. Importantly, this Principle does not supersede the express prohibition on incompatible processing ⁽²⁹⁾.

⁽²⁵⁾ Annex I, Section III.10.a. See also the guidance prepared by the DoC, in consultation with the European Data Protection Board, under the Privacy Shield, which clarified the obligations of US processors receiving personal data from the Union under the framework. As these rules have not changed, this guidance/FAQ remains relevant under the EU-U.S. DPF (<https://www.privacyshield.gov/article?id=Processing-FAQs>).

⁽²⁶⁾ Annex I, Section II.3.b.

⁽²⁷⁾ Annex I, Section II.5.a. Compatible purposes may include auditing, fraud prevention, or other purposes consistent with the expectations of a reasonable person given the context of the collection (see Annex I, footnote 6).

⁽²⁸⁾ Annex I, Section II.2.a. This does not apply when an organisation provides personal data to a processor acting on its behalf and under its instructions (Annex I, Section II.2.b). That said, in this case the organisation needs to have a contract in place and ensure compliance with the *Accountability for Onward Transfer Principle*, as described in further detail in recital 43. In addition, the *Choice Principle* (as well as the *Notice Principle*) may be restricted when personal data is processed in the context of due diligence (as part of a potential merger or takeover) or audits, to the extent and for as long as necessary to meet statutory or public interest requirements, or to the extent and for as long as the application of these Principles would prejudice the legitimate interests of the organisation in the specific context of due diligence investigations or audits (Annex I, Section III.4). Supplemental Principle 15 (Annex I, Section III.15.a and b) also foresees an exception to the *Choice Principle* (as well as to the *Notice and Accountability for Onward Transfer Principles*) for personal data from publicly available sources (unless the EU data exporter indicates that the information is subject to restrictions that require application of those principles) or personal data collected from records open to consultation by the public in general (as long as it is not combined with non-public record information and any conditions for consultation are respected). Similarly, Supplemental Principle 14 (Annex I, Section III.14.f) provides an exception to the *Choice Principle* (as well as to the *Notice and Accountability for Onward Transfer Principles*) for the processing of personal data by a pharmaceutical or medical device company for product safety and efficacy monitoring activities, to the extent that adherence to the Principles interferes with compliance with regulatory requirements.

⁽²⁹⁾ This applies to all data transfers under the EU-U.S. DPF, including where these concern data collected in the context of the employment relationship. While a certified U.S. organisation may therefore in principle use human resources data for different, non-employment-related purposes (e.g. certain marketing communications), it must respect the prohibition on incompatible processing and moreover may do so only in accordance with the *Notice and Choice Principles*. Exceptionally, an organisation may use personal data for an additional compatible purpose without providing *Notice and Choice*, but only to the extent and for the period necessary to avoid prejudicing the ability of the organisation in making promotions, appointments, or other similar employment decisions (See Annex I, Section III.9.b.(iv)). The prohibition on the U.S. organisation to take any punitive action against the employee for exercising such choice, including any restriction of employment opportunities, will ensure that, despite the relationship of subordination and inherent dependency, the employee will be free from pressure and thus can exercise a genuine free choice. See Annex I, Section III.9.b.(i).

2.2.2. *Processing of special categories of personal data*

- (16) Specific safeguards should exist where ‘special categories’ of data are processed.
- (17) In accordance with the *Choice Principle*, specific safeguards apply to the processing of ‘sensitive information’, i.e. personal data specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, information on the sex life of the individual or any other information received from a third party that is identified and treated by that party as sensitive ⁽³⁰⁾. This means that any data that is considered sensitive under Union data protection law (including data on sexual orientation, genetic data and biometric data) will be treated as sensitive under the EU-U.S. DPF by certified organisations.
- (18) As a general rule, organisations must obtain affirmative express consent (i.e. opt-in) from individuals to use sensitive information for purposes other than those for which it was originally collected or subsequently authorised by the individual (through opt-in), or to disclose it to third parties ⁽³¹⁾.
- (19) Such consent does not have to be obtained in limited circumstances similar to comparable exceptions provided under Union data protection law, e.g. where the processing of sensitive data is in the vital interest of a person; is necessary for the establishment of legal claims; or is required to provide medical care or diagnosis ⁽³²⁾.

2.2.3. *Data accuracy, minimisation and security*

- (20) Data should be accurate and, where necessary, kept up to date. It should also be adequate, relevant and not excessive in relation to the purposes for which it is processed, and in principle be kept for no longer than is necessary for the purposes for which the personal data is processed.
- (21) Under the *Data Integrity and Purpose Limitation Principle* ⁽³³⁾, personal data must be limited to what is relevant for the purpose of the processing. In addition, organisations must, to the extent necessary for the purposes of the processing, take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete and current.
- (22) Moreover, personal information may be retained in a form identifying or rendering an individual identifiable (and thus in the form of personal data) ⁽³⁴⁾ only for as long as it serves the purpose(s) for which it was initially collected or subsequently authorised by the individual pursuant to the *Choice Principle*. This obligation does not prevent organisations from continuing to process personal information for longer periods, but only for the time and to the extent such processing reasonably serves one of the following specific purposes similar to comparable exceptions provided under Union data protection law: archiving in the public interest, journalism, literature and art, scientific and historical research and statistical analysis ⁽³⁵⁾. Where personal data is retained for one of these purposes, its processing is subject to the safeguards provided by the Principles ⁽³⁶⁾.
- (23) Personal data should also be processed in a manner that ensures its security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage. To that end, controllers and processors should take appropriate technical or organisational measures to protect personal data from possible threats. These measures should be assessed taking into consideration the state of the art, related costs and the nature, scope, context and purposes of processing, as well as the risks for the rights of individuals.

⁽³⁰⁾ Annex I, Section II.2.c.

⁽³¹⁾ Annex I, Section II.2.c.

⁽³²⁾ Annex I, Section III.1.

⁽³³⁾ Annex I, Section II.5.

⁽³⁴⁾ See Annex I, footnote 7, which clarifies that an individual is considered ‘identifiable’ as long as an organisation or third party could reasonably identify that individual, taking into account the means of identification reasonably likely to be used (considering, among other things, the cost and the amount of time required for identification and the available technology at the time of the processing).

⁽³⁵⁾ Annex I, Section II.5.b.

⁽³⁶⁾ *Ibid.*

- (24) Under the EU-U.S. DPF, this is ensured by the *Security Principle*, which requires, similarly to Article 32 Regulation (EU) 2016/679, to take reasonable and appropriate security measures, taking into account the risks involved in the processing and the nature of the data ⁽³⁷⁾.

2.2.4. *Transparency*

- (25) Data subjects should be informed of the main features of the processing of their personal data.
- (26) This is ensured through the *Notice Principle* ⁽³⁸⁾, which, similarly to the transparency requirements under Regulation (EU) 2016/679, requires organisations to inform data subjects about, inter alia, (i) the participation of the organisation in the DPF, (ii) the type of data collected, (iii) the purpose of the processing, (iv) the type or identity of third parties to which personal data may be disclosed and the purposes for doing so, (v) their individual rights, (vi) how to contact the organisation and (vii) available redress avenues.
- (27) This notice must be provided in a clear and conspicuous language when individuals are first asked to provide the personal data or as soon as practicable thereafter, but in any event before the data is used for a materially different (but compatible) purpose than the one for which it was collected, or before it is disclosed to a third party ⁽³⁹⁾.
- (28) In addition, organisations must make their privacy policies reflecting the Principles public (or, in the case of human resources data, make them readily available to the concerned individuals) and provide links to the DoC's website (with further details on certification, the rights of data subjects and available recourse mechanisms), the Data Privacy Framework List (DPF List) of participating organisations and the website of an appropriate alternative dispute settlement provider ⁽⁴⁰⁾.

2.2.5. *Individual rights*

- (29) Data subjects should have certain rights which can be enforced against the controller or processor, in particular the right of access to data, the right to object to the processing and the right to have data rectified and erased.
- (30) The *Access Principle* ⁽⁴¹⁾ of the EU-U.S. DPF provides individuals with such rights. In particular, data subjects have the right, without the need for justification, to obtain from an organisation confirmation of whether it is processing personal data related to them; have the data communicated to them; and obtain information about the purpose of the processing, the categories of personal data being processed and the (categories of) recipients to whom the data is disclosed ⁽⁴²⁾. Organisations are required to respond to access requests within a reasonable period of time ⁽⁴³⁾. An

⁽³⁷⁾ Annex I, Section II.4.a. In addition, as regards human resources data, the EU-U.S. DPF requires employers to accommodate the privacy preferences of employees by restricting access to the personal data, anonymising certain data or assigning codes or pseudonyms (Annex I, Section III.9.b.(iii)).

⁽³⁸⁾ Annex I, Section II.1.

⁽³⁹⁾ Annex I, Section II.1.b. Supplemental Principle 14 (Annex I, Section III.14.b and c) lays down specific provisions for the processing of personal data in the context of health research and clinical trials. In particular, this Principle allows organisations to process clinical trial data even after a person withdraws from the trial, if this was made clear in the notice provided when the individual agreed to participate. Similarly, where an EU-U.S. DPF organisation receives personal data for health research purposes, it may only use it for a new research activity in accordance with the *Notice* and *Choice* principles. In this case, the notice to the individual should in principle provide information about any future specific uses of the data (e.g. related studies). Where it is not possible to include from the outset all future uses of the data (because a new research use could arise from new insights or medical/research developments), an explanation that the data may be used in future unanticipated medical and pharmaceutical research activities must be included. If such further use is not consistent with the general research purposes for which the data was collected (i.e. if the new purposes are materially different, but still compatible with the original purpose, see recitals 14-15), new consent (i.e. opt-in) needs to be obtained. See in addition the specific restrictions/exceptions to the *Notice Principle* described in footnote 28.

⁽⁴⁰⁾ Annex I, Section III.6.d.

⁽⁴¹⁾ See also the Supplemental Principle on 'Access' (Annex I, Section III.8).

⁽⁴²⁾ Annex I, Section III.8.a.(i)-(ii).

⁽⁴³⁾ Annex I, Section III.8.i.

organisation may set reasonable limits to the number of times within a given period that access requests from a particular individual will be met and may charge a fee that is not excessive, e.g. where requests are manifestly excessive, in particular because of their repetitive character ⁽⁴⁴⁾.

- (31) The right of access may only be restricted in exceptional circumstances similar to the ones provided under Union data protection law, in particular where the legitimate rights of others would be violated; where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the circumstances of the case (although expense and burden are not controlling factors in determining whether providing access is reasonable); to the extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security, public security or defence; the information contains confidential commercial information; or the information is processed solely for research or statistical purposes ⁽⁴⁵⁾. Any denial of, or limitation to a right has to be necessary and duly justified, with the organisation bearing the burden of demonstrating that these requirements are fulfilled ⁽⁴⁶⁾. In carrying out that assessment, the organisation must take particularly into account the individual's interests ⁽⁴⁷⁾. Where it is possible to separate information from other data to which a restriction applies, the organisation must redact the protected information and disclose the remaining information ⁽⁴⁸⁾.
- (32) In addition, data subjects have the right to obtain rectification or amendment of inaccurate data, and to obtain deletion of data that has been processed in violation of the Principles ⁽⁴⁹⁾. Moreover, as explained in recital 15, individuals have a right to object/opt-out to the processing of their data for materially different (but compatible) purposes than those for which the data was collected and to the disclosure of their data to third parties. When personal data is used for direct marketing purposes, individuals have a general right to opt-out from the processing at any time ⁽⁵⁰⁾.
- (33) The Principles do not specifically address the issue of decisions affecting the data subject based solely on the automated processing of personal data. However, as regards personal data that has been collected in the Union, any decision based on automated processing will typically be taken by the controller in the Union (which has a direct relationship with the concerned data subject) and is thus directly subject to Regulation (EU) 2016/679 ⁽⁵¹⁾. This includes transfer scenarios where the processing is carried out by a foreign (for instance U.S.) business operator acting as an agent (processor) on behalf of the controller in the Union (or as a sub-processor acting on behalf of the Union processor having received the data from a Union controller that collected it) which on this basis then takes the decision.
- (34) This was confirmed by a study commissioned by the Commission in 2018 in the context of the second annual review of the functioning of the Privacy Shield ⁽⁵²⁾, which concluded that, at the time, there was no evidence suggesting that automated decision-making was normally being carried out by Privacy Shield organisations on the basis of personal data transferred under the Privacy Shield.

⁽⁴⁴⁾ Annex I, Section III.8.f.(i)-(ii) and g.

⁽⁴⁵⁾ Annex I, Section III.4; 8.b, c, e; 14.e, f and 15.d.

⁽⁴⁶⁾ Annex I, Section III.8.e.(ii). The organisation must inform the individual of the reasons for the denial/restriction and provide a contact point for any further inquiries, Section III.8.a.(iii).

⁽⁴⁷⁾ Annex I, Section III.8.a.(ii)-(iii).

⁽⁴⁸⁾ Annex I, Section III.8.a.(i).

⁽⁴⁹⁾ Annex I, Section II.6 and III.8.a.(i).

⁽⁵⁰⁾ Annex I, Section III.8.1.2.

⁽⁵¹⁾ Conversely, in the exceptional case where the U.S. organisation has a direct relationship with the Union data subject, this will typically be a consequence of it having targeted the individual in the Union by offering him or her goods or services or monitoring his or her behaviour. In this scenario, the U.S. organisation will itself fall within the scope of application of Regulation (EU) 2016/679 (Article 3(2)) and thus has to directly comply with Union data protection law.

⁽⁵²⁾ SWD(2018)497final, section 4.1.5. The study focused on (i) the extent to which Privacy Shield organisations in the U.S. take decisions affecting individuals based on automated processing of personal data transferred from companies in the EU under the Privacy Shield; and (ii) the safeguards for individuals that U.S. federal law provides for this kind of situations and the conditions for these safeguards to apply.

- (35) In any event, in areas where companies most likely resort to the automated processing of personal data to take decisions affecting the individual (e.g. credit lending, mortgage offers, employment, housing and insurance), U.S. law offers specific protections against adverse decisions ⁽⁵³⁾. These acts typically provide that individuals have the right to be informed of the specific reasons underlying the decision (e.g. the rejection of a credit), to dispute incomplete or inaccurate information (as well as reliance on unlawful factors), and to seek redress. In the area of consumer credit, the Fair Credit Reporting Act (FCRA) and Equal Credit Opportunity Act (ECOA) contain safeguards that provide consumers with some form of a right to explanation and a right to contest the decision. These Acts are relevant in a wide range of areas, including credit, employment, housing and insurance. In addition, certain anti-discrimination laws, such as Title VII of the Civil Rights Act and the Fair Housing Act, provide individuals with protections with respect to models used in automated decision-making that could lead to discrimination on the basis of certain characteristics, and grant individuals rights to challenge such decisions, including automated ones. With respect to health information, the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule creates certain rights that are similar to those of Regulation (EU) 2016/679 with respect to accessing personal health information. In addition, guidance from the U.S. authorities require medical providers to receive information that allow them to inform individuals of automated decision-making systems used in the medical sector ⁽⁵⁴⁾.
- (36) Therefore, these rules offer protections similar to those provided under Union data protection law in the unlikely situation in which automated decisions would be taken by the EU-U.S. DPF organisation itself.

2.2.6. *Restrictions on onward transfers*

- (37) The level of protection afforded to personal data transferred from the Union to organisations in the United States must not be undermined by the further transfer of such data to a recipient in the United States or another third country.
- (38) Under the *Accountability for Onward Transfer Principle* ⁽⁵⁵⁾, special rules apply for so-called ‘onward transfers’, i.e. transfers of personal data from an EU-U.S. DPF organisation to a third party controller or processor, irrespective of whether the latter is located in the United States or a third country outside the United States (and the Union). Any onward transfer can only take place (i) for limited and specified purposes, (ii) on the basis of a contract between the EU-U.S. DPF organisation and the third party ⁽⁵⁶⁾ (or comparable arrangement within a corporate group ⁽⁵⁷⁾) and (iii) only if that contract requires the third party to provide the same level of protection as the one guaranteed by the Principles.
- (39) This obligation to provide the same level of protection as guaranteed by the Principles, read in combination with the *Data Integrity and Purpose Limitation Principle*, notably means that the third party may only process the personal information transmitted to it for purposes that are not incompatible with the purposes for which it was collected or subsequently authorised by the individual (in accordance with the *Choice Principle*).

⁽⁵³⁾ See e.g. the Equal Credit Opportunity Act (15 U.S.C. 1691 et seq.), Fair Credit Reporting Act (15 USC § 1681 et seq.), or the Fair Housing Act (42 U.S.C. 3601 et seq.). In addition, the United States has subscribed to the Organisation for Economic Cooperation and Development Artificial Intelligence Principles, which inter alia include principles on transparency, explainability, security and accountability.

⁽⁵⁴⁾ See e.g. the guidance available at 2042-What personal health information do individuals have a right under HIPAA to access from their health care providers and health plans? | HHS.gov.

⁽⁵⁵⁾ See Annex I, Section II.3 and Supplemental Principle ‘Obligatory contracts for Onward Transfers’ (Annex I, Section III.10).

⁽⁵⁶⁾ As an exception to this general principle, an organisation may onward transfer personal data of a small number of employees without entering into a contract with the recipient for occasional employment-related operational needs, e.g. the booking of a flight, hotel room, or insurance coverage. However, also in this case, the organisation still has to comply with the *Notice* and *Choice* Principles (see Annex I, Section III.9.e).

⁽⁵⁷⁾ See Supplemental Principle ‘Obligatory contracts for Onward Transfers’ (Annex I, Section III.10.b). While this principle allows for transfers based also on non-contractual instruments (e.g. intra-group compliance and control programs), the text makes clear that these instruments must always “ensur[e] the continuity of protection of personal information under the Principles”. Moreover, given that the certified U.S. organisation will remain responsible for compliance with the Principles, it will have a strong incentive to use instruments that are indeed effective in practice.

- (40) The *Accountability for Onward Transfer Principle* should also be read in conjunction with the *Notice Principle* and, in the case of an onward transfer to a third party controller ⁽⁵⁸⁾, with the *Choice Principle*, according to which data subjects must be informed (among others) about the type/identity of any third party recipient, the purpose of the onward transfer and the choice offered, and can object (opt out) or, in the case of sensitive data, have to give “affirmative express consent” (opt in) for the onward transfer.
- (41) The obligation to provide the same level of protection as required by the Principles applies to any and all third parties involved in the processing of the data so transferred irrespective of their location (in the U.S. or another third country) as well as when the original third party recipient itself transfers those data to another third party recipient, for example for sub-processing purposes.
- (42) In all cases, the contract with the third-party recipient must provide that the latter will notify the EU-U.S. DPF organisation if it makes a determination that it can no longer meet its obligation. When such a determination is made, the processing by the third party must cease or other reasonable and appropriate steps must be taken to remedy the situation ⁽⁵⁹⁾.
- (43) Additional protections apply in the case of an onward transfer to a third party agent (i.e. a processor). In such a case, the U.S. organisation must ensure that the agent only acts on its instructions and take reasonable and appropriate steps (i) to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organisation's obligations under the Principles and, (ii) to stop and remediate unauthorised processing, upon notice ⁽⁶⁰⁾. The organisation may be required by the DoC to provide a summary or representative copy of the privacy provisions of the contract ⁽⁶¹⁾. Where compliance problems arise in a (sub-)processing chain, the organisation acting as the controller of the personal data will in principle face liability, as specified in the *Recourse, Enforcement and Liability Principle*, except if it proves that it is not responsible for the event giving rise to the damage ⁽⁶²⁾.

2.2.7. *Accountability*

- (44) Under the accountability principle, entities processing data are required to put in place appropriate technical and organisational measures to effectively comply with their data protection obligations and be able to demonstrate such compliance, in particular to the competent supervisory authority.
- (45) Once an organisation has voluntarily decided to certify ⁽⁶³⁾ under the EU-U.S. DPF, its effective compliance with the Principles is compulsory and enforceable. Under the *Recourse, Enforcement and Liability Principle* ⁽⁶⁴⁾, EU-U.S. DPF organisations must provide effective mechanisms to ensure compliance with the Principles. Organisations must also take measures to verify ⁽⁶⁵⁾ that their privacy policies conform to the Principles and are in fact complied with. This can be done either through a system of self-assessment, which must include internal procedures ensuring that employees receive training on the implementation of the organisation's privacy policies and that compliance is periodically reviewed in an objective manner, or outside compliance reviews, the methods of which may include auditing, random checks or use of technology tools.

⁽⁵⁸⁾ Individuals will have no opt-out right where the personal data is transferred to a third party that is acting as an agent to perform tasks on behalf of and under the instructions of the U.S. organisation. However, this requires a contract with the agent and the U.S. organisation will bear the responsibility to guarantee the protections provided under the Principles by exercising its powers of instruction.

⁽⁵⁹⁾ The situation is different depending on whether the third party is a controller or a processor (agent). In the first scenario, the contract with the third party must provide that the latter ceases processing or takes other reasonable and appropriate steps to remedy the situation. In the second scenario, it is for the EU-U.S. DPF organisation - as the one controlling the processing under whose instructions the agent operates - to take these measures. See Annex I, Section II.3.

⁽⁶⁰⁾ Annex I, Section II.3.b.

⁽⁶¹⁾ *Ibid.*

⁽⁶²⁾ Annex I, Section II.7.d.

⁽⁶³⁾ See also Supplemental Principle ‘Self-Certification’ (Annex I, Section III.6).

⁽⁶⁴⁾ See also Supplemental Principle ‘Dispute Resolution and Enforcement’ (Annex I, Section III.11).

⁽⁶⁵⁾ See also Supplemental Principle ‘Verification’ (Annex I, Section III.7).

- (46) In addition, organisations must retain records on the implementation of their EU-U.S. DPF practices and make them available upon request in the context of an investigation or a complaint about non-compliance to an independent dispute resolution body or competent enforcement authority ⁽⁶⁶⁾.

2.3. Administration, oversight and enforcement

- (47) The EU-U.S. DPF will be administered and monitored by the DoC. The Framework provides for oversight and enforcement mechanisms in order to verify and ensure that EU-U.S. DPF organisations comply with the Principles and that any failure to comply is addressed. These mechanisms are set out in the Principles (Annex I) and the commitments undertaken by the DoC (Annex III), the FTC (Annex IV) and the DoT (Annex V).

2.3.1. (Re-)certification

- (48) To certify under the EU-U.S. DPF (or re-certify on an annual basis), organisations are required to publicly declare their commitment to comply with the Principles, make their privacy policies available and fully implement them ⁽⁶⁷⁾. As part of their (re-)certification application, organisations have to submit information to the DoC on, inter alia, the name of the relevant organisation, a description of the purposes for which the organisation will process personal data, the personal data that will be covered by the certification, as well as the chosen verification method, the relevant independent recourse mechanism and the statutory body that has jurisdiction to enforce compliance with the Principles ⁽⁶⁸⁾.
- (49) Organisations can receive personal data on the basis of the EU-U.S. DPF from the date they are placed on the DPF list by the DoC. To ensure legal certainty and avoid 'false claims', organisations certifying for the first time are not allowed to publicly refer to their adherence to the Principles before the DoC has determined that the organisation's certification submission is complete and added the organisation to the DPF List ⁽⁶⁹⁾. To be allowed to continue to rely on the EU-U.S. DPF to receive personal data from the Union, such organisations must annually re-certify their participation in the framework. When an organisation leaves the EU-U.S. DPF for any reason, it must remove all statements implying that the organisation continues to participate in the Framework ⁽⁷⁰⁾.
- (50) As reflected in the commitments set out in Annex III, the DoC will verify whether organisations meet all certification requirements and have put in place a (public) privacy policy containing the information required under the *Notice Principle* ⁽⁷¹⁾. Building on the experience with the (re-)certification process under the Privacy Shield, the DoC will carry out a number of checks, including to verify whether organisations' privacy policies contain a hyperlink to the correct complaint form on the website of the relevant dispute resolution mechanism and, when several entities and subsidiaries of one organisation are included in a certification submission, whether the privacy policies of each of those entities meet the certification requirements and are readily available to data subjects ⁽⁷²⁾. In addition, where necessary, the DoC will carry out cross-checks with the FTC and DoT to verify that the organisations are subject to oversight body identified in their (re-)certification submissions, and will work with alternative dispute resolution bodies to verify that the organisations are registered for the independent recourse mechanism identified in their (re-)certification submission ⁽⁷³⁾.

⁽⁶⁶⁾ Annex I, Section III.7.

⁽⁶⁷⁾ Annex I, Section I. 2.

⁽⁶⁸⁾ Annex I, Section III.6.b and Annex III, see section 'Verify Self-Certification Requirements'.

⁽⁶⁹⁾ Annex I, footnote 12.

⁽⁷⁰⁾ Annex I, Section III.6.h.

⁽⁷¹⁾ Annex I, Section III.6.a and footnote 12, as well as and Annex III, see section 'Verify Self-Certification Requirements'.

⁽⁷²⁾ Annex III, section 'Verify Self-Certification Requirements'.

⁽⁷³⁾ Similarly, the DoC will work with the third party that will serve as the custodian of the funds collected through a fee for the DPA panel (see recital 73) to verify that organisations choosing the DPAs as their independent recourse mechanism have paid the fee for the relevant year. See Annex III, section 'Verify Self-Certification Requirements'.

- (51) The DoC will inform organisations that, in order to complete the (re-)certification, they must address all issues identified during its review. In case an organisation fails to respond within a timeframe set by the DoC (for example, as regards re-certification the expectation would be that the process is completed within 45 days) ⁽⁷⁴⁾ or otherwise fails to complete its certification, the submission will be considered abandoned. In that case, any misrepresentation about participation or compliance with the EU-U.S. DPF may be subject to enforcement action by the FTC or DoT ⁽⁷⁵⁾.
- (52) To ensure the proper application of the EU-U.S. DPF, interested parties, such as data subjects, data exporters and the national data protection authorities (DPAs), must be able to identify those organisations adhering to the Principles. To ensure such transparency at the 'entry point', the DoC has committed to maintain and make available to the public the list of organisations that have certified their adherence to the Principles and fall within the jurisdiction of at least one of the enforcement authorities referred to in Annexes IV and V to this Decision ⁽⁷⁶⁾. The DoC will update the list on the basis of an organisation's annual re-certification submission and whenever an organisation withdraws or is removed from the EU-U.S. DPF. Furthermore, to guarantee transparency also at the 'exit point', the DoC will maintain and make available to the public a record of organisations that have been removed from the list, in each case identifying the reason for such removal ⁽⁷⁷⁾. Finally, it will provide a link to the FTC's webpage on the EU-U.S. DPF, which will list the FTC's enforcement action under the Framework ⁽⁷⁸⁾.

2.3.2. *Compliance monitoring*

- (53) The DoC will monitor on an ongoing basis the effective compliance with the Principles by EU-U.S. DPF organisations through different mechanisms ⁽⁷⁹⁾. In particular, it will carry out 'spot checks' of randomly selected organisations, as well as ad hoc spot checks of specific organisations when potential compliance issues are identified (e.g. reported to the DoC by third parties) to verify whether (i) point(s) of contact for handling complaints and data subject requests are available and responsive; (ii) the organisation's privacy policy is readily available, both on its website and via a hyperlink on the DoC's website; (iii) the organisation's privacy policy continues to comply with the certification requirements and (iv) the organisations' chosen independent dispute resolution mechanism is available to handle complaints ⁽⁸⁰⁾.
- (54) If there is credible evidence that an organisation does not comply with its commitments under the EU-U.S. DPF (including if the DoC receives complaints or the organisation does not respond satisfactorily to inquiries of the DoC), the DoC will require the organisation to complete and submit a detailed questionnaire ⁽⁸¹⁾. An organisation that fails to satisfactorily and timely reply to the questionnaire will be referred to the relevant authority (the FTC or DoT) for possible enforcement action ⁽⁸²⁾. As part of its compliance monitoring activities under the Privacy Shield, the DoC regularly conducted the spot checks mentioned in recital 53 and continuously monitored public reports,

⁽⁷⁴⁾ Annex III, footnote 2.

⁽⁷⁵⁾ See Annex III, section 'Verify Self-Certification Requirements'.

⁽⁷⁶⁾ Information about the management of the DPF List can be found in Annex III (see the introduction under 'Administration and Supervision of the Data Privacy Framework Program by the Department of Commerce') and Annex I (Section I.3, Section I.4, III.6.d, and Section III.11.g).

⁽⁷⁷⁾ Annex III, see the introduction under 'Administration and Supervision of the Data Privacy Framework Program by the Department of Commerce'.

⁽⁷⁸⁾ See Annex III, section 'Tailor the Data Privacy Framework Website to Targeted Audiences'.

⁽⁷⁹⁾ See Annex III, section 'Conduct Periodic ex officio Compliance Reviews and Assessments of the Data Privacy Framework Program'.

⁽⁸⁰⁾ As part of its monitoring activities, the DoC may use different tools, including to check for broken links to privacy policies or actively monitor the news for reports that provide credible evidence of non-compliance.

⁽⁸¹⁾ See Annex III, section 'Conduct Periodic ex officio Compliance Reviews and Assessments of the Data Privacy Framework Program'.

⁽⁸²⁾ See Annex III, section 'Conduct Periodic ex officio Compliance Reviews and Assessments of the Data Privacy Framework Program'.

which allowed it to identify, address and resolve compliance issues ⁽⁸³⁾. Organisations that persistently fail to comply with the Principles will be removed from the DPF List and must return or delete the personal data received under the Framework ⁽⁸⁴⁾.

- (55) In other cases of removal, such as voluntary withdrawal from participation or failure to recertify, the organisation must either delete or return the data, or may retain it, provided it affirms to the DoC on an annual basis its commitment to continue to apply the Principles or provides adequate protection for the personal data by another authorized means (e.g. by using a contract that fully reflects the requirements of the relevant standard contractual clauses approved by the Commission) ⁽⁸⁵⁾. In this case, an organisation also has to identify a contact point within the organisation for all EU-U.S. DPF-related questions.

2.3.3. *Identifying and addressing false claims of participation*

- (56) The DoC will monitor any false claims of EU-U.S. DPF participation or the improper use of the EU-U.S. DPF certification mark, both ex officio and on the basis of complaints (e.g. received from DPAs) ⁽⁸⁶⁾. In particular, the DoC will on an ongoing basis verify that organisations that (i) withdraw from participation in the EU-U.S. DPF, (ii) fail to complete the annual re-certification (i.e. either started, but failed to complete the annual re-certification process in a timely manner or did not even start the annual re-certification process), (iii) are removed as a participant, notably for “persistent failure to comply,” or (iv) fail to complete an initial certification (i.e. started, but failed to complete the initial certification process in a timely manner), remove from any relevant published privacy policy references to the EU-U.S. DPF that imply that the organisation actively participates in the Framework ⁽⁸⁷⁾. The DoC will also conduct internet searches to identify references to the EU-U.S. DPF in organisations’ privacy policies, including to identify false claims by organisations that never participated in the EU-U.S. DPF ⁽⁸⁸⁾.
- (57) Where the DoC finds that references to the EU-U.S. DPF have not been removed or are improperly used, it will inform the organisation about a possible referral to the FTC/DoT ⁽⁸⁹⁾. If an organisation fails to respond satisfactorily, the DoC will refer the matter to the relevant agency for potential enforcement action ⁽⁹⁰⁾. Any misrepresentation to the general public by an organisation concerning its adherence to the Principles in the form of misleading statements or practices is subject to enforcement action by the FTC, DoT or other relevant U.S. enforcement authorities. Misrepresentations to the DoC are enforceable under the False Statements Act (18 U.S.C. § 1001).

⁽⁸³⁾ During the second annual review of the Privacy Shield, the DoC informed that it had conducted spot checks on 100 organisations and sent compliance questionnaires in 21 cases (after which the detected issues were rectified), see Commission SWD (2018) 497 final, p. 9. Similarly, the DoC reported during the third annual review of the Privacy Shield that it had detected three incidents through its monitoring of public reports and started the practice of carrying out spot checks on 30 companies each month, which led to follow-up with compliance questionnaires in 28% of the cases (after which the detected issues were immediately rectified, or, in three cases, were resolved after a warning letter), see Commission SWD (2019) 495 final, p. 8.

⁽⁸⁴⁾ Annex I, Section III.11.g. A persistent failure to comply arises, in particular, where an organisation refuses to comply with a final determination by any privacy self-regulatory, independent dispute resolution, or enforcement authority.

⁽⁸⁵⁾ Annex I, Section III.6.f.

⁽⁸⁶⁾ Annex III, section ‘Search for and Address False Claims of Participation’.

⁽⁸⁷⁾ *Ibid.*

⁽⁸⁸⁾ *Ibid.*

⁽⁸⁹⁾ *Ibid.*

⁽⁹⁰⁾ Under the Privacy Shield, the DoC reported during the third annual review of the framework that it had identified 669 cases of false claims of participation (between October 2018 and October 2019), most of which were resolved after the DoC’s warning letter, with 143 cases being referred to the FTC (see recital 62 below). See Commission SWD (2019) 495 final, p. 10.

2.3.4. **Enforcement**

- (58) In order to ensure that an adequate level of data protection is guaranteed in practice, an independent supervisory authority tasked with powers to monitor and enforce compliance with the data protection rules should be in place.
- (59) EU-U.S. DPF organisations must be subject to the jurisdiction of the competent U.S. authorities – the FTC and DoT – which have the necessary investigatory and enforcement powers to effectively ensure compliance with the Principles ⁽⁹¹⁾.
- (60) The FTC is an independent authority composed of five Commissioners, who are appointed by the President with the advice and consent of the Senate ⁽⁹²⁾. Commissioners are appointed for a seven-year term and may only be removed by the President for inefficiency, neglect of duty, or malfeasance in office. The FTC may not have more than three Commissioners of the same political party and Commissioners may not, during their appointment, engage in any other business, vocation, or employment.
- (61) The FTC can investigate compliance with the Principles, as well as false claims of adherence to the Principles or participation in the EU-U.S. DPF by organisations which either are no longer on the DPF List or have never certified ⁽⁹³⁾. The FTC can enforce compliance by seeking administrative or federal court orders (including ‘consent orders’ achieved via settlements) ⁽⁹⁴⁾ for preliminary or permanent injunctions or other remedies, and will systematically monitor compliance with such orders ⁽⁹⁵⁾. Where organisations fail to comply with such orders, the FTC may seek civil penalties and other remedies, including for any injury caused by the unlawful conduct. Each consent order issued to an EU-U.S. DPF organisation will have self-reporting provisions ⁽⁹⁶⁾, and organisations will be required to make public any relevant EU-U.S. DPF-related sections of any compliance or assessment report submitted to the FTC. Finally, the FTC will maintain an online list of organisations subject to FTC or court orders in EU-U.S. DPF cases ⁽⁹⁷⁾.
- (62) With respect to the Privacy Shield, the FTC took enforcement action in around 22 cases, both with respect to violations of specific requirements of the framework (e.g. failure to affirm to the DoC that the organisation continued to apply the Privacy Shield protections after it left the framework, failure to verify, through a self-assessment or outside compliance review, that the organisation complied with the framework) ⁽⁹⁸⁾ and false claims of participation in the framework (e.g. by organisations that failed to complete the necessary steps to obtain certification, or allowed their certification to lapse but misrepresented their continued participation) ⁽⁹⁹⁾. This enforcement action *inter alia* resulted from the proactive use of administrative subpoenas to obtain materials from certain Privacy Shield participants to check to check for substantive violations of the Privacy Shield obligations ⁽¹⁰⁰⁾.

⁽⁹¹⁾ An EU-U.S. DPF organisation has to publicly declare its commitment to comply with the Principles, disclose its privacy policies in line with these Principles and fully implement them. Failure to comply is enforceable under Section 5 of the FTC Act prohibiting unfair and deceptive acts in or affecting commerce (15 U.S.C. §45) and 49 U.S.C. §41712 prohibiting a carrier or ticket agent from engaging in an unfair or deceptive practice in air transportation or the sale of air transportation.

⁽⁹²⁾ 15 U.S.C. § 41.

⁽⁹³⁾ Annex IV.

⁽⁹⁴⁾ According to information from the FTC, it has no power to conduct on-site inspections in the area of privacy protection. However, it has the power to compel organisations to produce documents and provide witness statements (see Section 20 of the FTC Act), and may use the court system to enforce such orders in case of non-compliance.

⁽⁹⁵⁾ See Annex IV, section ‘Seeking and Monitoring Orders’.

⁽⁹⁶⁾ FTC or court orders may require companies to implement privacy programs and to regularly make compliance reports or independent third-party assessments of those programs available to the FTC.

⁽⁹⁷⁾ Annex IV, section ‘Seeking and Monitoring Orders’.

⁽⁹⁸⁾ Commission SWD (2019) 495 final, p. 11.

⁽⁹⁹⁾ See the cases listed on the FTC’s website, available via <https://www.ftc.gov/business-guidance/privacy-security/privacy-shield>. See also Commission SWD (2017) 344 final, p.17; Commission SWD (2018) 497 final, p. 12 and Commission SWD (2019) 495 final, p. 11.

⁽¹⁰⁰⁾ See e.g. see Prepared Remarks of Chairman Joseph Simons at the Second Privacy Shield Annual Review (ftc.gov).

- (63) More generally, the FTC has in the past years taken enforcement action in a number of cases concerning compliance with specific data protection requirements that are also provided under the EU-U.S. DPF, e.g. as regards the principles of purpose limitation and data retention ⁽¹⁰¹⁾, data minimisation ⁽¹⁰²⁾, data security ⁽¹⁰³⁾ and data accuracy ⁽¹⁰⁴⁾.
- (64) The DoT has exclusive authority to regulate the privacy practices of airlines, and shares jurisdiction with the FTC with respect to the privacy practices of ticket agents in the sale of air transportation. DoT officers first aim at reaching a settlement and, if this is not possible, may initiate enforcement proceedings involving an evidentiary hearing before a DoT administrative law judge who has the authority to issue cease-and-desist orders and civil penalties ⁽¹⁰⁵⁾. Administrative law judges benefit from several protections under the Administrative Procedure Act (APA) to ensure their independence and impartiality. For example, they can only be dismissed for good cause; are assigned to cases in rotation; may not perform duties inconsistent with their duties and responsibilities as administrative law judges; are not subject to supervision by the investigative team of the authority they are employed by (in this case the DoT); and must conduct their adjudicative/enforcement function impartially ⁽¹⁰⁶⁾. The DoT has committed to monitor enforcement orders and ensure that orders resulting from EU-U.S. DPF cases are available on its website ⁽¹⁰⁷⁾.

2.4. Redress

- (65) In order to ensure adequate protection and in particular the enforcement of individual rights, the data subject should be provided with effective administrative and judicial redress.
- (66) The EU-U.S. DPF, through the *Recourse, Enforcement and Liability Principle*, requires organisations to provide recourse for individuals who are affected by non-compliance and thus the possibility for Union data subjects to lodge complaints regarding non-compliance by EU-U.S. DPF organisations and to have these complaints resolved, if necessary by a decision providing an effective remedy ⁽¹⁰⁸⁾. As part of their certification, organisations must satisfy the requirements of this Principle by providing for effective and readily available independent recourse mechanisms by which each individual's complaints and disputes can be investigated and expeditiously resolved at no cost to the individual ⁽¹⁰⁹⁾.

⁽¹⁰¹⁾ See e.g. the FTC's order in Drizly, LLC., inter alia requiring the company (1) to destroy any personal data it collected that is not necessary for it to provide products or services to consumers, (2) refrain from collecting or storing personal information unless it is necessary for specific purposes outlined in a retention schedule.

⁽¹⁰²⁾ See e.g. the FTC order in CafePress (24 March 2022) requiring inter alia to minimize the amount of data that is collected.

⁽¹⁰³⁾ See e.g. the FTC's enforcement action in Drizzly, LLC and CafePress, where it required the relevant companies to put in place a dedicated security program or specific security measures. In addition, as regards data breaches, see also the FTC order of 27 January 2023 in Chegg, the settlement reached with Equifax in 2019 (<https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach>)

⁽¹⁰⁴⁾ See e.g. the case of RealPage, Inc (16 October 2018), where the FTC took enforcement action under the FCRA against a tenant screening company that provided background reports on individuals to property owners and property management companies, based on information from rental histories, public record information (including criminal and eviction histories) and credit information, which were used as a factor in determining eligibility for housing. The FTC found that the company did not take reasonable measures to ensure the accuracy of the information that it provided on the basis of its auto-decision tool.

⁽¹⁰⁵⁾ See Annex V, section 'Enforcement Practices'.

⁽¹⁰⁶⁾ See 5 U.S.C. §§ 3105, 7521(a), 554(d) and 556(b)(3).

⁽¹⁰⁷⁾ Annex V, see section 'Monitoring and Making Public Enforcement Orders Concerning EU-U.S. DPF Violations'.

⁽¹⁰⁸⁾ Annex I, Section II.7.

⁽¹⁰⁹⁾ Annex I, Section III.11.

- (67) Organisations may choose independent recourse mechanisms in either the Union or in the United States. As explained in more detail in recital 73, this includes the possibility to voluntarily commit to cooperate with the EU DPAs. Where organisations process human resources data, such commitment to cooperate with EU DPAs is mandatory. Other alternatives include independent alternative dispute resolution or private-sector developed privacy programs that incorporate the Principles into their rules. The latter must include effective enforcement mechanisms in accordance with the requirements of the *Recourse, Enforcement and Liability Principle*.
- (68) Consequently, the EU-U.S. DPF provides data subjects with a number of possibilities to enforce their rights, lodge complaints regarding non-compliance by EU-U.S. organisations and to have their complaints resolved, if necessary by a decision providing an effective remedy. Individuals can bring a complaint directly to an organisation, to an independent dispute resolution body designated by the organisation, to national DPAs, the DoC or to the FTC. In cases where their complaints have not been resolved by any of these recourse or enforcement mechanisms, individuals also have a right to invoke binding arbitration (Annex I of Annex I to this Decision). Except for the arbitral panel, which requires certain remedies to be exhausted before it can be invoked, individuals are free to pursue any or all of the redress mechanisms of their choice, and are not obliged to choose one mechanism over the other or to follow a specific sequence.
- (69) Firstly, Union data subjects may pursue cases of non-compliance with the Principles through direct contacts with the EU-U.S. DPF organisations ⁽¹¹⁰⁾. To facilitate resolution, the organisation must put in place an effective redress mechanism to deal with such complaints. An organisation's privacy policy must therefore clearly inform individuals about a contact point, either within or outside the organisation, that will handle complaints (including any relevant establishment in the Union that can respond to inquiries or complaints), as well as on the designated independent dispute resolution body (see recital 70). Upon receipt of an individual's complaint, directly from the individual or through the DoC following referral by a DPA, the organisation must provide a response to the Union data subject within a period of 45 days ⁽¹¹¹⁾. Likewise, organisations are required to respond promptly to inquiries and other requests for information from the DoC or from a DPA ⁽¹¹²⁾ (where the organisation has committed to cooperate with the DPA) relating to their adherence to the Principles.
- (70) Secondly, individuals can also bring a complaint directly to the independent dispute resolution body (either in the United States or in the Union) designated by an organisation to investigate and resolve individual complaints (unless they are obviously unfounded or frivolous) and to provide appropriate recourse free of charge to the individual ⁽¹¹³⁾. Sanctions and remedies imposed by such a body must be sufficiently rigorous to ensure compliance by organisations with the Principles and should provide for a reversal or correction by the organisation of the effects of non-compliance and, depending on the circumstances, the termination of the further processing of the personal data at stake and/or their deletion, as well as publicity for findings of non-compliance ⁽¹¹⁴⁾. Independent dispute resolution bodies designated by an organisation are required to include on their public websites relevant information regarding the EU-U.S. DPF and the services they provide under it ⁽¹¹⁵⁾. Each year, they must publish an annual report providing aggregate statistics regarding these services ⁽¹¹⁶⁾.

⁽¹¹⁰⁾ Annex I, Section III.11.d.(i).

⁽¹¹¹⁾ Annex I, Section III.11.d.(i).

⁽¹¹²⁾ This is the handling authority designated by the panel of DPAs provided for in the Supplemental Principle on 'The Role of the Data Protection Authorities' (Annex I, Section III.5).

⁽¹¹³⁾ Annex I, Section III.11.d.

⁽¹¹⁴⁾ Annex I, Section II.7 and III.11.e.

⁽¹¹⁵⁾ Annex I, Section III.11.d.(ii).

⁽¹¹⁶⁾ The annual report must include: (1) the total number of EU-U.S. DPF-related complaints received during the reporting year; (2) the types of complaints received; (3) dispute resolution quality measures, such as the length of time taken to process complaints; and (4) the outcomes of the complaints received, notably the number and types of remedies or sanctions imposed.

- (71) As part of its compliance review procedures, the DoC may verify that EU-U.S. DPF organisations are actually registered with the independent recourse mechanisms they claim they are registered with ⁽¹¹⁷⁾. Both the organisations and the responsible independent recourse mechanisms are required to respond promptly to inquiries and requests by the DoC for information relating to the EU-U.S. DPF. The DoC will work with independent recourse mechanisms to verify that they include information on their websites regarding the Principles and the services they provide under the EU-U.S. DPF and that they publish annual reports ⁽¹¹⁸⁾.
- (72) In cases where the organisation fails to comply with the ruling of a dispute resolution or self-regulatory body, the latter must notify such non-compliance to the DoC and the FTC (or another U.S. authority with jurisdiction to investigate non-compliance by the organisation), or a competent court ⁽¹¹⁹⁾. If an organisation refuses to comply with a final determination by any privacy self-regulatory, independent dispute resolution or government body, or where such a body determines that an organisation frequently fails to comply with the Principles, this may be considered as a persistent failure to comply with the result that the DoC, after first providing 30 days' notice and an opportunity to respond to the organisation that has failed to comply, will strike the organisation off the DPF List ⁽¹²⁰⁾. If, after removal from the list, the organisation continues to make the claim of EU-U.S. DPF certification, the DoC will refer it to the FTC or other enforcement agency ⁽¹²¹⁾.
- (73) Thirdly, individuals may also bring their complaints to a national DPA in the Union, which may make use of their investigatory and remedial powers under Regulation (EU) 2016/679. Organisations are obliged to cooperate in the investigation and the resolution of a complaint by a DPA either when it concerns the processing of human resources data collected in the context of an employment relationship or when the respective organisation has voluntarily submitted to the oversight by DPAs ⁽¹²²⁾. Notably, organisations have to respond to inquiries, comply with the advice given by the DPA, including for remedial or compensatory measures, and provide the DPA with written confirmation that such action has been taken ⁽¹²³⁾. In cases of non-compliance with the advice given by the DPA, the DPA will refer such cases to the DoC (which may remove organisations from the EU-U.S. DPF list) or, for possible enforcement action, to the FTC or the DoT (failure to cooperate with the DPAs or to comply with the Principles is actionable under U.S. law) ⁽¹²⁴⁾.
- (74) To facilitate cooperation for an effective handling of complaints, both the DoC and the FTC have put in place a dedicated point of contact that is responsible for liaising directly with DPAs ⁽¹²⁵⁾. Those points of contact assist with DPA enquiries regarding an organisation's compliance with the Principles.
- (75) The advice provided by the DPAs ⁽¹²⁶⁾ is issued after both sides in the dispute have had a reasonable opportunity to comment and to provide any evidence they wish. The panel may deliver advice as quickly as the requirement for due process allows, and as a general rule within 60 days after receiving a complaint ⁽¹²⁷⁾. If an organisation fails to comply within 25 days of delivery of the advice and has offered no satisfactory explanation for the delay, the panel may give notice of its intention either to submit the matter to the FTC (or other competent U.S. enforcement authority), or to conclude that the commitment to cooperate has been seriously breached. In the first alternative,

⁽¹¹⁷⁾ Annex I, Section 'Verify Self-Certification Requirements'.

⁽¹¹⁸⁾ See Annex III, section 'Facilitate Cooperation with Alternative Dispute Resolution Bodies That Provide Principles-Related Services'. See also Annex I, Section III.11.d.(ii)-(iii).

⁽¹¹⁹⁾ See Annex I, Section III.11.e.

⁽¹²⁰⁾ See Annex I, Section III.11.g, in particular points (ii) and (iii).

⁽¹²¹⁾ See Annex III, section on 'Search for and Address False Claims of Participation'.

⁽¹²²⁾ Annex I, Section II.7.b.

⁽¹²³⁾ Annex I, Section III.5.

⁽¹²⁴⁾ Annex I, Section III.5.c.(ii).

⁽¹²⁵⁾ Annex III (see section 'Facilitate Cooperation with DPAs') and Annex IV (see sections 'Referral Prioritization and Investigation' and 'Enforcement Cooperation with EU DPAs').

⁽¹²⁶⁾ The rules of procedure of the informal DPA panel should be established by the DPAs based on their competence to organise their work and cooperate among each other.

⁽¹²⁷⁾ Annex I, Section III.5.c.(i).

this may lead to enforcement action based on Section 5 of the FTC Act (or similar statute) ⁽¹²⁸⁾. In the second alternative, the panel will inform the DoC which will consider the organisation's refusal to comply with the advice of the DPA panel as a persistent failure to comply that will lead to the organisation's removal from the DPF List.

- (76) If the DPA to which the complaint has been addressed has taken no or insufficient action to address a complaint, the individual complainant has the possibility to challenge such (in-)action in the national courts of the respective EU Member State.

- (77) Individuals may also bring complaints to DPAs even when the DPA panel has not been designated as an organisation's dispute resolution body. In these cases, the DPA may refer such complaints either to the DoC or the FTC. In order to facilitate and increase cooperation on matters relating to individual complaints and non-compliance by EU-U.S. DPF organisations, the DoC will establish a dedicated contact point to act as a liaison and to assist with DPA inquiries regarding an organisation's compliance with the Principles ⁽¹²⁹⁾. Likewise, the FTC has committed to establish a dedicated point of contact ⁽¹³⁰⁾.

- (78) Fourthly, the DoC has committed to receive, review and undertake best efforts to resolve complaints about an organisation's non-compliance with the Principles ⁽¹³¹⁾. To this end, the DoC provides special procedures for DPAs to refer complaints to a dedicated contact point, track them and follow up with organisations to facilitate resolution ⁽¹³²⁾. In order to expedite the processing of individual complaints, the contact point liaises directly with the respective DPA on compliance issues and in particular updates it on the status of complaints within a period of not more than 90 days following referral ⁽¹³³⁾. This allows data subjects to bring complaints of non-compliance by EU-U.S. DPF organisations directly to their national DPA and have them channelled to the DoC as the U.S. authority administering the EU-U.S. DPF.

- (79) Where, on the basis of its ex officio verifications, complaints or any other information, the DoC concludes that an organisation has persistently failed to comply with the Principles it may remove such an organisation from the DPF list ⁽¹³⁴⁾. Refusal to comply with a final determination by any privacy self-regulatory, independent dispute resolution or government body, including a DPA, will be regarded as a persistent failure to comply ⁽¹³⁵⁾.

- (80) Fifthly, an EU-U.S. DPF organisation must be subject to the jurisdiction of U.S. authorities, in particular the FTC ⁽¹³⁶⁾, which have the necessary investigatory and enforcement powers to effectively ensure compliance with the Principles. The FTC gives priority consideration to referrals of non-compliance with the Principles received from independent dispute resolution or self-regulatory bodies, the DoC and DPAs (acting on their own initiative or upon complaints) to determine whether Section 5 of the FTC Act has been violated ⁽¹³⁷⁾. The FTC has committed to create a standardised referral process, to designate a point of contact at the agency for DPA referrals, and to exchange information on referrals. In addition, it may accept complaints directly from individuals and undertake EU-U.S. DPF investigations on its own initiative, in particular as part of its wider investigation of privacy issues.

⁽¹²⁸⁾ Annex I, Section III.5.c.(ii).

⁽¹²⁹⁾ See Annex III, section 'Facilitate Cooperation with DPAs'.

⁽¹³⁰⁾ See Annex IV, sections 'Referral Prioritization and Investigation' and 'Enforcement Cooperation with EU DPAs'.

⁽¹³¹⁾ Annex III, see e.g. section 'Facilitate Cooperation with DPAs'.

⁽¹³²⁾ Annex I, Section II.7.e and Annex III, section 'Facilitate Cooperation with DPAs'.

⁽¹³³⁾ *Ibid.*

⁽¹³⁴⁾ Annex I, Section III.11.g.

⁽¹³⁵⁾ Annex I, Section III.11.g.

⁽¹³⁶⁾ An EU-U.S. DPF organisation has to publicly declare its commitment to comply with the Principles, publicly disclose its privacy policies in line with these Principles and fully implement them. Failure to comply is enforceable under Section 5 of the FTC Act prohibiting unfair and deceptive acts in or affecting commerce.

⁽¹³⁷⁾ See also the similar commitments undertaken by the DoT, Annex V.

- (81) Sixthly, as a recourse mechanism of 'last resort' in case none of the other available redress avenues has satisfactorily resolved an individual's complaint, the Union data subject may invoke binding arbitration by the 'EU-U.S. Data Privacy Framework Panel' (EU-U.S. DPF Panel) ⁽¹³⁸⁾. Organisations must inform individuals about their possibility to invoke binding arbitration and they are obliged to respond once an individual has invoked this option by delivering notice to the concerned organisation ⁽¹³⁹⁾.
- (82) This EU-U.S. DPF Panel consists of a pool of at least ten arbitrators that will be designated by the DoC and the Commission based on their independence, integrity, as well as experience in U.S. privacy and Union data protection law. For each individual dispute, the parties select from this pool a panel of one or three ⁽¹⁴⁰⁾ arbitrators.
- (83) The International Centre for Dispute Resolution (ICDR), the international division of the American Arbitration Association (AAA), was selected by the DoC to administer arbitrations. Proceedings before the EU-U.S. DPF Panel will be governed by a set of agreed arbitration rules and a code of conduct for appointed arbitrators. The ICDR-AAA website provides clear and concise information to individuals about the arbitration mechanism and the procedure to file for arbitration.
- (84) The arbitration rules agreed between the DoC and the Commission supplement the EU-U.S. DPF which contains several features which enhance the accessibility of this mechanism for Union data subjects: (i) in preparing a claim before the panel, the data subject may be assisted by his or her national DPA; (ii) while the arbitration will take place in the United States, Union data subjects may choose to participate through video or telephone conference, to be provided at no cost to the individual; (iii) while the language used in the arbitration will as a rule be English, interpretation at the arbitral hearing and translation will in principle be provided upon a reasoned request and at no cost to the data subject; (iv) finally, while each party has to bear its own attorney's fees, if represented by an attorney before the panel, the DoC will maintain a fund supplied with annual contributions by the EU-U.S. DPF organisations, which are to cover the costs of the arbitration procedure up to maximum amounts to be determined by the U.S. authorities in consultation with the Commission ⁽¹⁴¹⁾.
- (85) The EU-U.S. DPF Panel has the authority to impose individual-specific, non-monetary equitable relief ⁽¹⁴²⁾ necessary to remedy non-compliance with the Principles. While the panel takes into account other remedies already obtained by other EU-U.S. DPF mechanisms when making its determination, individuals may still resort to arbitration if they consider these other remedies to be insufficient. This allows Union data subjects to invoke arbitration in all cases where the action or inaction of EU-U.S. DPF organisations, independent recourse mechanisms or the competent U.S. authorities (for instance the FTC) has not satisfactorily resolved their complaints. Arbitration may not be invoked if a DPA has the legal authority to resolve the claim at issue with respect to the EU-U.S. DPF organisation, namely in those cases where the organisation is either obliged to cooperate and comply with the advice of the DPAs as regards the processing of human resources data collected in the employment context, or has voluntarily committed to do so. Individuals can enforce the arbitration decision in the U.S. courts under the Federal Arbitration Act, thereby ensuring a legal remedy in case an organisation fails to comply.

⁽¹³⁸⁾ See Annex I, Annex I 'Arbitral Model'.

⁽¹³⁹⁾ See Annex I, Section II.1.a.(xi) and II.7.c.

⁽¹⁴⁰⁾ The number of arbitrators on the panel will have to be agreed between the parties.

⁽¹⁴¹⁾ Annex I of Annex I, Section G.6.

⁽¹⁴²⁾ Individuals may not claim damages in arbitration, but invoking arbitration does not foreclose the option to seek damages in the ordinary U.S. courts.

- (86) Seventh, where an organisation does not comply with its commitment to respect the Principles and published privacy policy, additional avenues for judicial redress are available under U.S. law, including to obtain compensation for damages. For example, individuals can under certain conditions obtain judicial redress (including compensation for damages) under State consumer laws in cases of fraudulent misrepresentation, unfair or deceptive acts or practices ⁽¹⁴³⁾, and under tort law (in particular under the torts of intrusion upon seclusion ⁽¹⁴⁴⁾, appropriation of name or likeness ⁽¹⁴⁵⁾ and public disclosure of private facts ⁽¹⁴⁶⁾).
- (87) Together, the various redress avenues described above ensure that each complaint regarding non-compliance with the EU-U.S DPF by certified organisations will be effectively adjudicated and remedied.

3. ACCESS AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN THE UNITED STATES

- (88) The Commission also assessed the limitations and safeguards, including the oversight and individual redress mechanisms available in United States law as regards the collection and subsequent use by U.S. public authorities of personal data transferred to controllers and processors in the U.S. in the public interest, in particular for criminal law enforcement and national security purposes (government access) ⁽¹⁴⁷⁾. In assessing whether the conditions under which government access to data transferred to the United States under this Decision fulfil the 'essential equivalence' test pursuant to Article 45(1) of Regulation (EU) 2016/679, as interpreted by the Court of Justice in light of the Charter of Fundamental Rights, the Commission took into account several criteria.
- (89) In particular, any limitation to the right to the protection of personal data must be provided for by law and the legal basis which permits the interference with such a right must itself define the scope of the limitation to the exercise of the right concerned ⁽¹⁴⁸⁾. In addition, in order to satisfy the requirement of proportionality, according to which derogations from and limitations to the protection of personal data must apply only in so far as is strictly necessary in a democratic society to meet specific objectives of general interest equivalent to those recognized by the Union, this legal basis must lay down clear and precise rules governing the scope and application of the measures in question and impose minimum safeguards so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse ⁽¹⁴⁹⁾. Moreover, these rules and

⁽¹⁴³⁾ See e.g. state consumer protection laws in California (Cal. Civ. Code §§ 1750 - 1785 (West) Consumers Legal Remedies Act); District of Columbia (D.C. Code §§ 28-3901); Florida (Fla. Stat. §§ 501.201 - 501.213, Deceptive and Unfair Trade Practices Act); Illinois (815 Ill. Comp. Stat. 505/1 - 505/12, Consumer Fraud and Deceptive Business Practices Act); Pennsylvania (73 Pa. Stat. Ann. §§ 201-1 - 201-9.3 (West) Unfair Trade Practices and Consumer Protection Law).

⁽¹⁴⁴⁾ I.e. in case of an intentional interference with an individual's private affairs or concerns, in a way that would be highly offensive to a reasonable person (Restatement (2nd) of Torts, §652(b)).

⁽¹⁴⁵⁾ This tort commonly applies in case of the appropriation and use of an individual's name or likeness to advertise a business or product, or for some similar commercial purpose (see Restatement (2nd) of Torts, §652C).

⁽¹⁴⁶⁾ I.e. when information concerning the private life of an individual is made public, where this is highly offensive to a reasonable person and the information is not of legitimate concern to the public (Restatement (2nd) of Torts, §652D).

⁽¹⁴⁷⁾ This is also relevant in light of Section I.5 of Annex I. Pursuant to this Section and similarly to the GDPR, compliance with data protection requirements and rights that are part of the Privacy Principles can be subject to limitations. However, such limitations are not absolute, but can only be relied on under several conditions, for example to the extent necessary to comply with a court order or meet public interest, law enforcement, or national security requirements. In this context and for the sake of clarity, this Section also refers to the conditions set out in EO 14086 that are assessed inter alia in recitals 127-141.

⁽¹⁴⁸⁾ See *Schrems II*, paragraphs 174-175 and the case-law cited. See also, as regards access by public authorities of Member States, Case C-623/17 *Privacy International* ECLI:EU:C:2020:790, paragraph 65; and Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others* ECLI:EU:C:2020:791, paragraph 175.

⁽¹⁴⁹⁾ See *Schrems II*, paragraphs 176 and 181, as well as the case-law cited. See also, as regards access by public authorities of Member States, *Privacy International*, paragraph 68; and *La Quadrature du Net and Others*, paragraph 132.

safeguards must be legally binding and enforceable by individuals ⁽¹⁵⁰⁾. In particular, data subjects must have the possibility of bringing legal action before an independent and impartial tribunal in order to have access to their personal data, or to obtain the rectification or erasure of such data ⁽¹⁵¹⁾.

3.1. Access and use by U.S. public authorities for criminal law enforcement purposes

- (90) As regards interference with personal data transferred under the EU-U.S. DPF for criminal law enforcement purposes, the law of the United States imposes a number of limitations on the access and use of personal data, and provides oversight and redress mechanisms which are in line with the requirements referred to in recital 89 of this Decision. The conditions under which such access can take place and the safeguards applicable to the use of those powers are assessed in detail in the following sections. In this respect, the U.S. government (through the Department of Justice, DoJ) has also provided assurances on the applicable limitations and safeguards (Annex VI to this Decision).

3.1.1. Legal bases, limitations and safeguards

3.1.1.1. Limitations and safeguards as regards the collection of personal data for criminal law enforcement purposes

- (91) Personal data processed by certified U.S. organisations that would be transferred from the Union on the basis of the EU-U.S. DPF may be accessed for criminal law enforcement purposes by U.S. federal prosecutors and federal investigative agents under different procedures, as explained in more detail in recitals 92-99. These procedures apply in the same way when information is obtained from any U.S. organisation, regardless of the nationality or place of residence of the concerned data subjects ⁽¹⁵²⁾.
- (92) Firstly, upon request of a federal law enforcement officer or an attorney for the government, a judge may issue a warrant for a search or seizure (including of electronically stored information) ⁽¹⁵³⁾. Such a warrant may only be issued if there is 'probable cause' ⁽¹⁵⁴⁾ that 'seizable items' (evidence of a crime, illegally possessed items, or property designed or intended for use or used in committing a crime) are likely to be found in the place specified by the warrant. The warrant must identify the property or item to be seized and designate the judge to which the warrant must be returned. A person subject to a search or whose property is subject to a search may move to suppress

⁽¹⁵⁰⁾ See *Schrems II*, paragraphs 181-182.

⁽¹⁵¹⁾ See *Schrems I*, paragraph 95 and *Schrems II*, paragraph 194. In that respect, the CJEU has notably stressed that compliance with Article 47 of the Charter of Fundamental Rights, guaranteeing the right to an effective remedy before an independent and impartial tribunal, "contributes to the required level of protection in the European Union [and] must be determined by the Commission before it adopts an adequacy decision pursuant to Article 45(1) of Regulation (EU) 2016/679" (*Schrems II*, paragraph 186).

⁽¹⁵²⁾ See Annex VI. See for instance, with respect to the Wiretap Act, Stored Communications Act and Pen Register Act (mentioned in more detail in recital 95-98), *Suzlon Energy Ltd v. Microsoft Corp.*, 671 F.3d 726, 729 (9th Cir. 2011).

⁽¹⁵³⁾ Federal Rules of Criminal Procedure, 41. In a 2018 judgment, the Supreme Court confirmed that a search warrant or warrant exception is also required for law enforcement authorities to access historical cell site location records, that provide a comprehensive overview of a user's movements and that the user can have a reasonable expectation of privacy with respect to such information (*Timothy Ivory Carpenter v. United States of America*, No. 16-402, 585 U.S. (2018)). As a result, such data generally cannot be obtained from a cellular company on the basis of a court order on the basis of reasonable grounds to believe that the information is relevant and material to an ongoing criminal investigation, but requires showing the existence of probable cause when a warrant is used.

⁽¹⁵⁴⁾ According to the Supreme Court, 'probable cause' is a "practical, non-technical" standard that calls upon the "factual and practical considerations of everyday life on which reasonable and prudent men [...] act" (*Illinois v. Gates*, 462 U.S. 213, 232 (1983)). As regards search warrants, probable cause exists when there is a fair probability that a search will result in evidence of a crime being discovered (id).

evidence obtained or derived from an unlawful search if that evidence is introduced against that person during a criminal trial ⁽¹⁵⁵⁾. When a data holder (e.g. a company) is required to disclose data pursuant to a warrant, it may notably challenge the requirement to disclose as unduly burdensome ⁽¹⁵⁶⁾.

- (93) Secondly, a subpoena may be issued by a grand jury (an investigative arm of the court impanelled by a judge or magistrate) in the context of investigations of certain serious crimes ⁽¹⁵⁷⁾, usually at the request of a federal prosecutor, to require someone to produce or make available business records, electronically stored information, or other tangible items. In addition, different statutes authorise the use of administrative subpoenas to produce or make available business records, electronically stored information, or other tangible items in investigations involving health care fraud, child abuse, Secret Service protection, controlled substance cases, and Inspector General investigations ⁽¹⁵⁸⁾. In both cases, the information must be relevant to the investigation and the subpoena cannot be unreasonable, i.e. overbroad, oppressive or burdensome (and can be challenged by the recipient of the subpoena on those grounds) ⁽¹⁵⁹⁾.
- (94) Very similar conditions apply to administrative subpoenas issued to seek access to data held by companies in the US for civil or regulatory (“public interest”) purposes. The authority of agencies with civil and regulatory responsibilities to issue such administrative subpoenas must be established in statute. The use of an administrative subpoena is subject to a “reasonableness test”, which requires that the investigation is conducted pursuant to a legitimate purpose, the information requested under the subpoena is relevant to that purpose, the agency does not already have the information it is seeking with the subpoena, and the necessary administrative steps to issue the subpoena have been followed ⁽¹⁶⁰⁾. Case law of the Supreme Court has also clarified the need to balance the importance of the public interest in the information being requested with the importance of personal and organisational privacy interests ⁽¹⁶¹⁾. While the use of an administrative subpoena is not subject to prior judicial approval, it becomes subject to judicial review in case of a challenge by the recipient on the above-mentioned grounds, or if the issuing agency seeks to enforce the subpoena in court ⁽¹⁶²⁾. In addition to these general overarching limitations, specific (stricter) requirements may follow from individual statutes ⁽¹⁶³⁾.

⁽¹⁵⁵⁾ *Mapp v. Ohio*, 367 U.S. 643 (1961).

⁽¹⁵⁶⁾ See *In re Application of United States*, 610 F.2d 1148, 1157 (3d Cir. 1979) (holding that “due process requires a hearing on the issue of burdensomeness before compelling a telephone company to provide” assistance with a search warrant) and *In re Application of United States*, 616 F.2d 1122 (9th Cir. 1980).

⁽¹⁵⁷⁾ The Fifth Amendment to the U.S. Constitution requires grand jury indictment for any “capital or otherwise infamous crime.” The grand jury consists of 16 to 23 members, and determines whether probable cause exists to believe a crime has been committed. To reach this conclusion, grand juries are vested with investigative powers that allow them to issue subpoenas.

⁽¹⁵⁸⁾ See Annex VI.

⁽¹⁵⁹⁾ Federal Rules of Criminal Procedure, 17.

⁽¹⁶⁰⁾ *United States v. Powell*, 379 U.S. 48 (1964).

⁽¹⁶¹⁾ *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186 (1946).

⁽¹⁶²⁾ The Supreme Court has clarified that, in case of a challenge of an administrative subpoena, a court must consider whether (1) the investigation is for a lawfully authorized purpose, (2) the subpoena authority at issue is within the power of Congress to command, and (3) the “documents sought are relevant to the inquiry.” The Court also noted that an administrative subpoena request must be “reasonable”, i.e. requiring “specification of the documents to be produced adequate, but not excessive, for the purposes of the relevant inquiry,” including “particularity in ‘describing the place to be searched, and the persons or things to be seized.’”

⁽¹⁶³⁾ For example, the Right to Financial Privacy Act provides a government authority with the power to obtain financial records held by a financial institution pursuant to an administrative subpoena only if (1) there is reason to believe that the records sought are relevant to a legitimate law enforcement inquiry and (2) a copy of the subpoena or summons has been provided to the customer together with a notice stating with reasonable specificity the nature of the inquiry (12 U.S.C. §3405). Another example is the Fair Credit Reporting Act, which prohibits consumer reporting agencies from disclosing consumer reports in response to administrative subpoena requests (and only allows them to respond to grand jury subpoena requests or court orders, 15 U.S.C. §1681 et seq.). As regards access to communication information, the specific requirements of the Stored Communications Act apply, including with respect to the possibility to use administrative subpoenas (see recitals 96-97 for a detailed overview).

- (95) Thirdly, several legal bases enable criminal law enforcement authorities to obtain access to communications data. A court may issue an order authorising the collection of real-time, non-content dialling, routing, addressing and signalling information about a phone number or e-mail (through the use of a pen register or trap and trace device), if it finds that the authority has certified that the information likely to be obtained is relevant to a pending criminal investigation ⁽¹⁶⁴⁾. The order must, inter alia, specify the identity, if known, of the suspect; the attributes of the communications to which it applies and a statement of the offense to which the information to be collected relates. The use of a pen register or trap and trace device may be authorised for a maximum period of sixty days, which may only be extended by a new court order.
- (96) In addition, access for criminal law enforcement purposes to subscriber information, traffic data and stored content of communications held by internet service providers, telephone companies, and other third party service providers may be obtained on the basis of the Stored Communications Act ⁽¹⁶⁵⁾. To obtain the stored content of electronic communications, criminal law enforcement authorities must in principle obtain a warrant from a judge based on probable cause to believe that the account in question contains evidence of a crime ⁽¹⁶⁶⁾. For subscriber registration information, IP addresses and associated time stamps, and billing information, criminal law enforcement authorities may use a subpoena. For most other stored, non-content information, such as e-mail headers without the subject line, a criminal law enforcement authority must obtain a court order, which will be issued if the judge is satisfied that there are reasonable grounds to believe that the requested information is relevant and material to an ongoing criminal investigation.
- (97) Providers that receive requests under the Stored Communications Act may voluntarily notify a customer or subscriber whose information is sought, except when the relevant criminal law enforcement authority obtains a protective order prohibiting such notification ⁽¹⁶⁷⁾. Such a protective order is a court order requiring a provider of electronic communications services or remote computing services to whom a warrant, subpoena or court order is directed, not to notify any other person of the existence of the warrant, subpoena or court order, for as long as the court deems appropriate. Protective orders are granted if a court finds that there is reason to believe that notification would seriously jeopardise an investigation or unduly delay a trial, e.g. because it would result in endangering the life or physical safety of an individual, flight from prosecution, intimidation of potential witnesses, etc. A Deputy Attorney General memorandum (which is binding on all DoJ attorneys and agents) requires prosecutors to make a detailed determination regarding the need for a protective order and provide a justification to the court on how the statutory criteria for obtaining a protective order are met in the specific case ⁽¹⁶⁸⁾. The memorandum also requires that applications for protective orders must generally not seek to delay notification for more than one year. Where, in exceptional circumstances, orders of longer duration might be necessary, such orders may only be sought with the written agreement of a supervisor designated by the U.S. Attorney or the appropriate Assistant Attorney General. In addition, a prosecutor must, when closing an investigation, immediately assess whether there is a basis to maintain any outstanding protective orders and, where this is not the case, terminate the protective order and ensure the service provider is notified thereof ⁽¹⁶⁹⁾.

⁽¹⁶⁴⁾ 18 U.S.C. § 3123.

⁽¹⁶⁵⁾ 18 U.S.C. §§ 2701-2713.

⁽¹⁶⁶⁾ 18 U.S.C. §§ 2701(a)-(b)(1)(A). If the concerned subscriber or customer is notified (either in advance or, in certain circumstances, through a delayed notification), the content information stored for longer than 180 days may also be obtained on the basis of an administrative subpoena or grand jury subpoena (18 U.S.C. §§ 2701(b)(1)(B)) or a court order (if there are reasonable grounds to believe that the information relevant and material to an ongoing criminal investigation (18 U.S.C. §§ 2701(d)). However, in accordance with a federal appeals court ruling, government investigators generally obtain search warrants from judges in order to collect the contents of private communication or stored data from a commercial communications service provider. *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

⁽¹⁶⁷⁾ 18 U.S.C. § 2705(b).

⁽¹⁶⁸⁾ See the Memorandum issued by Deputy Attorney General Rod Rosenstein on 19 October 2017 on a more restrictive policy on applications for protective (or non-disclosure) orders, available at <https://www.justice.gov/criminal-ccips/page/file/1005791/download>.

⁽¹⁶⁹⁾ Memorandum issued by Deputy Attorney General Lisa Moncao on 27 May 2022 on a supplemental policy regarding applications for protective orders pursuant to 18 U.S.C. § 2705(b).

- (98) Criminal law enforcement authorities may also intercept in real time wire, oral or electronic communications on the basis of a court order in which a judge finds, inter alia, that there is probable cause to believe that the wiretap or electronic interception will produce evidence of a federal crime, or the whereabouts of a fugitive fleeing from prosecution ⁽¹⁷⁰⁾.
- (99) Further protections are provided by various Department of Justice policies and guidelines, including the Attorney General Guidelines for Domestic FBI Operations (AGG-DOM), which, inter alia require that the Federal Bureau of Investigation (FBI) uses the least intrusive investigative methods feasible, taking into account the effect on privacy and civil liberties ⁽¹⁷¹⁾.
- (100) According to the representations made by the U.S. government, the same or higher protections described above apply to law enforcement investigations at State level (with respect to investigations carried out under State laws) ⁽¹⁷²⁾. In particular, constitutional provisions, as well as statutes and case-law at State level reaffirm the above mentioned protections against unreasonable searches and seizures by requiring the issuance of a search warrant ⁽¹⁷³⁾. Similar to the protections afforded at the federal level, search warrants may be issued only upon a showing of probable cause and must describe the place to be searched and the person or thing to be seized ⁽¹⁷⁴⁾.

⁽¹⁷⁰⁾ 18 U.S.C. §§ 2510-2522.

⁽¹⁷¹⁾ Attorney General's Guidelines for Domestic Federal Bureau of Investigation (FBI) Operations (September 2008), available at <http://www.justice.gov/archive/opa/docs/guidelines.pdf>. Additional rules and policies that prescribe limitations on the investigative activities of federal prosecutors are set out in the United States Attorneys' Manual, available at <http://www.justice.gov/usam/united-states-attorneys-manual>. To depart from these Guidelines, prior approval must be obtained from the FBI's Director, Deputy Director or Executive Assistant Director designated by the Director, unless such approval cannot be obtained because of the immediacy or gravity of a threat to the safety of persons or property or to national security (in which case Director or other authorising person needs to be notified as soon as practicable). Where the Guidelines are not followed, the FBI must notify the DoJ thereof, who in turn informs the Attorney General and Deputy Attorney General.

⁽¹⁷²⁾ Annex VI, footnote 2. See also e.g., *Arnold v. City of Cleveland*, 67 Ohio St.3d 35, 616 N.E.2d 163, 169 (1993) ("In the areas of individual rights and civil liberties, the United States Constitution, where applicable to the states, provides a floor below which state court decisions may not fall"); *Cooper v. California*, 386 U.S. 58, 62, 87 S.Ct. 788, 17 L.Ed.2d 730 (1967) ("Our holding, of course, does not affect the State's power to impose higher standards on searches and seizures than required by the Federal Constitution if it chooses to do so."); *Petersen v. City of Mesa*, 63 P.3d 309, 312 (Ariz. Ct. App. 2003) ("Although the Arizona Constitution may impose stricter standards on searches and seizures than does the federal constitution, Arizona courts cannot provide less protection than does the Fourth Amendment").

⁽¹⁷³⁾ The majority of states have replicated the protections of the Fourth Amendment in their constitutions. See Alabama Const. art. I, § 5; Alaska Const. art. I, § 14; 1; Arkansas Const. art. II, § 15; California Const. art. I, § 13; Colorado Const. art. II, § 7; Connecticut Const. art. I, § 7; Delaware Const. art. I, § 6; Florida. Const. art. I, § 12; Georgia Const. art. I, § I, para. XIII; Hawai Const. art. I, § 7; Idaho Const. art. I, § 17; Illinois Const. art. I, § 6; Indiana Const. art. I, § 11; Iowa Const. art. I, § 8; Kansas Const. Bill of Rights, § 15; Kentucky Const. § 10; Louisiana Const. art. I, § 5; Maine Const. art. I, § 5; Massachusetts Const. Decl. of Rights art. 14; Michigan Const. art. I, § 11; Minnesota Const. art. I, § 10; Mississippi Const. art. III, § 23; Missouri Const. art. I, § 15; Montana Const. art. II, § 11; Nebraska Const. art. I, § 7; Nevad Const. art. I, § 18; New Hampshire Const. pt. 1, art. 19; N.J. Const. art. II, § 7; New Mexico Const. art. II, § 10; New York Const. art. I, § 12; North Dakota Const. art. I, § 8; Ohio Const. art. I, § 14; Oklahoma Const. art. II, § 30; Oregon Const. art. I, § 9; Pennsylvania Const. art. I, § 8; Rhode Island Const. art. I, § 6; South Carolina Const. art. I, § 10; South Dakota Const. art. VI, § 11; Tennessee Const. art. I, § 7; Texas Const. art. I, § 9; Utah Const. art. I, § 14; Vermont Const. ch. I, art. 11; West Virginia Const. art. III, § 6; Wisconsin Const. art. I, § 11; Wyoming Const. art. I, § 4. Others (e.g. Maryland, North Carolina and Virginia) have enshrined in their constitutions specific language concerning warrants that has been judicially interpreted to provide similar or higher protections to the Fourth Amendment (see Maryland. Decl. of Rts. art. 26; North Carolina Const. art. I, § 20; Virginia Const. art. I, § 10, and relevant case law, e.g. *Hamel v. State*, 943 A.2d 686, 701 (Md. Ct. Spec. App. 2008; *State v. Johnson*, 861 S.E.2d 474, 483 (N.C. 2021) and *Lowe v. Commonwealth*, 337 S.E.2d 273, 274 (Va. 1985)). Finally, Arizona and Washington have constitutional provisions that protect privacy more generally (Arizona Const. art. 2, § 8; Washington Const. art. I, § 7), which have been interpreted by courts as providing more protections than the Fourth Amendment (see e.g. *State v. Bolt*, 689 P.2d 519, 523 (Ariz. 1984), *State v. Ault*, 759 P.2d 1320, 1324 (Ariz. 1988), *State v. Myrick*, 102 Wn.2d 506, 511, 688 P.2d 151, 155 (1984) , *State v. Young*, 123 Wn.2d 173, 178, 867 P.2d 593, 598 (1994)).

⁽¹⁷⁴⁾ See, e.g. California Penal Code § 1524.3(b); Rule 3.6-3.13 Alabama Rules of Criminal Procedure; Section 10.79.035; Revised Code of Washington; Section 19.2-59 of Chapter 5, Title 19.2 Criminal Procedure, Code of Virginia.

3.1.1.2. Further use of the information collected

- (101) As regards the further use of data collected by federal criminal law enforcement authorities, different statutes, guidelines and standards impose specific safeguards. With the exception of the specific instruments applicable to the activities of the FBI (AGG-DOM and FBI Domestic Investigations and Operations Guide), the requirements described in this section generally apply to the further use of data by any federal authority, including to data accessed for civil or regulatory purposes. This includes the requirements following from the Office of Management and Budget memos/regulations, the Federal Information Security Management Modernization Act, the E-Government Act and the Federal Records Act.
- (102) In accordance with authority provided by the Clinger-Cohen Act (P.L. 104-106, Division E) and the Computer Security Act of 1987 (P.L. 100-235), the Office of Management and Budget (OMB) issued Circular No. A-130 to establish general binding guidance that applies to all federal agencies (including law enforcement authorities) when they handle personally identifiable information ⁽¹⁷⁵⁾. In particular, the circular requires all federal agencies to “limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of personally identifiable information to that which is legally authorized, relevant, and reasonably deemed necessary for the proper performance of authorised agency functions” ⁽¹⁷⁶⁾. In addition, to the extent reasonably practicable, federal agencies must ensure that personally identifiable information is accurate, relevant, timely and complete, and reduced to the minimum necessary for the proper performance of an agency’s functions. More generally, federal agencies must establish a comprehensive privacy program to ensure compliance with applicable privacy requirements, develop and evaluate privacy policies and manage privacy risks; maintain procedures to detect, document and report privacy compliance incidents; develop privacy awareness and training programmes for employees and contractors; and put in place policies and procedures to ensure that personnel is held accountable for complying with privacy requirements and policies ⁽¹⁷⁷⁾.
- (103) In addition, the E-Government Act ⁽¹⁷⁸⁾ requires all federal agencies (including criminal law enforcement authorities) to put in place information security protections that are commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction; have a Chief Information Officer to ensure compliance with information security requirements and perform an annual independent evaluation (e.g. by an Inspector General, see recital 109) of their information security program and practices ⁽¹⁷⁹⁾. Similarly, the Federal Records Act (FRA) ⁽¹⁸⁰⁾ and supplemental regulations ⁽¹⁸¹⁾ require information held by federal agencies to be subject to safeguards ensuring the physical integrity of the information and protecting it against unauthorized access.
- (104) Pursuant to federal statutory authority, including the Federal Information Security Modernisation Act of 2014, the OMB and the National Institute of Standards and Technology (NIST) have developed standards which are binding on federal agencies (including criminal law enforcement authorities) and that further specify the minimum information security requirements that have to be put in place, including access controls, ensuring awareness and training, contingency planning, incident response, auditing and accountability tools, ensuring system and information integrity, conducting privacy and security risk assessments etc. ⁽¹⁸²⁾. Moreover, all federal agencies

⁽¹⁷⁵⁾ I.e. “information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual”, see OMB Circular No. A-130, p. 33 (definition of ‘personally identifiable information’).

⁽¹⁷⁶⁾ OMB Circular No. A-130, Managing Information as a Strategic Resource, Appendix II, Responsibilities for Managing Personally Identifiable Information, 81 Fed. Reg. 49,689 (28 July 2016), p. 17.

⁽¹⁷⁷⁾ Appendix II, §5(a)-(h).

⁽¹⁷⁸⁾ 44 U.S.C. Chapter 36.

⁽¹⁷⁹⁾ 44 U.S.C. §§ 3544-3545.

⁽¹⁸⁰⁾ FAC, 44 U.S.C. § 3105.

⁽¹⁸¹⁾ 36 C.F.R. §§ 1228.150, et seq., 1228.228, and Appendix A.

⁽¹⁸²⁾ See e.g. OMB Circular No. A-130; NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations (10 December 2020); and the NIST Federal Information Processing Standards 200: Minimum Security Requirements for Federal Information and Information Systems.

(including criminal law enforcement authorities) must, in accordance with guidelines of the OMB, maintain and implement a plan for handling data breaches, including when it comes to responding to such breaches and assessing the risks of harm ⁽¹⁸³⁾.

- (105) As regards data retention, the FRA ⁽¹⁸⁴⁾ requires U.S. federal agencies (including criminal law enforcement authorities) to establish retention periods for their records (after which such records must be disposed), which must be approved by the National Archives and Record Administration ⁽¹⁸⁵⁾. The length of these retention period is fixed in light of different factors, such as the type of investigation, whether the evidence is still relevant to the investigation, etc. With respect to the FBI, AGG-DOM provides that the FBI must have in place such a records retention plan and maintain a system that can promptly retrieve the status of and basis for investigations.
- (106) Finally, OMB Circular No. A-130 also contains certain requirements for disseminating personally identifiable information. In principle, the dissemination and disclosure of personally identifiable information must be limited to what is legally authorised, relevant and reasonably deemed necessary for the proper performance of an agency's functions ⁽¹⁸⁶⁾. When sharing personally identifiable information with other government entities, U.S. federal agencies must impose, where relevant, conditions (including the implementation of specific security and privacy controls) that govern the processing of the information through written agreements (including contracts, data use agreements, information exchange agreements and memoranda of understanding) ⁽¹⁸⁷⁾. As regards the grounds on which information may be disseminated, the AGG-DOM and FBI Domestic Investigations and Operations Guide ⁽¹⁸⁸⁾ for instance provide that the FBI may be under a legal requirement to do so (e.g. under an international agreement) or is allowed to disseminate information in certain circumstances, e.g. to other U.S. agencies if disclosure is compatible with the purpose for which the information was collected and it is related to their responsibilities; to congressional committees; to foreign agencies if the information is related to their responsibilities and the dissemination is consistent with the interests of the United States; the dissemination is notably necessary to protect the safety or security of persons or property, or to protect against or prevent a crime or threat to the national security and the disclosure is compatible with the purpose for which the information was collected ⁽¹⁸⁹⁾.

3.1.2. Oversight

- (107) The activities of federal criminal law enforcement agencies are subject to oversight by various bodies ⁽¹⁹⁰⁾. As explained in recitals 92-99, in most cases this includes prior oversight by the judiciary, which has to authorise individual collection measures before they can be used. In addition, other bodies oversee different stages of the activities of criminal law enforcement authorities, including the collection and processing of personal data. Together, these judicial and non-judicial bodies ensure that law enforcement authorities are subject to independent oversight.

⁽¹⁸³⁾ Memorandum 17-12, 'Preparing for and Responding to a Breach of Personally Identifiable Information' available at https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf and OMB Circular No. A-130. For example, the procedures for responding to data breaches of the Department of Justice, see <https://www.justice.gov/file/4336/download>.

⁽¹⁸⁴⁾ FRA, 44 U.S.C. §§3101 et seq.

⁽¹⁸⁵⁾ The National Archives and Record Administration has the authority to assess agency records management practices, and may determine whether continued retention of certain records is warranted (44 U.S.C. §§ 2904(c), 2906).

⁽¹⁸⁶⁾ OMB Circular No. A-130, Section 5.f.1.(d)

⁽¹⁸⁷⁾ OMB Circular No. A-130, Appendix I §3(d).

⁽¹⁸⁸⁾ See also FBI Domestic Investigations and Operations Guide (DIOG) Section 14.

⁽¹⁸⁹⁾ AGG-DOM, Section VI, B and C; FBI Domestic Investigations and Operations Guide (DIOG) Section 14.

⁽¹⁹⁰⁾ The mechanisms mentioned in this section also apply to the collection and use of data by federal authorities for civil and regulatory purposes. Federal civil and regulatory agencies are subject to scrutiny from their respective Inspectors Generals and oversight from Congress, including the Government Accountability Office, Congress's auditing and investigatory agency. Unless the agency has a designated Privacy and Civil Liberties Officer - a position typically found within agencies like the Department of Justice and the Department of Homeland Security (DHS) due to their law enforcement and national security responsibilities - these duties fall to the agency's Senior Agency Official for Privacy (SAOP). All federal agencies are legally obligated to designate an SAOP, who bears the responsibility for ensuring the agency's compliance with privacy laws and overseeing related matters. See, e.g., OMB M-16-24, Role and Designation of Senior Agency Officials for Privacy (2016).

- (108) Firstly, Privacy and Civil Liberties Officers exist within various departments with criminal law enforcement responsibilities ⁽¹⁹¹⁾. While the specific powers of these officers may vary somewhat depending on the authorising statute, they typically encompass the supervision of procedures to ensure that the respective department/agency is adequately considering privacy and civil liberties concerns and has put in place adequate procedures to address complaints from individuals who consider that their privacy or civil liberties have been violated. The heads of each department or agency must ensure that Privacy and Civil Liberties Officers have the material and resources to fulfil their mandate, are given access to any material and personnel necessary to carry out their functions, and are informed about and are consulted on proposed policy changes ⁽¹⁹²⁾. Privacy and Civil Liberties Officers periodically report to Congress, including on the number and nature of the complaints received by the department/agency and a summary of the disposition of such complaints, the reviews and inquiries conducted and the impact of the activities carried out by the Officer ⁽¹⁹³⁾.
- (109) Secondly, an independent Inspector General oversees the activities of the Department of Justice, including the FBI ⁽¹⁹⁴⁾. Inspectors General are statutorily independent ⁽¹⁹⁵⁾ and responsible for conducting independent investigations, audits, and inspections of the Department's programs and operations. They have access to all records, reports, audits, reviews, documents, papers, recommendations or other relevant material, if need be by subpoena, and may take testimony ⁽¹⁹⁶⁾. While Inspectors General issue non-binding recommendations for corrective action, their reports, including on follow-up action (or the lack thereof) ⁽¹⁹⁷⁾ are generally made public and sent to Congress, which can on this basis exercise its oversight function (see recital 111) ⁽¹⁹⁸⁾.

⁽¹⁹¹⁾ See 42 U.S.C. § 2000ee-1. This includes for instance the Department of Justice, the Department of Homeland Security and the FBI. In the DHS, additionally, a Chief Privacy Officer is responsible for preserving and enhancing privacy protections and promoting transparency within the Department (6 U.S.C. 142, Section 222). All DHS systems, technology, forms, and programs that collect personal data or have a privacy impact are subject to the oversight of the Chief Privacy Officer who has access to all records, reports, audits, reviews, documents, papers, recommendations, and other materials available to the Department, and if need be by subpoena. The Privacy Officer has to report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations.

⁽¹⁹²⁾ 42 U.S.C. § 2000ee-1(d).

⁽¹⁹³⁾ See 42 U.S.C. §§ 2000ee-1 (f)(1)-(2). For example, the report of the DOJ's Chief Privacy and Civil Liberties Officer and the Office of Privacy and Civil Liberties covering the period October 2020- March 2021 shows that 389 privacy reviews were carried out, including of information systems and other programs (https://www.justice.gov/d9/pages/attachments/2021/05/10/2021-4-21opclsection803reportfy20sa1_final.pdf).

⁽¹⁹⁴⁾ Similarly, the Homeland Security Act of 2002 established an Office of Inspector General in the Department of Homeland Security.

⁽¹⁹⁵⁾ Inspectors General have secure tenure and may only be removed by the President who must communicate to Congress in writing the reasons for any such removal.

⁽¹⁹⁶⁾ See Inspector General Act of 1978, § 6.

⁽¹⁹⁷⁾ See in this respect for instance the overview prepared by the DoJ Office of the Inspector General of its recommendations made and the extent to which they have been implemented through department and agency follow-up actions, <https://oig.justice.gov/sites/default/files/reports/22-043.pdf>.

⁽¹⁹⁸⁾ See Inspector General Act of 1978, §§ 4(5), 5. For example, the Office of the Inspector General within the Department of Justice recently published its semi-annual report to Congress (1 October 2021- 31 March 2022, <https://oig.justice.gov/node/23596>), which provides an overview of its audits, evaluations, inspections, special reviews and investigations of DOJ programs and operations. These activities included an investigation of a former contractor regarding unlawful disclosure of electronic surveillance (the wiretapping of an individual) in an ongoing investigation, which led to the sentencing of the contractor. The Office of the Inspector General also conducted an investigation of the DOJ agencies' information security programmes and practices, which includes testing the effectiveness of information security policies, procedures, and practices of a representative subset of agency systems.

- (110) Thirdly, to the extent they carry out counter-terrorism activities, departments with criminal law enforcement responsibilities are subject to oversight by the Privacy and Civil Liberties Oversight Board (PCLOB), an independent agency within the executive branch composed of a bipartisan, five-member Board appointed by the President for a fixed six-year term with Senate approval ⁽¹⁹⁹⁾. According to its founding statute, the PCLOB is entrusted with responsibilities in the field of counterterrorism policies and their implementation, with a view to protect privacy and civil liberties. In its review it can access all relevant agency records, reports, audits, reviews, documents, papers and recommendations, including classified information, conduct interviews and hear testimony ⁽²⁰⁰⁾. It receives reports from the civil liberties and privacy officers of several federal departments/agencies ⁽²⁰¹⁾, may issue recommendations to the government and law enforcement authorities, and regularly reports to Congressional committees and the President ⁽²⁰²⁾. Reports of the Board, including the ones to Congress, must be made publicly available to the greatest extent possible ⁽²⁰³⁾.
- (111) Finally, criminal law enforcement activities are subject to oversight by specific Committees in the U.S. Congress (the House and Senate Judiciary Committees). The Judiciary Committees conduct regular oversight in different ways, in particular through hearings, investigations, reviews and reports ⁽²⁰⁴⁾.

3.1.3. *Redress*

- (112) As indicated, criminal law enforcement authorities must in most cases obtain prior judicial authorisation to collect personal data. Although this is not required for administrative subpoenas, these are limited to specific situations and will be subject to independent judicial review at least where the government seeks enforcement in court. In particular, recipients of administrative subpoenas may challenge them in court on the grounds that they are unreasonable, i.e. overbroad, oppressive or burdensome ⁽²⁰⁵⁾.
- (113) Individuals may first of all lodge requests or complaints with criminal law enforcement authorities concerning the handling of their personal data. This includes the possibility to request access to and correction of personal data ⁽²⁰⁶⁾. As regards activities relating to counter-terrorism, individuals may also lodge a complaint with Privacy and Civil Liberties Officers (or other privacy officials) within law enforcement authorities ⁽²⁰⁷⁾.
- (114) Moreover, U.S. law provides for a number of judicial redress avenues for individuals, against a public authority or one of its officials, where these authorities process personal data ⁽²⁰⁸⁾. These avenues, which include in particular the APA, the Freedom of Information Act (FOIA) and the Electronic Communications Privacy Act (ECPA), are open to all individuals irrespective of their nationality, subject to any applicable conditions.

⁽¹⁹⁹⁾ Members of the Board must be selected solely on the basis of their professional qualifications, achievements, public stature, expertise in civil liberties and privacy, and relevant experience, and without regard to political affiliation. There may in no event be more than three members of the Board that belong to the same political party. An individual appointed to the Board may not, while serving on the Board, be an elected official, officer, or employee of the Federal Government, other than in the capacity as a member of the Board. See 42 U.S.C. § 2000ee (h).

⁽²⁰⁰⁾ 42 U.S.C. § 2000ee (g).

⁽²⁰¹⁾ See 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). These include at least the Department of Justice, the Department of Defense, the Department of Homeland Security, plus any other department, agency or element of the executive branch designated by the PCLOB to be appropriate for coverage.

⁽²⁰²⁾ 42 U.S.C. § 2000ee, (e).

⁽²⁰³⁾ 42 U.S.C. § 2000ee (f).

⁽²⁰⁴⁾ For example, the Committees organise thematic hearings (see e.g. a recent hearing of the House Judiciary Committee on “digital dragnets”, <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983>), as well as, regular oversight hearings, e.g. of the FBI and DoJ, see <https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation>; <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966> and <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899>.

⁽²⁰⁵⁾ See Annex VI.

⁽²⁰⁶⁾ OMB Circular No. A-130, Appendix II, Section 3(a) and (f), which requires federal agencies to ensure appropriate access and correction upon request of individuals, and to establish procedures to receive and address privacy-related complaints and requests.

⁽²⁰⁷⁾ See 42 U.S.C. § 2000ee-1 as regards for instance the DoJ and the Department of Homeland Security. See also OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy*.

⁽²⁰⁸⁾ The redress mechanisms mentioned in this section also apply to the collection and use of data by federal authorities for civil and regulatory purposes.

- (115) Generally, under the judicial review provisions of the APA ⁽²⁰⁹⁾, “any person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action”, is entitled to seek judicial review ⁽²¹⁰⁾. This includes the possibility to ask the court to “hold unlawful and set aside agency action, findings, and conclusions found to be [...] arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law” ⁽²¹¹⁾.
- (116) More specifically, Title II of the ECPA ⁽²¹²⁾ sets forth a system of statutory privacy rights and as such governs law enforcement access to the contents of wire, oral or electronic communications stored by third-party service providers ⁽²¹³⁾. It criminalises the unlawful (i.e. not authorised by court or otherwise permissible) access to such communications and provides recourse for an affected individual to file a civil action in U.S. federal court for actual and punitive damages as well as equitable or declaratory relief against a government official that has wilfully committed such unlawful acts, or against the United States.
- (117) In addition, several other statutes afford individuals the right to bring suit against a U.S. public authority or official with respect to the processing of their personal data, such as the Wiretap Act ⁽²¹⁴⁾, the Computer Fraud and Abuse Act ⁽²¹⁵⁾, the Federal Torts Claim Act ⁽²¹⁶⁾, the Right to Financial Privacy Act ⁽²¹⁷⁾, and the Fair Credit Reporting Act ⁽²¹⁸⁾.

⁽²⁰⁹⁾ 5 U.S.C. § 702.

⁽²¹⁰⁾ Generally, only “final” agency action — rather than “preliminary, procedural, or intermediate” agency action — is subject to judicial review. See 5 U.S.C. § 704.

⁽²¹¹⁾ 5 U.S.C. § 706(2)(A).

⁽²¹²⁾ 18 U.S.C. §§ 2701-2712.

⁽²¹³⁾ The ECPA protects communications held by two defined classes of network service providers, namely providers of: (i) electronic communication services, for instance telephony or e-mail; (ii) remote computing services like computer storage or processing services.

⁽²¹⁴⁾ 18 U.S.C. §§ 2510 et seq. Under the Wiretap Act (18 U.S.C. § 2520), a person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used may bring a civil action for violation of the Wiretap Act, including under certain circumstances against an individual government official or the United States. For the collection of non-content information (e.g. IP address, e-mail to/from address), see also the Pen Registers and Trap and Trace Devices chapter of Title 18 (18 U.S.C. §§ 3121-3127 and, for civil action, § 2707).

⁽²¹⁵⁾ 18 U.S.C. § 1030. Under the Computer Fraud and Abuse Act, a person may bring suit against any person with respect to intentional unauthorised access (or exceeding authorised access) to obtain information from a financial institution, a U.S. government computer system or other specified computer, including under certain circumstances against an individual government official.

⁽²¹⁶⁾ 28 U.S.C. §§ 2671 et seq. Under the Federal Tort Claims Act, a person may bring suit, under certain circumstances, against the United States with respect to “the negligent or wrongful act or omission of any employee of the Government while acting within the scope of his office or employment”.

⁽²¹⁷⁾ 12 U.S.C. §§ 3401 et seq. Under the Right to Financial Privacy Act, a person may bring suit, under certain circumstances, against the United States with respect to the obtaining or disclosing of protected financial records in violation of the statute. Government access to protected financial records is generally prohibited unless the government makes the request subject to a lawful subpoena or search warrant or, subject to limitations, a formal written request and the individual whose information is sought receives notice of such a request.

⁽²¹⁸⁾ 15 U.S.C. §§ 1681-1681x. Under the Fair Credit Reporting Act, a person may bring suit against any person who fails to comply with requirements (in particular the need for lawful authorisation) regarding the collection, dissemination and use of consumer credit reports, or, under certain circumstances, against a government agency.

- (118) Also, under FOIA ⁽²¹⁹⁾, 5 U.S.C. § 552 any person has the right to obtain access to federal agency records, including where these contain the individual's personal data. After exhausting administrative remedies, an individual may invoke such right to access in court unless those records are protected from public disclosure by an exemption or special law enforcement exclusion ⁽²²⁰⁾. In this case, the court will assess whether any exemption applies or has been lawfully invoked by the relevant public authority.

3.2. Access and use by U.S. public authorities for national security purposes

- (119) The law of the United States contains various limitations and safeguards with respect to the access and use of personal data for national security purposes, and provides oversight and redress mechanisms that are in line with the requirements referred to in recital 89 of this Decision. The conditions under which such access can take place and the safeguards applicable to the use of these powers are assessed in detail in the following sections.

3.2.1. Legal bases, limitations and safeguards

3.2.1.1. Applicable legal framework

- (120) Personal data transferred from the Union to EU-U.S. DPF organisations may be collected by U.S. authorities for national security purposes on the basis of different legal instruments, subject to specific conditions and safeguards.
- (121) Once personal data has been received by organisations located in the United States, U.S. intelligence agencies may seek access to such data for national security purposes only as authorised by statute, specifically under the Foreign Intelligence Surveillance Act (FISA) or and statutory provisions authorising access through National Security Letters (NSL) ⁽²²¹⁾. FISA contains several legal bases that may be used to collect (and subsequently process) the personal data of Union data subjects transferred under the EU-U.S. DPF (Section 105 FISA ⁽²²²⁾, Section 302 FISA ⁽²²³⁾, Section 402 FISA ⁽²²⁴⁾, Section 501 FISA ⁽²²⁵⁾ and Section 702 FISA ⁽²²⁶⁾), as described in more detail in recitals 142-152.

⁽²¹⁹⁾ 5 U.S.C. § 552.

⁽²²⁰⁾ These exclusions are, however, framed. For example, according to 5 U.S.C. § 552 (b)(7), FOIA rights are ruled out for “records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions, if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual.” Also, “[w]henver a request is made which involves access to records [the production of which could reasonably be expected to interfere with enforcement proceedings] and— (A) the investigation or proceeding involves a possible violation of criminal law; and (B) there is reason to believe that (i) the subject of the investigation or proceeding is not aware of its pendency, and (ii) disclosure of the existence of the records could reasonably be expected to interfere with enforcement proceedings, the agency may, during only such time as that circumstance continues, treat the records as not subject to the requirements of this section.” (5 U.S.C. § 552 (c)(1)).

⁽²²¹⁾ 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; and 18 U.S.C. § 2709. See recital 153.

⁽²²²⁾ 50 U.S.C. § 1804, which concerns traditional individualized electronic surveillance.

⁽²²³⁾ 50 U.S.C. § 1822, which concerns physical searches for foreign intelligence purposes.

⁽²²⁴⁾ 50 U.S.C. § 1842 with § 1841(2) and Section 3127 of Title 18, which concerns the installation of pen registers or trap and trace devices.

⁽²²⁵⁾ 50 U.S.C. § 1861, which permits FBI to submit “an application for an order authorizing a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility to release records in its possession for an investigation to gather foreign intelligence information or an investigation concerning international terrorism.”

⁽²²⁶⁾ 50 U.S. Code § 1881a, which allows US Intelligence Community elements to seek access to information, including the content of internet communications, from U.S. companies, targeting certain non-U.S. persons outside the United States with the legally compelled assistance of electronic communication providers.

- (122) U.S. intelligence agencies also have possibilities to collect personal data outside the United States, which may include personal data in transit between the Union and the United States. The collection outside the United States is based on Executive Order 12333 (EO 12333) ⁽²²⁷⁾, issued by the President ⁽²²⁸⁾.
- (123) The collection of signals intelligence is the form of intelligence collection that is the most relevant for the present adequacy finding, as it concerns the collection of electronic communications and data from information systems. Such collection may be carried out by U.S. intelligence agencies both within the United States (on the basis of FISA) and while data is in transit to the United States (on the basis of EO 12333).
- (124) On 7 October 2022, the U.S. President issued EO 14086 on Enhancing Safeguards for United States Signals Intelligence setting limitations and safeguards for all U.S. signals intelligence activities. This EO replaces Presidential Policy Directive (PPD-28) to a large extent ⁽²²⁹⁾, strengthens the conditions, limitations and safeguards that apply to all signals intelligence activities (i.e. on the basis of FISA and EO 12333), regardless of where they take place ⁽²³⁰⁾, and establishes a new redress mechanism through which these safeguards can be invoked and enforced by individuals ⁽²³¹⁾ (see in more detail recitals 176-194). In doing so, it implements in U.S. law the outcome of the talks that took place between the EU and U.S. following the invalidation of the Commission's adequacy decision on the Privacy Shield by the Court of Justice (see recital 6). It is, therefore, a particularly important element of the legal framework assessed in this Decision.
- (125) The limitations and safeguards introduced by EO 14086 supplement those provided by Section 702 FISA and EO 12333. The requirements described below (in sections 3.2.1.2 and 3.2.1.3) must be applied by intelligence agencies when engaging in signals intelligence activities pursuant to Section 702 FISA and EO 12333, e.g. when selecting/identifying categories of foreign intelligence information to be acquired pursuant to Section 702 FISA; collecting foreign intelligence or counterintelligence pursuant to EO 12333; and making individual targeting decisions under Section 702 FISA and EO 12333.
- (126) The requirements laid down in this Executive Order issued by the President are binding on the entire Intelligence Community. They must be further implemented through agency policies and procedures that transpose them into concrete directions for day-to-day operations. In this respect, EO 14086 provides U.S. intelligence agencies with a maximum of one year to update their existing policies and procedures (i.e. by 7 October 2023) to bring them in line with the EO's requirements. Such updated policies and procedures have to be developed in consultation with the Attorney General, the Civil Liberties Protection Officer of the Director of National Intelligence (ODNI CLPO) and the PCLOB – an independent oversight body authorised to review Executive Branch policies and their implementation, with a view to protect privacy and civil liberties (see recital 110 as regards the role and status of the PCLOB) – and be made publicly available ⁽²³²⁾. In addition, once the updated policies and procedures are in place, the PCLOB will conduct a review to ensure that they are consistent with the EO. Within 180 days of

⁽²²⁷⁾ EO 12333: United States Intelligence Activities, Federal Register Vol. 40, No 235 (8 December 1981 as amended 30 July 2008). EO 12333 more generally defines the goals, directions, duties and responsibilities of U.S. intelligence efforts (including the role of the various Intelligence Community elements) and sets out the general parameters for the conduct of intelligence activities.

⁽²²⁸⁾ Under Article II of the U.S. Constitution, responsibility ensuring national security including in particular gathering foreign intelligence falls within the President's authority as Commander in Chief of the armed forces.

⁽²²⁹⁾ EO 14086 supersedes a previous Presidential Directive, PPD 28, with the exception of its Section 3 and a complementing Annex, (which requires intelligence agencies to annually review their signals intelligence priorities and requirements, taking into account the benefits of signals intelligence activities for the U.S.' national interests, as well as the risk posed by those activities) and Section 6 (which contains general provisions), see the National Security Memorandum on Partial Revocation of Presidential Policy Directive 28, available at <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/>

⁽²³⁰⁾ See Section 5(f) EO 14086, which explains that the EO has the same scope of application as PPD-28, which, according to its footnote 3, applied to signals intelligence activities conducted in order to collect communications or information about communications, except signals intelligence activities undertaken to test or develop signals intelligence capabilities.

⁽²³¹⁾ See in this respect e.g. Section 5(h) of EO 14086, which clarifies that the safeguards in the EO create a legal entitlement and can be enforced by individuals through the redress mechanism.

⁽²³²⁾ See Section 2(c)(iv)(C) EO 14086.

completion of such a review by the PCLOB, each intelligence agency must carefully consider and implement or otherwise address all of the PCLOB's recommendations. On 3 July 2023, the U.S. government published such updated policies and procedures ⁽²³³⁾.

3.2.1.2. *Limitations and safeguards as regards the collection of personal data for national security purposes*

- (127) EO 14086 sets a number of overreaching requirements that apply to all signals intelligence activities (collection, use, dissemination, etc. of personal data).
- (128) Firstly, such activities must be based on statute or Presidential authorisation and undertaken in compliance with U.S. law, including the Constitution ⁽²³⁴⁾.
- (129) Secondly, appropriate safeguards must be in place to ensure that privacy and civil liberties are integral considerations in the planning of such activities ⁽²³⁵⁾.
- (130) In particular, any signals intelligence activity may only be carried out "following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority" (as regards the notion of 'validated intelligence priority', see recital 135) ⁽²³⁶⁾.
- (131) Moreover, such activities may only be conducted "to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized" ⁽²³⁷⁾. In other words, a proper balance must be achieved "between the importance of the intelligence priority pursued and the impact on the privacy and civil liberties of affected individuals, regardless of their nationality or wherever they might reside" ⁽²³⁸⁾.
- (132) Finally, to ensure compliance with these general requirements - which reflect the principles of legality, necessity and proportionality - signals intelligence activities are subject to oversight (see in more detail section 3.2.2) ⁽²³⁹⁾.
- (133) These overarching requirements are further substantiated with respect to the collection of signals intelligence through a number of conditions and limitations ensuring that the interference with the rights of individuals is limited to what is necessary and proportionate to advance a legitimate objective.
- (134) Firstly, the EO limits the grounds on which data can be collected as part of signals intelligence activities in two ways. On the one hand, the EO lays down the legitimate objectives that may be pursued by signals intelligence collection, e.g. to understand or assess the capabilities, intentions, or activities of foreign organisations, including international terrorist organisations, that pose a current or potential threat to the national security of the United States; to protect against foreign military capabilities and activities; to understand or assess transnational threats that impact global security, such as climate and other ecological change, public health risks and humanitarian threats ⁽²⁴⁰⁾. On the other hand, the EO lists certain objectives that must never be pursued by signals intelligence activities, e.g. for the

⁽²³³⁾ <https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086>.

⁽²³⁴⁾ Section 2(a)(i) EO 14086.

⁽²³⁵⁾ Section 2(a)(ii) EO 14086.

⁽²³⁶⁾ Section 2(a)(ii)(A) EO 14086. This does not always require that signals intelligence is the sole means for advancing aspects of a validated intelligence priority. For example, the collection of signals intelligence may be used to ensure alternative pathways for validation (e.g. to corroborate information received from other intelligence sources) or for maintaining reliable access to the same information (Section 2(c)(i)(A) EO 14086).

⁽²³⁷⁾ Section 2(a)(ii)(B) EO 14086.

⁽²³⁸⁾ Section 2(a)(ii)(B) EO 14086.

⁽²³⁹⁾ Section 2(a)(iii), in conjunction with Section 2(d) EO 14086.

⁽²⁴⁰⁾ Section 2(b)(i) EO 14086. Because of the circumscribed list of legitimate objectives in the EO, which does not encompass possible future threats, the EO provides for the possibility for the President to update this list if new national security imperatives emerge, such as new threats to national security. Such updates must in principle be publicly released, unless the President determines that doing so would itself pose a risk to the national security of the United States (Section 2(b)(i)(B) EO 14086).

purpose of burdening criticism, dissent, or the free expression of ideas or political opinions by individuals or the press; for the purpose of disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation, or religion; or to afford a competitive advantage to U.S. companies ⁽²⁴¹⁾.

- (135) Moreover, the legitimate objectives laid down in EO 14086 cannot by themselves be relied upon by intelligence agencies to justify signals intelligence collection but must be further substantiated, for operational purposes, into more concrete priorities for which signals intelligence may be collected. In other words, actual collection can only take place to advance a more specific priority. Such priorities are established through a dedicated process aimed at ensuring compliance with the applicable legal requirements, including those relating to privacy and civil liberties. More specifically, intelligence priorities are first developed by the Director of National Intelligence (through the so-called National Intelligence Priorities Framework) and submitted to the President for approval ⁽²⁴²⁾. Before proposing intelligence priorities to the President, the Director must, in accordance with EO 14086, obtain an assessment from the ODNI CLPO for each priority as to whether it (1) advances one or more legitimate objectives listed in the EO; (2) was neither designed nor is anticipated to result in signals intelligence collection for a prohibited objective listed in the EO; and (3) was established after appropriate consideration for the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside ⁽²⁴³⁾. In case the Director disagrees with the CLPO's assessment, both views must be presented to the President ⁽²⁴⁴⁾.
- (136) Therefore, this process notably ensures that privacy considerations are taken into account from the initial stage where intelligence priorities are developed.
- (137) Secondly, once an intelligence priority has been established, a number of requirements govern the decision as to whether and to what extent signals intelligence may be collected to advance such a priority. These requirements operationalise the overarching necessity and proportionality standards set forth by Section 2(a) of the EO.
- (138) In particular, signals intelligence may only be collected "following a determination that, based on a reasonable assessment of all relevant factors, the collection is necessary to advance a specific intelligence priority" ⁽²⁴⁵⁾. In determining whether a specific signals intelligence collection activity is necessary to advance a validated intelligence priority, U.S. intelligence agencies must consider the availability, feasibility and appropriateness of other less intrusive sources and methods, including from diplomatic and public sources ⁽²⁴⁶⁾. When available, such alternative, less intrusive sources and methods must be prioritised ⁽²⁴⁷⁾.
- (139) When, in the application of such criteria, the collection of signals intelligence is considered necessary, it must be as "tailored as feasible" and must "not disproportionately impact privacy and civil liberties" ⁽²⁴⁸⁾. To ensure that privacy and civil liberties are not disproportionately affected – i.e. to strike a proper balance between national security needs and the protection of privacy and civil liberties – all relevant factors have to be duly taken into account, such as the nature of the pursued objective; the intrusiveness of the collection activity, including its duration; the probable contribution of the collection to the objective pursued; the reasonably foreseeable consequences to individuals; and the nature and sensitivity of the data to be collected ⁽²⁴⁹⁾.

⁽²⁴¹⁾ Section 2(b)(ii) EO 14086.

⁽²⁴²⁾ Section 102A of the National Security Act and Section 2(b)(iii) EO 14086.

⁽²⁴³⁾ In exceptional cases (in particular, when such process cannot be carried out because of a need to address a new or evolving intelligence requirement), such priorities can be set directly by the President or the head of an element of the Intelligence Community, who in principle have to apply the same criteria as the ones described in section 2(b)(iii)(A)(1)-(3), see Section 4(n) EO 14086.

⁽²⁴⁴⁾ Section 2(b)(iii)(C) EO 14086.

⁽²⁴⁵⁾ Section 2(b) and (c)(i)(A) EO 14086.

⁽²⁴⁶⁾ Section 2(c)(i)(A) EO 14086.

⁽²⁴⁷⁾ Section 2(c)(i)(A) EO 14086.

⁽²⁴⁸⁾ Section 2(c)(i)(B) EO 14086.

⁽²⁴⁹⁾ Section 2(c)(i)(B) EO 14086.

(140) As regards the type of signals intelligence collection, collection of data within the United States, which is the most relevant for the present adequacy finding as it concerns data that has been transferred to organisations in the U.S., must always be targeted, as explained in more detail in recitals 142-153.

(141) 'Bulk collection' ⁽²⁵⁰⁾ may only be carried out outside the United States, on the basis of EO 12333. Also in this case, pursuant to EO 14086, targeted collection must be prioritised ⁽²⁵¹⁾. Conversely, bulk collection is only allowed where the information necessary to advance a validated intelligence priority cannot reasonably be obtained by targeted collection ⁽²⁵²⁾. When it is necessary to carry out bulk collection of data outside the United States, specific safeguards under EO 14086 apply ⁽²⁵³⁾. Firstly, methods and technical measures must be applied in order to limit the data collected to only what is necessary to advance a validated intelligence priority, while minimizing the collection of non-pertinent information ⁽²⁵⁴⁾. Secondly, the EO limits the use of information collected in bulk (including querying) to six specific objectives, including protecting against terrorism, the taking of hostages, and the holding of individuals captive by or on behalf of a foreign government, organisation or person; protecting against foreign espionage, sabotage, or assassination; protecting against threats from the development possession, or proliferation of weapons of mass destruction or related technologies and threats, etc. ⁽²⁵⁵⁾ Finally, any querying of signals intelligence obtained in bulk may only take place where necessary to advance a validated intelligence priority, in pursuit of these six objectives and in accordance with policies and procedures that appropriately take into account the impact of the queries on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside ⁽²⁵⁶⁾.

(142) In addition to the requirements of EO 14086, the signals intelligence collection of data that has been transferred to an organisation in the United States is subject to specific limitations and safeguards governed by Section 702 FISA ⁽²⁵⁷⁾. Section 702 FISA allows the collection of foreign intelligence information through the targeting of non-U.S. persons reasonably believed to be located outside the United States with the compelled assistance of U.S. electronic communication service providers ⁽²⁵⁸⁾. In order to collect foreign intelligence information pursuant to Section 702 FISA, the Attorney General and the Director of National Intelligence submit annual certifications to the Foreign

⁽²⁵⁰⁾ I.e. the collection of large quantities of signals intelligence that, due to technical or operational considerations, is acquired without the use of discriminants (for example, without the use of specific identifiers or selection terms), see Section 4(b) EO 14086. Pursuant to EO 14086 and as further explained in recital 141, bulk collection under EO 12333 takes place only when necessary to advance specific validated intelligence priorities and is subject to a number of limitations and safeguards designed to ensure that data is not accessed on an indiscriminate basis. Bulk collection is therefore to be contrasted to collection taking place on a generalised and indiscriminate basis ('mass surveillance') without limitations and safeguards.

⁽²⁵¹⁾ Section 2(c)(ii)(A) EO 14086.

⁽²⁵²⁾ Section 2(c)(ii)(A) EO 14086.

⁽²⁵³⁾ The specific rules on bulk collection of EO 14086 also apply to a targeted signals intelligence collection activity that temporarily uses data acquired without discriminants (e.g. specific selection terms or identifiers), i.e. in bulk (which is only possible outside the territory of the United States). This is not the case when such data is only used to support the initial technical phase of the targeted signals intelligence collection activity, retained only for a short period of time required to complete this phase and deleted immediately thereafter (Section 2(c)(ii)(D) EO 14086). In this case, the only purpose of the initial collection without discriminants is to allow a targeted collection of information by applying a specific identifier or selection term. In such a scenario, only data that responds to the application of a certain discriminant is inserted into government databases, while the remaining data is destroyed. Such targeted collection therefore remains governed by the general rules that apply to signals intelligence collection, including Section 2(a)-(b) and 2(c)(i) EO 14086.

⁽²⁵⁴⁾ Section 2(c)(ii)(A) EO 14086.

⁽²⁵⁵⁾ Section 2(c)(ii)(B) EO 14086. In case new national security imperatives emerge, such as new threats to national security, the President may update this list. Such updates must in principle be publicly released, unless the President determines that doing so would in itself pose a risk to the national security of the United States (Section 2(c)(ii)(C) EO 14086). As regards queries of data collected in bulk, see Section 2(c)(iii)(D) EO 14086.

⁽²⁵⁶⁾ Section 2(a)(ii)(A), in conjunction with Section 2(c)(iii)(D) EO 14086. See also Annex VII.

⁽²⁵⁷⁾ 50 U.S.C. § 1881.

⁽²⁵⁸⁾ 50 U.S.C. § 1881a (a). In particular, as noted by the PCLOB, Section 702 surveillance "consists entirely of targeting specific [non-U.S.] persons about whom an individualised determination has been made" (Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, 2 July 2014, Section 702 Report, p. 111). See also NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702, 16 April 2014. The term 'electronic communication service provider' is defined in 50 U.S.C. § 1881 (a)(4).

Intelligence Surveillance Court (FISC) which identify categories of foreign intelligence information to be acquired ⁽²⁵⁹⁾. Certifications must be accompanied by targeting, minimization and querying procedures, which are also approved by the Court and are legally binding on U.S. intelligence agencies.

(143) The FISC is an independent tribunal ⁽²⁶⁰⁾ created by federal statute whose decisions can be appealed to the Foreign Intelligence Surveillance Court of Review (FISCR) ⁽²⁶¹⁾ and, ultimately, the Supreme Court of the United States ⁽²⁶²⁾. The FISC (and FISCR) is supported by a standing panel of five attorneys and five technical experts that have an expertise in national security matters as well as civil liberties ⁽²⁶³⁾. From this group the court appoints an individual to serve as *amicus curiae* to assist in the consideration of any application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law, unless the court finds that such appointment is not appropriate ⁽²⁶⁴⁾. This ensures in particular that privacy considerations are properly reflected in the court's assessment. The court may also appoint an individual or organisation to serve as *amicus curiae*, including to provide technical expertise, whenever it deems this appropriate or, upon motion, permit an individual or organisation leave to file an *amicus curiae* brief ⁽²⁶⁵⁾.

(144) The FISC reviews the certifications and the related procedures (in particular targeting and minimisation procedures) for compliance with the requirements of FISA. If it considers that the requirements are not fulfilled, it can deny the certification in full or in part and request the procedures to be amended ⁽²⁶⁶⁾. In this respect, the FISC has repeatedly confirmed that its review of Section 702 targeting and minimization procedures is not confined to the procedures as written, but also includes how the procedures are implemented by the government ⁽²⁶⁷⁾.

(145) Individual targeting determinations are made by the National Security Agency (NSA, the intelligence agency responsible for targeting under Section 702 FISA) in accordance with FISC-approved targeting procedures, which require the NSA to assess, based on the totality of the circumstances, that targeting a specific person is likely to acquire a category of foreign intelligence information identified in a certification ⁽²⁶⁸⁾. This assessment must be particularized and fact-based, informed by analytical judgment, the specialized training and experience of the

⁽²⁵⁹⁾ 50 U.S.C. § 1881a (g).

⁽²⁶⁰⁾ The FISC is comprised of judges appointed by the Chief Justice of the United States from among sitting U.S. district court judges, who previously have been appointed by the President and confirmed by the Senate. The judges, who have life tenure and can only be removed for good cause, serve on the FISC for staggered seven-year terms. FISA requires that the judges be drawn from at least seven different U.S. judicial circuits. See 50 U.S.C. § 1803 (a). The judges are supported by experienced judicial law clerks that constitute the court's legal staff and prepare legal analysis on collection requests. See Letter from the Honourable Reggie B. Walton, Presiding Judge, U.S. Foreign Intelligence Surveillance Court, to the Honourable Patrick J. Leahy, Chairman, Committee on the Judiciary, U.S. Senate (29 July 2013) (Walton Letter), p. 2, available at <https://fas.org/irp/news/2013/07/fisc-leahy.pdf>.

⁽²⁶¹⁾ The FISCR is composed of judges appointed by the Chief Justice of the United States and drawn from U.S. district courts or courts of appeals, serving for a staggered seven year term. See 50 U.S.C. § 1803 (b).

⁽²⁶²⁾ See 50 U.S.C. §§ 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i)(4).

⁽²⁶³⁾ 50 U.S.C. § 1803 (i)(1),(3)(A).

⁽²⁶⁴⁾ 50 U.S.C. § 1803 (i)(2)(A).

⁽²⁶⁵⁾ 50 U.S.C. § 1803 (i)(2)(B).

⁽²⁶⁶⁾ See e.g. FISC Opinion of 18 October 2018, available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, as confirmed by the Foreign Intelligence Court of Review in its Opinion of 12 July 2019, available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf.

⁽²⁶⁷⁾ See e.g. FISC, Memorandum Opinion and Order at 35 (18 Nov. 2020) (Authorised for Public Release on 26 April 2021), (Annex D).

⁽²⁶⁸⁾ 50 U.S.C. § 1881a(a), Procedures used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended, of March 2018 (NSA targeting procedures), available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Targeting_27Mar18.pdf, p. 1-4, further explained in PCLOB report, pp. 41-42.

analyst, as well as the nature of the foreign intelligence information to be obtained ⁽²⁶⁹⁾. The targeting is carried out by identifying so-called selectors that identify specific communications facilities, like the target's e-mail address or telephone number, but never key words or names of individuals ⁽²⁷⁰⁾.

- (146) NSA analysts will first identify non-U.S. persons located abroad whose surveillance will lead, based on the analysts' assessment, to the relevant foreign intelligence specified in the certification ⁽²⁷¹⁾. As set out in the NSA's targeting procedures, the NSA can only direct surveillance at a target when it has already learned something about the target ⁽²⁷²⁾. This may follow from information from different sources, for instance human intelligence. Through these other sources, the analyst must also learn about a specific selector (i.e. communication account) used by the potential target. Once these individualised persons have been identified and their targeting has been approved by an extensive review mechanism within the NSA ⁽²⁷³⁾, selectors identifying communication facilities (such as e-mail addresses) used by the targets will be 'tasked' (i.e. developed and applied) ⁽²⁷⁴⁾.

- (147) The NSA must document the factual basis for the selection of the target ⁽²⁷⁵⁾ and, at regular intervals after the initial targeting, affirm that the targeting standard continues to be met ⁽²⁷⁶⁾. Once the targeting standard is no longer satisfied, collection must be ceased ⁽²⁷⁷⁾. The selection by the NSA of each target and its record of each recorded targeting assessment and rationale is reviewed for compliance with the targeting procedures on a bi-monthly basis by officials in the intelligence oversight offices at the Department of Justice, who are under an obligation to report any violation to the FISC and to Congress ⁽²⁷⁸⁾. The NSA's written documentation facilitates the FISC's oversight of whether specific individuals are properly targeted under Section 702 FISA, in accordance with its supervision powers described in recitals 173-174 ⁽²⁷⁹⁾. Finally, the Director of National Intelligence (DNI) is also required to report each year the total number of Section 702 FISA targets in public annual Statistical Transparency Reports. Companies that receive Section 702 FISA directives may publish aggregate data (via transparency reports) on the requests they receive ⁽²⁸⁰⁾.

⁽²⁶⁹⁾ NSA targeting procedures, p. 4.

⁽²⁷⁰⁾ See PCLOB, Section 702 Report, pp. 32-33, 45 with further references. See also Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: December 1, 2016 – May 31, 2017, p. 41 (October 2018), available at: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

⁽²⁷¹⁾ PCLOB, Section 702 Report, pp. 42-43.

⁽²⁷²⁾ NSA targeting procedures, p. 2.

⁽²⁷³⁾ PCLOB, Section 702 Report, p. 46. For example, the NSA must verify that there is a connection between the target and the selector, must document the foreign intelligence information expected to be acquired, this information must be reviewed and approved by two senior NSA analysts, and the overall process will be tracked for subsequent compliance reviews by the ODNI and Department of Justice. See NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702, 16 April 2014.

⁽²⁷⁴⁾ 50 U.S.C. § 1881a (h).

⁽²⁷⁵⁾ NSA targeting procedures, p. 8. See also PCLOB, Section 702 Report, p. 46. Failure to provide a written justification constitutes a documentation compliance incident that must be reported to the FISC and Congress. See Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: December 1, 2016 – May 31, 2017, p. 41 (October 2018), DOJ/ODNI Compliance Report to FISC for Dec. 2016 – May 2017 at p. A-6, available at https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

⁽²⁷⁶⁾ See U.S. Government Submission to Foreign Intelligence Surveillance Court, 2015 Summary of Notable Section 702 Requirements, at 2-3 (July 15, 2015) and the information provided in Annex VII.

⁽²⁷⁷⁾ See U.S. Government Submission to Foreign Intelligence Surveillance Court, 2015 Summary of Notable Section 702 Requirements, at 2-3 (15 July 2015), which provides that the government "[i]f the Government later assesses that the continued tasking of a target's selector is not expected to result in the acquisition of foreign intelligence information, prompt detasking is required, and delay may result in a reportable compliance incident". See also the information provided in Annex VII.

⁽²⁷⁸⁾ PCLOB, Section 702 Report, pp. 70-72; Rule 13(b) of the Rules of Procedure of the United States Intelligence Surveillance Court, available at <https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf>.

⁽²⁷⁹⁾ See also DOJ/ODNI Compliance Report to FISC for Dec. 2016 – May 2017 at p. A-6.

⁽²⁸⁰⁾ 50 U.S.C. § 1874.

- (148) As regards the other legal bases to collect personal data transferred to organisations in the U.S., different limitations and safeguards apply. In general, the collection of data in bulk is specifically prohibited under Section 402 FISA (pen register and trap and trace authority) and through the use of NSL, and the use of specific 'selection terms' is instead required ⁽²⁸¹⁾.
- (149) To conduct traditional individualized electronic surveillance (pursuant to Section 105 FISA), intelligence agencies must submit an application to the FISC with a statement of the facts and circumstances relied upon to justify the belief that there is probable cause that the facility is used or about to be used by a foreign power or an agent of a foreign power ⁽²⁸²⁾. The FISC will assess, among others, whether on the basis of the submitted facts there is probable cause that this is indeed the case ⁽²⁸³⁾.
- (150) To carry out a search of premises or property that is intended to result in an inspection, seizure, etc. of information, material, or property (e.g. a computer device) on the basis of Section 301 FISA, an application for an order by the FISC is required ⁽²⁸⁴⁾. Such application must, inter alia, show that there is probable cause that the target of the search is a foreign power or an agent of a foreign power; that the premise or property to be searched contains foreign intelligence information and that the premise to be searched is owned, used, possessed by, or is in transit to or from an (agent of a) foreign power ⁽²⁸⁵⁾.
- (151) Similarly, the installation of pen registers or trap and trace devices (pursuant to Section 402 FISA) requires an application for an order by the FISC (or a U.S. Magistrate Judge) and the use of a specific selection term, i.e. a term that specifically identifies a person, account, etc. and is used to limit, to the greatest extent reasonably possible, the scope of the information sought ⁽²⁸⁶⁾. This authority does not concern the contents of communications, but rather aims at information about the customer or subscriber using a service (such as name, address, subscriber number, length/type of service received, source/mechanism of payment).
- (152) Section 501 FISA ⁽²⁸⁷⁾, which allows the collection of business records of a common carrier (i.e. any person or entity transporting people or property by land, rail, water or air for compensation), public accommodation facility (e.g. a hotel, motel or inn), vehicle rental facility, or physical storage facility (i.e. which provides space for or services related to the storage of goods and materials) ⁽²⁸⁸⁾, also requires an application to the FISC or a Magistrate Judge. This application must specify the records sought and the specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of foreign power ⁽²⁸⁹⁾.
- (153) Finally, NSL are authorised by different statutes and allow investigating agencies to obtain certain information (not including the content of communications) from certain entities (e.g. financial institutions, credit reporting agencies, electronic communication providers) contained in credit reports, financial records and electronic subscriber and transactional records ⁽²⁹⁰⁾. The NSL statute that authorises access to electronic communications may be used only by the FBI and requires that requests use a term that specifically identifies a person, entity, telephone number, or account and certify that the information is relevant to an authorized national security investigation to protect against international terrorism or clandestine intelligence activities ⁽²⁹¹⁾. Recipients of an NSL have the right to challenge it in court ⁽²⁹²⁾.

⁽²⁸¹⁾ 50 U.S. Code § 1842(c)(3) and, as regards NSL, 12 U.S.C. § 3414(a)(2); 15 U.S.C. § 1681u; 15 U.S.C. § 1681v(a); and 18 U.S.C. § 2709(a).

⁽²⁸²⁾ 'An agent of a foreign power' may include non-U.S. persons that engage in international terrorism or the international proliferation of weapons of mass destruction (including preparatory acts) (50 U.S.C. § 1801 (b)(1)).

⁽²⁸³⁾ 50 U.S.C. § 1804. See also § 1841(4) with respect to the choice of selection terms.

⁽²⁸⁴⁾ 50 U.S.C. § 1821(5).

⁽²⁸⁵⁾ 50 U.S.C. § 1823(a).

⁽²⁸⁶⁾ 50 U.S.C. § 1842 with § 1841(2) and Section 3127 of Title 18.

⁽²⁸⁷⁾ 50 U.S.C. § 1862.

⁽²⁸⁸⁾ 50 U.S.C. §§ 1861-1862.

⁽²⁸⁹⁾ 50 U.S.C. § 1862(b).

⁽²⁹⁰⁾ 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; and 18 U.S.C. § 2709.

⁽²⁹¹⁾ 18 U.S.C. § 2709(b).

⁽²⁹²⁾ E.g., 18 U.S.C. § 2709(d).

3.2.1.3. Further use of the information collected

- (154) The processing of personal data collected by U.S. intelligence agencies through signals intelligence is subject to a number of safeguards.
- (155) Firstly, each intelligence agency must ensure appropriate data security and prevent access by unauthorised persons to personal data collected through signals intelligence. In this respect, different instruments, including statute, guidelines and standards further specify the minimum information security requirements that have to be put in place (e.g. multifactor authentication, encryption, etc.) ⁽²⁹³⁾. Access to collected data must be limited to authorised, trained personnel with a need to know the information to perform their mission ⁽²⁹⁴⁾. More generally, intelligence agencies must provide appropriate training to their employees, including on procedures for reporting and addressing violations of the law (including EO 14086) ⁽²⁹⁵⁾.
- (156) Secondly, intelligence agencies must comply with Intelligence Community standards for accuracy and objectivity, in particular with respect to ensuring data quality and reliability, the consideration of alternative sources of information and objectivity in performing analyses ⁽²⁹⁶⁾.
- (157) Thirdly, as regards data retention, EO 14086 clarifies that personal data of non-U.S. persons is subject to the same retention periods as the ones that apply to the data of U.S. persons ⁽²⁹⁷⁾. Intelligence agencies are required to define specific retention periods and/or the factors that must be taken into account to determine the length of applicable retention periods (e.g. whether the information is evidence of a crime; whether the information constitutes foreign intelligence information; whether the information is needed to protect the safety of persons or organisations, including victims or targets of international terrorism), which are laid down in different legal instruments ⁽²⁹⁸⁾.
- (158) Fourthly, specific rules apply as regards the dissemination of personal data collected through signals intelligence. As a general requirement, personal data on non-U.S. persons may only be disseminated if it involves the same type of information that can be disseminated about U.S. persons, e.g. information needed to protect the safety of a person or organisation (such as targets, victims or hostages of international terrorist organisations) ⁽²⁹⁹⁾. Moreover, personal data may not be disseminated solely because of a person's nationality or country of residence or for the purpose of circumventing the requirements of EO 14086 ⁽³⁰⁰⁾. Dissemination within the U.S. government may only take place if an authorised and trained individual has a reasonable belief that the recipient has a need to know the

⁽²⁹³⁾ Section 2(c)(iii)(B)(1) EO 14086. See also Title VIII of the National Security Act (detailing the requirements for access to classified information), E.O. 12333 section 1.5 (requiring the Heads of Intelligence Community Agencies to follow information sharing and security guidelines, information privacy, and other legal requirements), National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems" (directing the Committee on National Security Systems to provide system security guidance for national security systems to executive departments and agencies), and National Security Memorandum 8, "Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems" (establishing timelines and guidance for how cybersecurity requirements will be implemented for national security systems, including multifactor authentication, encryption, cloud technologies, and endpoint detection services).

⁽²⁹⁴⁾ Section 2(c)(iii)(B)(2) EO 14086. In addition, personal data for which no final retention determination has been made may only be accessed in order to make or support such a determination or to conduct authorised administrative, testing, development, security or oversight functions (Section 2(c)(iii)(B)(3) EO 14086).

⁽²⁹⁵⁾ Section 2(d)(ii) EO 14086.

⁽²⁹⁶⁾ Section 2(c)(iii)(C) EO 14086.

⁽²⁹⁷⁾ Section 2(c)(iii)(A)(2)(a)-(c) EO 14086. More generally, each agency must put in place policies and procedures designed to minimise the dissemination and retention of personal data collected through signals intelligence (Section 2(c)(iii)(A) EO 14086).

⁽²⁹⁸⁾ See e.g. Section 309 of the Intelligence Authorization Act for Fiscal Year 2015; minimisation procedures adopted by individual intelligence agencies under Section 702 FISA and authorised by the FISC; procedures approved by the Attorney General and the FRA (requiring U.S. federal agencies, including national security agencies, to establish retention periods for their records that must be approved by the National Archives and Record Administration).

⁽²⁹⁹⁾ Section 2(c)(iii)(A)(1)(a) and 5(d) EO 14086, in conjunction with Section 2.3 EO 12333.

⁽³⁰⁰⁾ Section 2(c)(iii)(A)(1)(b) and (e) EO 14086.

information ⁽³⁰¹⁾ and will protect it appropriately ⁽³⁰²⁾. To determine whether personal data can be disseminated to recipients outside the U.S. government (including a foreign government or international organisation), the purpose of the dissemination, the nature and extent of the data being disseminated, and the potential for harmful impact on the person(s) concerned must be taken into account ⁽³⁰³⁾.

- (159) Finally, including in order to facilitate oversight of compliance with the applicable legal requirements as well as effective redress, each intelligence agency is required under EO 14086 to keep appropriate documentation about the collection of signals intelligence. The documentation requirements cover elements such as the factual basis for the assessment that a specific collection activity is necessary to advance a validated intelligence priority ⁽³⁰⁴⁾.
- (160) In addition to the abovementioned safeguards of EO 14086 for the use of information collected through signals intelligence, all US intelligence agencies are subject to more general requirements on purpose limitation, data minimisation, accuracy, security, retention and dissemination, following in particular from OMB Circular No. A-130, the E-Government Act, the Federal Records Act (see recitals 101-106) and guidance from the Committee on National Security Systems (CNSS) ⁽³⁰⁵⁾.

3.2.2. *Oversight*

- (161) The activities of U.S. intelligence agencies are subject to supervision by different bodies.
- (162) Firstly, EO 14086 requires each intelligence agency to have senior-level legal, oversight and compliance officials to ensure compliance with applicable U.S. law ⁽³⁰⁶⁾. In particular, they must conduct periodic oversight of signals intelligence activities and ensure that any non-compliance is remedied. Intelligence agencies must provide such officials with access to all relevant information to carry out their oversight functions and may not take any actions to impede or improperly influence their oversight activities ⁽³⁰⁷⁾. Moreover, any significant non-compliance incident ⁽³⁰⁸⁾ identified by an oversight official or any other employee must promptly be reported to the head of the intelligence agency and the Director of National Intelligence, who must ensure that any necessary actions are taken to remediate and prevent the recurrence of the significant incident of non-compliance ⁽³⁰⁹⁾.
- (163) This oversight function is fulfilled by officers with a designated compliance role, as well as Privacy and Civil Liberties Officers and Inspectors General ⁽³¹⁰⁾.

⁽³⁰¹⁾ See e.g., the AGG-DOM for instance provides that the FBI may only disseminate information if the recipient has a need to know to accomplish the recipient's mission or to protect the public.

⁽³⁰²⁾ Section 2(c)(iii)(A)(1)(c) EO 14086. Intelligence agencies may for instance disseminate information in circumstances relevant to a criminal investigation or relating to a crime, including for example by disseminating warnings of threats of killing, serious bodily injury, or kidnapping; disseminating cyber threat, incident, or intrusion response information; and notifying victims or warning potential victims of crime.

⁽³⁰³⁾ Section 2(c)(iii)(A)(1)(d) EO 14086.

⁽³⁰⁴⁾ Section 2(c)(iii)(E) EO 14086.

⁽³⁰⁵⁾ See CNSS Policy No. 22, Cybersecurity Risk Management Policy and CNSS Instruction 1253, which provides detailed guidance on security measures to be put in place for national security systems.

⁽³⁰⁶⁾ Section 2(d)(i)(A)-(B) EO 14086.

⁽³⁰⁷⁾ Sections 2(d)(i)(B)-(C) EO 14086.

⁽³⁰⁸⁾ I.e. a systemic or intentional failure to comply with applicable U.S. law that could impugn the reputation or integrity of an element of the Intelligence Community or otherwise call into question the propriety of an Intelligence Community activity, including in light of any significant impact on the privacy and civil liberties interests of the person or persons concerned, see Section 5(l) EO 14086.

⁽³⁰⁹⁾ Section 2(d)(iii) EO 14086.

⁽³¹⁰⁾ Section 2(d)(i)(B) EO 14086.

- (164) As is the case with respect to criminal law enforcement authorities, Privacy and Civil Liberties Officers exist at all intelligence agencies ⁽³¹¹⁾. The powers of these officers typically encompass the supervision of procedures to ensure that the respective department/agency is adequately considering privacy and civil liberties concerns and has put in place adequate procedures to address complaints from individuals who consider that their privacy or civil liberties have been violated (and in some cases, like the Office of the Director of National Intelligence (ODNI), may themselves have the power to investigate complaints ⁽³¹²⁾). The heads of intelligence agencies must ensure that Privacy and Civil Liberties Officers have the resources to fulfil their mandate, are given access to any material and personnel necessary to carry out their functions, and are informed about and are consulted on proposed policy changes ⁽³¹³⁾. Privacy and Civil Liberties Officers periodically report to Congress and the PCLOB, including on the number and nature of the complaints received by the department/agency with a summary of the disposition of such complaints, the reviews and inquiries conducted and the impact of the activities carried out by the Officer ⁽³¹⁴⁾.
- (165) Secondly, each intelligence agency has an independent Inspector General with the responsibility, among others, to oversee foreign intelligence activities. This includes, within the ODNI, an Office of the Inspector General of the Intelligence Community with comprehensive jurisdiction over the entire Intelligence Community which is authorised to investigate complaints or information concerning allegations of unlawful conduct, or abuse of authority, in connection with ODNI and/or Intelligence Community programs and activities ⁽³¹⁵⁾. As is the case for criminal law enforcement authorities (see recital 109), such Inspectors General are statutorily independent ⁽³¹⁶⁾ and responsible for conducting audits and investigations relating to the programs and operations carried out by the respective agency for national intelligence purposes, including with respect to abuse or violation of the law ⁽³¹⁷⁾.

⁽³¹¹⁾ See 42 U.S.C. § 2000ee-1. This includes for instance the Department of State, the Department of Justice, the Department of Homeland Security, the Department of Defense, the NSA, Central Intelligence Agency (CIA), FBI and the ODNI.

⁽³¹²⁾ See Section 3(c) EO 14086.

⁽³¹³⁾ 42 U.S.C. § 2000ee-1(d).

⁽³¹⁴⁾ See 42 U.S.C. § 2000ee-1 (f)(1),(2). For example the report of the NSA's Civil Liberties, Privacy and Transparency Office covering January 2021 – June 2021 shows that it carried out 591 reviews for civil liberties and privacy impacts in various contexts, e.g. with respect to collection activities, information-sharing arrangements and decisions, data retention decisions, etc., taking into account different factors, such as the amount and type of information associated with the activity, the individuals involved, the purpose and anticipated use for the data, the safeguards in place to mitigate potential risks to privacy, etc. (https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/REPORT%20CLPT%20JANUARY%20-%20JUNE%202021%20_FINAL.PDF). Similarly, the reports of the CIA's Office of Privacy and Civil Liberties for January – June 2019 provide information on the Office's oversight activities, e.g. a review of compliance with Attorney General Guidelines under EO 12333 with respect to the retention and dissemination of information, guidance provided on the implementation of PPD 28 and requirements to identify and address data breaches, and reviews of the use and handling of personal information (<https://www.cia.gov/static/9d762fbef6669c7e6d7f17e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi-Annual-Report.pdf>).

⁽³¹⁵⁾ This Inspector General is appointed by the President, with Senate confirmation, and can be removed only by the President.

⁽³¹⁶⁾ Inspectors General have secure tenure and may only be removed by the President who must communicate to Congress in writing the reasons for any such removal. This does not necessarily mean that they are completely free from instructions. In some cases, the head of the department may prohibit the Inspector General from initiating, carrying out, or completing an audit or investigation where this is considered necessary to preserve important national (security) interests. However, Congress must be informed of the exercise of this authority and on this basis could hold the respective director responsible. See, e.g. Inspector General Act of 1978, § 8 (for the Department of Defense); § 8E (for the DOJ), § 8G (d)(2)(A),(B) (for the NSA); 50. U.S.C. § 403q (b) (for the CIA); Intelligence Authorization Act For Fiscal Year 2010, Sec 405(f) (for the Intelligence Community).

⁽³¹⁷⁾ Inspector General Act of 1978, as amended, Pub. L. 117-108 of 8 April 2022. For example, as explained in its semi-annual reports to Congress covering the period 1 April 2021 to 31 March 2022, the NSA Inspector General carried out evaluations of the handling of U.S. person information collected under EO 12333, the process to purge signals intelligence data, an automated targeting tool used by the NSA, and compliance with documentation and querying rules with respect to Section 702 FISA collection, and issued several recommendations in this context (see <https://oig.nsa.gov/Portals/71/Reports/SAR/NSA%20OIG%20SAR%20-%20APR%202021%20-%20SEP%202021%20-%20UNCLASSIFIED.pdf?ver=1wttrthntGdfEb-EKTOm3gg%3d%3d>, pp. 5-8 and <https://oig.nsa.gov/Portals/71/Images/NSAOIGMAR2022.pdf?ver=jbq2rCrJ00HJ9qDXGHqHLw%3d%3d×tamp=1657810395907>, pp. 10-13). See also the recent audits and investigations carried out by the Inspector General of the Intelligence Community on information security and unauthorised disclosures of classified national security information (https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf, pp. 8, 11 and https://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21_SAR/Oct%202021-Mar%202022%20ICIG%20SAR_Unclass_FINAL.pdf, pp. 19-20).

They have access to all records, reports, audits, reviews, documents, papers, recommendations or other relevant material, if need be by subpoena, and may take testimony ⁽³¹⁸⁾. Inspectors General refer cases of suspected criminal violations for prosecution and make recommendations for corrective action to agency heads ⁽³¹⁹⁾. While their recommendations are non-binding, their reports, including on follow-up action (or the lack thereof) ⁽³²⁰⁾ are generally made public and sent to Congress, which can on this basis exercise its own oversight function (see recitals 168-169) ⁽³²¹⁾.

(166) Thirdly, the Intelligence Oversight Board (IOB), which is established within the President's Intelligence Advisory Board (PIAB), oversees compliance by U.S. intelligence authorities with the Constitution and all applicable rules ⁽³²²⁾. The PIAB is an advisory body within the Executive Office of the President that consists of 16 members appointed by the President from outside the U.S. government. The IOB consists of a maximum of five members designated by the President from among PIAB members. According to EO 12333 ⁽³²³⁾, the heads of all intelligence agencies are required to report any intelligence activity for which there is reason to believe that it may be unlawful or contrary to an Executive Order or Presidential Directive to the IOB. To ensure that the IOB has access to the information necessary to perform its functions, Executive Order 13462 directs the Director of National Intelligence and heads of intelligence agencies to provide any information and assistance the IOB determines is needed to perform its functions, to the extent permitted by law ⁽³²⁴⁾. The IOB is in turn required to inform the President about intelligence activities it believes may be in violation of U.S. law (including Executive Orders) and are not being adequately addressed by the Attorney General, Director of National Intelligence or the head of an intelligence agency ⁽³²⁵⁾. In addition, the IOB is required to inform the Attorney General about possible violations of criminal law.

(167) Fourthly, intelligence agencies are subject to oversight by the PCLOB. According to its founding statute, the PCLOB is entrusted with responsibilities in the field of counterterrorism policies and their implementation, with a view to protect privacy and civil liberties. In its review of intelligence agencies actions, it can access all relevant agency records, reports, audits, reviews, documents, papers and recommendations, including classified information, conduct interviews and hear testimony ⁽³²⁶⁾. It receives reports from the civil liberties and privacy officers of several federal departments/agencies ⁽³²⁷⁾, may issue recommendations to the government and intelligence agencies, and regularly reports to Congressional committees and the President ⁽³²⁸⁾. Reports of the Board, including the ones to Congress, must be made publicly available to the greatest extent possible ⁽³²⁹⁾. The PCLOB has issued several oversight and follow-up reports, including an analysis of the programs run on the basis of Section 702 FISA and the protection of privacy in this context, the implementation of PPD 28 and EO 12333 ⁽³³⁰⁾. The PCLOB is also charged

⁽³¹⁸⁾ See Inspector General Act of 1978, § 6.

⁽³¹⁹⁾ See *ibid.* §§ 4, 6-5.

⁽³²⁰⁾ As regards the follow-up that is provided to reports and recommendations of Inspectors General, see e.g. the response to a report of the DoJ Inspector General that found that the FBI was not sufficiently transparent with the FISC in applications from 2014 to 2019, which led to reforms to enhance compliance, oversight, and accountability at the FBI (e.g. the FBI Director ordered more than 40 corrective actions, including 12 specific to the FISA process relating to documentation, supervision, file maintenance, training and audits) (see <https://www.justice.gov/opa/pr/departments-justice-and-federal-bureau-investigation-announce-critical-reforms-enhance> and <https://oig.justice.gov/reports/2019/o20012.pdf>). See for instance also the DoJ Inspector General's audit of the FBI Office of the General Counsel's roles and responsibilities in overseeing compliance with applicable laws, policies, and procedures relating to the FBI's national security activities and Appendix 2, which includes a letter from the FBI accepting all recommendations. In this respect, Appendix 3 provides an overview of the follow-up action and information the Inspector General required from the FBI in order to be able to close its recommendations (<https://oig.justice.gov/sites/default/files/reports/22-116.pdf>).

⁽³²¹⁾ See Inspector General Act of 1978, §§ 4(5), 5.

⁽³²²⁾ See EO 13462.

⁽³²³⁾ Section 1.6(c) EO 12333.

⁽³²⁴⁾ Section 8(a) EO 13462.

⁽³²⁵⁾ Section 6(b) EO 13462.

⁽³²⁶⁾ 42 U.S.C. § 2000ee (g).

⁽³²⁷⁾ See 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). These include at least the Department of Justice, the Department of Defense, the Department of Homeland Security, the Director of National Intelligence and the Central Intelligence Agency, plus any other department, agency or element of the executive branch designated by the PCLOB to be appropriate for coverage.

⁽³²⁸⁾ 42 U.S.C. § 2000ee (e).

⁽³²⁹⁾ 42 U.S.C. § 2000ee (f).

⁽³³⁰⁾ Available at <https://www.pclob.gov/Oversight>.

with carrying out specific oversight functions as regards the implementation of EO 14086, in particular by reviewing whether agency procedures are consistent with the EO (see recital 126) and evaluating the correction functioning of the redress mechanism (see recital 194).

(168) Fifthly, in addition to the oversight mechanisms within the executive branch, specific Committees in the U.S. Congress (the House and Senate Intelligence and Judiciary Committees) have oversight responsibilities regarding all U.S. foreign intelligence activities. Members of these Committees have access to classified information as well as intelligence methods and programs ⁽³³¹⁾. The Committees exercise their oversight functions in different ways, in particular through hearings, investigations, reviews and reports ⁽³³²⁾.

(169) The Congressional Committees receive regular reports on intelligence activities, including from the Attorney General, the Director of National Intelligence, intelligence agencies and other oversight bodies (e.g. Inspectors General), see recitals 164-165. In particular, according to the National Security Act, "[t]he President shall ensure that the congressional intelligence committees are kept fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence activity as required by this subchapter" ⁽³³³⁾. In addition, "[t]he President shall ensure that any illegal intelligence activity is reported promptly to the congressional intelligence committees, as well as any corrective action that has been taken or is planned in connection with such illegal activity" ⁽³³⁴⁾.

(170) Moreover, additional reporting requirements follow from specific statutes. In particular, FISA requires the Attorney General to "fully inform" the Senate and House Intelligence and Judiciary Committees regarding the government's activities under certain sections of FISA ⁽³³⁵⁾. It also requires the government to provide the Congressional committees with copies of all decisions, orders, or opinions of the FISC or FISCR that include "significant construction or interpretation" of FISA provisions. As regards surveillance under Section 702 FISA, parliamentary oversight is exercised through statutorily required reports to the Intelligence and Judiciary Committees, as well as frequent briefings and hearings. These include a semi-annual report by the Attorney General describing the use of Section 702 FISA, with supporting documents, including Department of Justice and ODNI compliance reports and a description of any incidents of non-compliance ⁽³³⁶⁾, and a separate semi-annual assessment by the Attorney General and the DNI documenting compliance with the targeting and minimization procedures ⁽³³⁷⁾.

⁽³³¹⁾ 50 U.S.C. § 3091.

⁽³³²⁾ For example, the Committees organise thematic hearings (see e.g. a recent hearing of the House Judiciary Committee on "digital dragnets", <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983>, and a hearing of the House Intelligence Committee on the use of AI by the Intelligence Community, <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263>) regular oversight hearings, e.g. of the FBI and DoJ national security division, see <https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation>; <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966> and <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899>. As an example of an investigation, see the Senate Intelligence Committee investigation of Russian interference in the 2016 U.S. elections, see <https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures>. In terms of reporting, see e.g. the overview of the Committee's (oversight) activities in the report of the Senate Intelligence Committee covering the period 4 January 2019 – 3 January 2021 to the Senate, <https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4>.

⁽³³³⁾ See 50 U.S.C. § 3091(a)(1). This provision contains the general requirements as regards Congressional oversight in the area of national security.

⁽³³⁴⁾ See 50 U.S.C. § 3091(b).

⁽³³⁵⁾ See 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.

⁽³³⁶⁾ See 50 U.S.C. § 1881f.

⁽³³⁷⁾ See 50 U.S.C. § 1881a(l)(1).

- (171) In addition, FISA requires the U.S. government to disclose to Congress (and the public) each year the number of FISA orders sought and received, as well as estimates of the number of U.S. and non-U.S. persons targeted by surveillance, among others ⁽³³⁸⁾. The Act also requires additional public reporting about the number of NSL issued, again both with regard to U.S. and non-U.S. persons (while at the same time allowing the recipients of FISA orders and certifications, as well as NSL requests, to issue transparency reports under certain conditions) ⁽³³⁹⁾.
- (172) More generally, the U.S. Intelligence Community undertakes various efforts to provide transparency about its (foreign) intelligence activities. For example, in 2015, the ODNI adopted Principles of Intelligence Transparency and a Transparency Implementation Plan, and directed each intelligence agency to designate an Intelligence Transparency Officer to foster transparency and lead transparency initiatives ⁽³⁴⁰⁾. As part of these efforts, the Intelligence Community has made and continues to make declassified parts of policies, procedures, oversight reports, reports on activities under Section 702 FISA and EO 12333, FISC decisions and other materials public, including on a dedicated webpage 'IC on the Record', managed by ODNI ⁽³⁴¹⁾.
- (173) Finally, the collection of personal data pursuant to Section 702 FISA is, in addition to the supervision by oversight bodies mentioned in recitals 162-168, subject to oversight by the FISC ⁽³⁴²⁾. Pursuant to Rule 13 of the FISC Rules of Procedure, compliance officers in U.S. intelligence agencies are required to report any violations of FISA 702 targeting, minimization, and querying procedures to the DoJ and ODNI, who in turn report them to the FISC. Moreover, the DoJ and ODNI submit semi-annual joint oversight assessment reports to the FISC, which identify targeting compliance trends; provide statistical data; describe categories of compliance incidents; describe in detail the reasons certain targeting compliance incidents occurred, and outline the measures intelligence agencies have taken to avoid recurrence ⁽³⁴³⁾.
- (174) Where necessary (e.g. if violations of targeting procedures are identified), the Court may order the relevant intelligence agency to take remedial action ⁽³⁴⁴⁾. The remedies in question may range from individual to structural measures, e.g. from terminating data acquisition and deleting of unlawfully obtained data to a change in the collection practice, including in terms of guidance and training for staff ⁽³⁴⁵⁾. Moreover, during its annual review of

⁽³³⁸⁾ 50 U.S.C. § 1873(b). In addition, according to Section 402, "the Director of National Intelligence, in consultation with the Attorney General, shall conduct a declassification review of each decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review (as defined in section 601(e)) that includes a significant construction or interpretation of any provision of law, including any novel or significant construction or interpretation of the term "specific selection term", and, consistent with that review, make publicly available to the greatest extent practicable each such decision, order, or opinion".

⁽³³⁹⁾ 50 U.S.C. §§ 1873(b)(7) and 1874.

⁽³⁴⁰⁾ <https://www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic>.

⁽³⁴¹⁾ See 'IC on the Record', available at <https://icontherecord.tumblr.com/>.

⁽³⁴²⁾ In the past, the FISC concluded that "[i]t is apparent to the Court that the implementing agencies, as well as [ODNI] and [DOJ's National Security Division], devote substantial resources to their compliance and oversight responsibilities under Section 702. As a general rule, instances of non-compliance are identified promptly and appropriate remedial actions are taken, to include purging information that was improperly obtained or otherwise subject to destruction requirements under applicable procedures". FISA Court, Memorandum Opinion and Order [caption redacted] (2014), available at <https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf>.

⁽³⁴³⁾ See, e.g., DOJ/ODNI FISA 702 Compliance Report to FISC for June 2018 – Nov. 2018 at 21-65.

⁽³⁴⁴⁾ 50 U.S.C. § 1803(h). See also PCLOB, Section 702 Report, p. 76. In addition, see FISC Memorandum Opinion and Order of 3 October 2011 as an example of a deficiency order in which the government was ordered to correct the identified deficiencies within 30 days. Available at <https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf>. See Walton Letter, Section 4, pp. 10 -11. See also FISC Opinion of 18 October 2018, available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, as confirmed by the Foreign Intelligence Court of Review in its Opinion of 12 July 2019, available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_12Jul19.pdf, in which the FISC inter alia ordered the government to comply with certain notification, documentation and reporting requirements towards the FISC.

⁽³⁴⁵⁾ See e.g. FISC, Memorandum Opinion and Order at 76 (6 Dec. 2019) (Authorised for Public Release on 4 September 2020), in which the FISC directed the government to submit a written report by 28 February 2020 on the steps the government was taking to improve processes for identifying and removing reports derived from FISA 702 information that were recalled for compliance reasons, as well as on other matters. See also Annex VII.

Section 702 certifications, the FISC considers non-compliance incidents to determine if the submitted certifications comply with FISA requirements. Similarly, if the FISC finds that the government's certifications were not sufficient, including because of particular compliance incidents, it can issue a so-called 'deficiency order' requiring the government to remedy the violation within 30 days or requiring the government to cease or not begin implementing the Section 702 certification. Finally, the FISC assesses trends it observes in compliance issues and may require changes to procedures or additional oversight and reporting to address compliance trends ⁽³⁴⁶⁾.

3.2.3. Redress

- (175) As explained in more detail in this section, a number of avenues in the United States provide Union data subjects with the possibility to bring legal action before an independent and impartial tribunal with binding powers. Together, they allow individuals to have access to their personal data, to have the lawfulness of government access to their data reviewed and, if a violation is found, to have such violation remedied, including through the rectification or erasure of their personal data.
- (176) First, a specific redress mechanism is established, under EO 14086, complemented by the AG Regulation establishing the Data Protection Review Court, to handle and resolve complaints from individuals concerning U.S. signals intelligence activities. Any individual in the EU is entitled to submit a complaint to the redress mechanism concerning an alleged violation of U.S. law governing signals intelligence activities (e.g. EO 14086, Section 702 FISA, EO 12333) that adversely affects their privacy and civil liberties interests ⁽³⁴⁷⁾. This redress mechanism is available to individuals from countries or regional economic integration organisations that have been designated by the U.S. Attorney General as 'qualifying states' ⁽³⁴⁸⁾. On 30 June 2023, the European Union and the three European Free Trade Association countries that together constitute the European Economic Area have been designated by the Attorney General under Section 3(f) EO 14086 as a 'qualifying state' ⁽³⁴⁹⁾. This designation is without prejudice to Article 4(2) of the Treaty on the European Union.
- (177) A Union data subject who wishes to lodge such a complaint must submit it to a supervisory authority in an EU Member State competent for the oversight of the processing of personal data by public authorities (a DPA) ⁽³⁵⁰⁾. This ensures easy access to the redress mechanism by allowing individuals to turn to an authority 'close to home' and with which they can communicate in their own language. After the requirements for filing a complaint referred to in recital 178 have been verified, the competent DPA will channel, via the secretariat of the European Data Protection Board, the complaint to the redress mechanism.
- (178) Bringing a complaint to the redress mechanism is subject to low admissibility requirements, as individuals do not need to demonstrate that their data has in fact been subject to U.S. signals intelligence activities ⁽³⁵¹⁾. At the same time, to provide a starting point for the redress mechanism to carry out a review, certain basic information must be provided, e.g. regarding the personal data reasonably believed to have been transferred to the U.S. and the means by which it was believed to have been transferred; the identities of the U.S. Government entities believed to be involved in the alleged violation (if known); the basis for alleging that a violation of U.S. law occurred (although this again does not require showing that personal data was in fact collected by U.S. intelligence agencies) and the nature of the relief sought.

⁽³⁴⁶⁾ See Annex VII.

⁽³⁴⁷⁾ See Section 4(k)(iv) EO 14086, which provides that a complaint to the redress mechanism must be brought by a complainant acting on his/her own behalf (i.e. not as a representative of a government, nongovernmental or intergovernmental organisation). The notion of "adversely affected" does not require the complainant to meet a certain threshold in order to have access to the redress mechanism (see recital 178 in this regard). Rather, it clarifies that the ODNI CLPO and DPRC have the authority to remediate violations of U.S. law governing signals intelligence activities that adversely affect a complainant's individual privacy and civil liberties interests. Conversely, violations of requirements under applicable US law that are not designed to protect individuals (e.g. budgetary requirements), would fall outside the jurisdiction of the ODNI CLPO and DPRC.

⁽³⁴⁸⁾ Section 3(f) EO 14086.

⁽³⁴⁹⁾ <https://www.justice.gov/opcl/executive-order-14086>.

⁽³⁵⁰⁾ Section 4(d)(v) EO 14086.

⁽³⁵¹⁾ See Section 4(k)(i)-(iv) EO 14086.

- (179) The initial investigation of complaints to this redress mechanism is carried out by the ODNI CLPO, whose existing statutory role and powers have been expanded for those specific actions taken pursuant to EO 14086 ⁽³⁵²⁾. Within the Intelligence Community, the CLPO is, inter alia, responsible for ensuring that the protection of civil liberties and privacy is appropriately incorporated in policies and procedures of the ODNI and intelligence agencies; overseeing compliance by the ODNI with applicable civil liberties and privacy requirements; and conducting privacy impact assessments ⁽³⁵³⁾. The ODNI CLPO can only be dismissed by the Director of National Intelligence for cause, i.e. in case of misconduct, malfeasance, breach of security, neglect of duty, or incapacity ⁽³⁵⁴⁾.
- (180) When conducting its review, the ODNI CLPO has access to the information for his/her assessment and can rely on the compelled assistance of Privacy and Civil Liberties Officers in the different intelligence agencies ⁽³⁵⁵⁾. Intelligence agencies are prohibited from impeding or improperly influencing the ODNI CLPO's reviews. This includes the Director of National Intelligence who must not interfere with the review ⁽³⁵⁶⁾. When reviewing a complaint, the ODNI CLPO must "apply the law impartially", having regard to both the national security interests in signal intelligence activities and privacy protections ⁽³⁵⁷⁾.
- (181) As part of its review, the ODNI CLPO determines whether a violation of applicable U.S. law has occurred and, if that is the case, decides on an appropriate remediation ⁽³⁵⁸⁾. The latter refers to measures that fully redress an identified violation, such as terminating unlawful acquisition of data, deleting unlawfully collected data, deleting the results of inappropriately conducted queries of otherwise lawfully collected data, restricting access to lawfully collected data to appropriately trained personnel, or recalling intelligence reports containing data acquired without lawful authorization or that were unlawfully disseminated ⁽³⁵⁹⁾. Decisions of the ODNI CLPO on individual complaints (including on the remediation) are binding on intelligence agencies concerned ⁽³⁶⁰⁾.
- (182) The ODNI CLPO must maintain documentation of its review and produce a classified decision explaining the basis for its factual findings, the determination with respect to whether a covered violation occurred and the determination of the appropriate remediation ⁽³⁶¹⁾. If the ODNI CLPO's review reveals a violation of any authority subject to the oversight of the FISC, the CLPO must also provide a classified report to the Assistant Attorney General for National Security, who in turn under an obligation to report the non-compliance to the FISC, which can take further enforcement action (in accordance with the procedure described in recitals 173-174) ⁽³⁶²⁾.
- (183) Once the review is completed, the ODNI CLPO informs the complainant, through the national authority, that "the review either did not identify any covered violations or the ODNI CLPO issued a determination requiring appropriate remediation" ⁽³⁶³⁾. This allows protection of the confidentiality of activities conducted to protect national security, while providing the individuals with a decision confirming that their complaint has been duly investigated and adjudicated. This decision can moreover be challenged by the individual. To this end, (s)he will be informed of the possibility to appeal to the DPRC for a review of the CLPO's determinations (see recitals 184 and further) and that, in case the Court would be seized, a special advocate will be selected to advocate regarding the complainant's interest ⁽³⁶⁴⁾.

⁽³⁵²⁾ Section 3(c)(iv) EO 14086. See also National Security Act 1947, 50 U.S.C. §403-3d, Section 103D concerning the role of the CLPO within the ODNI.

⁽³⁵³⁾ 50 U.S.C § 3029 (b).

⁽³⁵⁴⁾ Section 3(c)(iv) EO 14086.

⁽³⁵⁵⁾ Section 3(c)(iii) EO 14086.

⁽³⁵⁶⁾ Section 3(c)(iv) EO 14086.

⁽³⁵⁷⁾ Section 3(c)(i)(B)(i) and (iii) EO 14086.

⁽³⁵⁸⁾ Section 3(c)(i) EO 14086.

⁽³⁵⁹⁾ Section 4(a) EO 14086.

⁽³⁶⁰⁾ Section 3(c)(d) EO 14086.

⁽³⁶¹⁾ Section 3(c)(i)(F)-(G) EO 14086.

⁽³⁶²⁾ See also Section 3(c)(i)(D) EO 14086.

⁽³⁶³⁾ Section 3(c)(i)(E)(1) EO 14086.

⁽³⁶⁴⁾ Sections 3(c)(i)(E)(2)-(3) EO 14086.

- (184) Any complainant, as well as each element of the Intelligence Community, may seek review of the ODNI CLPO's decision before the Data Protection Review Court (DPRC). Such applications for review must be submitted within 60 days after receiving the notification from the ODNI CLPO that its review is complete and include any information the individual wishes to provide to the DPRC (e.g. arguments on questions of law or the application of law to the facts of the case) ⁽³⁶⁵⁾. Union data subjects may again submit their application to the competent DPA (see recital 177).
- (185) The DPRC is an independent tribunal established by the Attorney General on the basis of EO 14086 ⁽³⁶⁶⁾. It consists of at least six judges, appointed by the Attorney General in consultation with the PCLOB, the Secretary of Commerce and the Director of National Intelligence for renewable terms of four years ⁽³⁶⁷⁾. The appointment of judges by the Attorney General is informed by the criteria used by the executive branch when assessing candidates for the federal judiciary, giving weight to any prior judicial experience ⁽³⁶⁸⁾. In addition, the judges must be legal practitioners (i.e. active members in good standing of the bar and duly licensed to practice law) and have appropriate experience in privacy and national security law. The Attorney General must endeavour to ensure that at least half of the judges at any given time have prior judicial experience and all judges must hold security clearances to be able to access classified national security information ⁽³⁶⁹⁾.
- (186) Only individuals who meet the qualifications mentioned in recital 185 and are not employees of the executive branch at the time of their appointment or in the preceding two years can be appointed to the DPRC. Similarly, during their term of office at the DPRC, the judges may not have any official duties or employment within the U.S. Government (other than as judges at the DPRC) ⁽³⁷⁰⁾.
- (187) The independence of the adjudication process is achieved through a number of guarantees. In particular, the executive branch (the Attorney General and intelligence agencies) are barred from interfering with or improperly influencing the DPRC's review ⁽³⁷¹⁾. The DPRC itself is required to impartially adjudicate cases ⁽³⁷²⁾ and operates according to its own rules of procedure (adopted by majority vote). Moreover, DPRC judges may be dismissed only by the Attorney General and only for cause (i.e. misconduct, malfeasance, breach of security, neglect of duty or incapacity), after taking due account of the standards applicable to federal judges laid down in the Rules for Judicial-Conduct and Judicial-Disability Proceedings ⁽³⁷³⁾.

⁽³⁶⁵⁾ Sections 201.6(a)-(b) AG Regulation.

⁽³⁶⁶⁾ Section 3(d)(i) and the AG Regulation. The Supreme Court of the United States has recognised the possibility for the Attorney General to establish independent bodies with decision-making power, including to adjudicate individual cases, see in particular *United States ex rel. Accardi v. Shaughnessy*, 347 U.S. 260 (1954) and *United States v. Nixon*, 418 U.S. 683, 695 (1974). Compliance with the different requirements of EO 14086, e.g. the criteria and procedure for appointment and dismissal of DPRC judges, is notably subject to the supervision of the Inspector General of the Department of Justice (see also recital 109 on the statutory authority of Inspectors General).

⁽³⁶⁷⁾ Section 3(d)(i)(A) EO 14086 and Section 201.3(a) AG Regulation.

⁽³⁶⁸⁾ Section 201.3(b) AG Regulation.

⁽³⁶⁹⁾ Section 3(d)(i)(B) EO 14086.

⁽³⁷⁰⁾ Section 3(d)(i)(A) EO 14086 and Section 201.3(a) and (c) AG Regulation. Individuals appointed to the DPRC may participate in extrajudicial activities, including business, financial activities, non-profit fundraising and fiduciary activities, as well as the practice of law, as long as such activities do not interfere with the impartial performance of their duties or the effectiveness or independence of the DPRC (Section 201.7(c) AG Regulation).

⁽³⁷¹⁾ Sections 3(d)(iii)-(iv) EO 14086 and Section 201.7(d) AG Regulation.

⁽³⁷²⁾ Section 3(d)(i)(D) EO 14086 and Section 201.9 AG Regulation.

⁽³⁷³⁾ Section 3(d)(iv) EO 14086 and Section 201.7(d) AG Regulation. See also *Bumap v. United States*, 252 U.S. 512, 515 (1920), which confirmed the long-standing principle in US law that the power of removal is incident to the power to appoint (as also recalled by the Office of Legal Counsel of the DoJ in *The Constitutional Separation of Powers Between the President and Congress*, 20 Op. O.L. C. 124, 166 (1996)).

- (188) Applications to the DPRC are reviewed by panels of three judges, including a presiding judge, who must act in accordance with the Code of Conduct for U.S. Judges ⁽³⁷⁴⁾. Each panel is assisted by a Special Advocate ⁽³⁷⁵⁾, who has access to all information pertaining to the case, including classified information ⁽³⁷⁶⁾. The role of the Special Advocate is to ensure that the complainant's interests are represented and that the DPRC panel is well informed about all relevant issues of law and fact ⁽³⁷⁷⁾. To further inform its position on an application for review to the DPRC by an individual, the Special Advocate can seek information from the complainant through written questions ⁽³⁷⁸⁾.
- (189) The DPRC reviews the determinations made by the ODNI CLPO (both whether a violation of applicable U.S. law occurred and as regards the appropriate remediation) based, at a minimum, on the record of the ODNI CLPO's investigation, as well as any information and submissions provided by the complainant, the Special Advocate or an intelligence agency ⁽³⁷⁹⁾. A DPRC panel has access to all information necessary to conduct a review, which it may obtain through the ODNI CLPO (the panel may e.g. request the CLPO to supplement its record with additional information or factual findings if necessary to carry out the review) ⁽³⁸⁰⁾.
- (190) When concluding its review, the DPRC may (1) decide that there is no evidence indicating that signals intelligence activities occurred involving personal data of the complainant, (2) decide that the ODNI CLPO's determinations were legally correct and supported by substantial evidence, or (3) if the DPRC disagrees with the determinations of the ODNI CLPO (whether a violation of applicable U.S. law occurred or the appropriate remediation), issue its own determinations ⁽³⁸¹⁾.

⁽³⁷⁴⁾ Section 3(d)(i)(B) EO 14086 and Section 201.7(a)-(c) AG Regulation. The Office of Privacy and Civil Liberties of the Department of Justice (OPCL), which is responsible for providing administrative support to the DPRC and the Special Advocates (see Section 201.5 AG Regulation), selects a three-person panel on a rotating basis, seeking to ensure that each panel has at least one judge with prior judicial experience (if none of the judges on the panel has such experience, the presiding judge will be the judge first selected by the OPCL).

⁽³⁷⁵⁾ Section 201.4 AG Regulation. At least two Special Advocates are appointed by the Attorney General, in consultation with the Secretary of Commerce, the Director of National Intelligence, and the PCLOB, for two-renewable terms. Special Advocates must have appropriate experience in the field of privacy and national security law, be experienced attorneys, active members in good standing of the bar and duly licensed to practice law. In addition, at the time of their initial appointment, they must not have been employees of the Executive Branch for the preceding two years. For each review of an application, the presiding judge selects a Special Advocate to assist the panel, see Section 201.8(a) AG Regulation.

⁽³⁷⁶⁾ Section 201.8(c) and 201.11 AG Regulation.

⁽³⁷⁷⁾ Section 3(d)(i)(C) EO 14086 and Section 201.8(e) AG Regulation. The Special Advocate does not act as an agent of or have an attorney-client relationship with the complainant.

⁽³⁷⁸⁾ See Section 201.8(d)(e) AG Regulation. Such questions are first reviewed by the OPCL, in consultation with the relevant Intelligence Community element, with a view to identify and exclude any classified or privileged or protected information before forwarding it to complainant. Additional information received by the Special Advocate in response to such questions is included in the submissions of the Special Advocate to the DPRC.

⁽³⁷⁹⁾ Section 3(d)(i)(D) EO 14086.

⁽³⁸⁰⁾ Section 3(d)(iii) EO 14086 and Section 201.9(b) AG Regulation.

⁽³⁸¹⁾ Section 3(d)(i)(E) EO 14086 and Section 201.9(c)-(e) AG Regulation. According to the definition of 'appropriate remediation', in Section 4(a) EO 14086, the DPRC must take into account "the ways that a violation of the kind identified have customarily been addressed" when deciding on a remedial measure to fully address a violation, i.e. the DPRC will consider, among other factors, how similar compliance issues were remedied in the past to ensure that the remedy is effective and appropriate.

- (191) In all cases, the DPRC adopts a written decision by majority vote. In case the review reveals a violation of the applicable rules, the decision will specify any appropriate remediation, which includes deleting unlawfully collected data, deleting the results of inappropriately conducted queries, restricting access to lawfully collected data to appropriately trained personnel, or recalling intelligence reports containing data acquired without lawful authorization or that were unlawfully disseminated ⁽³⁸²⁾. The decision of the DPRC is binding and final with respect to the complaint before it ⁽³⁸³⁾. Moreover, if the review reveals a violation of any authority subject to the oversight of the FISC, the DPRC must also provide a classified report to the Assistant Attorney General for National Security, who in turn is under an obligation to report the non-compliance to the FISC, which can take further enforcement action (in accordance with the procedure described in recitals 173-174) ⁽³⁸⁴⁾.
- (192) Each decision of a DPRC panel is transmitted to the ODNI CLPO ⁽³⁸⁵⁾. In cases where the DPRC's review was triggered by an application from the complainant, the complainant is notified through the national authority that the DPRC completed its review and that "the review either did not identify any covered violations or the DPRC issued a determination requiring appropriate remediation" ⁽³⁸⁶⁾. The Office of Privacy and Civil Liberties of the DoJ maintains a record of all information reviewed by the DPRC and all decisions issued, which is made available for consideration as non-binding precedent for future DPRC panels ⁽³⁸⁷⁾.
- (193) The DoC is also required to maintain a record for each complainant who submitted a complaint ⁽³⁸⁸⁾. To enhance transparency, the DoC must, at least every five years, contact relevant intelligence agencies to verify whether information pertaining to a review by the DPRC has been declassified ⁽³⁸⁹⁾. If this is the case, the individual will be notified that such information may be available under applicable law (i.e. that (s)he may request access to under the Freedom of Information Act, see recital 199).
- (194) Finally, the correct functioning of this redress mechanism will be subject to regular and independent evaluation. More specifically, pursuant to EO 14086, the functioning of the redress mechanism is subject to annual review by the PCLOB, an independent body (see recital 110) ⁽³⁹⁰⁾. As part of this review, the PCLOB will, inter alia, assess whether the ODNI CLPO and DPRC has processed complaints in a timely manner; whether they have obtained full access to necessary information; whether the substantive safeguards of EO 14086 have been properly considered in the review process; and whether the Intelligence Community has fully complied with determinations made by the ODNI CLPO and DPRC. The PCLOB will produce a report on the outcome of its review to the President, Attorney General, Director of National Intelligence, head of intelligence agencies, the ODNI CLPO and congressional intelligence committees, that will also be made public in an unclassified version – and will in turn feed into the periodic review of the functioning of the present Decision that will be conducted by the Commission. The Attorney General, Director of National Intelligence, ODNI CLPO and heads of intelligence agencies are required to implement or otherwise address all recommendations included in such reports. In addition, the PCLOB will make an annual public certification as to whether the redress mechanism is processing complaints consistent with the requirements of EO 14086.

⁽³⁸²⁾ Section 4(a) EO 14086.

⁽³⁸³⁾ Section 3(d)(iii) EO 14086 and Section 201.9(g) AG Regulation. Given that the decision of the DPRC is final and binding, no other executive or administrative institution/body (including the President of the United States) can overrule the DPRC's decision. This was also confirmed in case law of the Supreme Court, which clarified that, by delegating the Attorney General's unique authority within the Executive Branch to issue binding decisions to an independent body, the Attorney General denies himself the ability to dictate the decision of that body in any way (see *United States ex rel. Accardi v. Shaughnessy*, 347 U.S. 260 (1954)).

⁽³⁸⁴⁾ Section 3(d)(i)(F) EO 14086 and Section 201.9(i) AG Regulation.

⁽³⁸⁵⁾ Section 201.9(h) AG Regulation.

⁽³⁸⁶⁾ Section 3(d)(i)(H) EO 14086 and Section 201.9(h) AG Regulation. As regards the nature of the notification see Section 201.9 (h)(3) AG Regulation.

⁽³⁸⁷⁾ Section 201.9(j) AG Regulation.

⁽³⁸⁸⁾ Section 3(d)(v)(A) EO 14086.

⁽³⁸⁹⁾ Section 3(d)(v) EO 14086.

⁽³⁹⁰⁾ Section 3(e) EO 14086. See also [https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20\(FINAL\).pdf](https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf).

(195) In addition to the specific redress mechanism established under EO 14086, redress avenues are available to all individuals (irrespective of nationality or place of residence) before ordinary U.S. courts ⁽³⁹¹⁾.

(196) In particular, FISA and a related statute provides the possibility for individuals to bring a civil action for money damages against the United States when information about them has been unlawfully and wilfully used or disclosed ⁽³⁹²⁾; to sue U.S. government officials acting in their personal capacity for money damages ⁽³⁹³⁾; and to challenge the legality of surveillance (and seek to suppress the information) in the event the U.S. government intends to use or disclose any information obtained or derived from electronic surveillance against the individual in judicial or administrative proceedings in the U.S. ⁽³⁹⁴⁾. More generally, if the government intends to use information obtained during intelligence operations against a suspect in a criminal case, constitutional and statutory requirements ⁽³⁹⁵⁾ impose obligations to disclose certain information so the defendant can challenge the legality of the Government's collection and use of the evidence.

(197) Moreover, there are several specific avenues to seek legal recourse against government officials for unlawful government access to, or use of personal data, including for purported national security purposes (i.e. the Computer Fraud and Abuse Act ⁽³⁹⁶⁾; Electronic Communications Privacy Act ⁽³⁹⁷⁾; and Right to Financial Privacy Act ⁽³⁹⁸⁾). All of these legal actions concern specific data, targets and/or types of access (e.g. remote access of a computer via the internet) and are available under certain conditions (e.g. intentional/wilful conduct, conduct outside of official capacity, harm suffered).

(198) A more general redress possibility is offered by the APA ⁽³⁹⁹⁾, according to which "any person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action", is entitled to seek judicial review ⁽⁴⁰⁰⁾. This includes the possibility to ask the court to "hold unlawful and set aside agency action, findings, and conclusions found to be [...] arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law" ⁽⁴⁰¹⁾. For example, a federal appellate court ruled on an APA claim in 2015 that the U.S. government's bulk collection of telephony metadata was not authorised by Section 501 FISA ⁽⁴⁰²⁾.

⁽³⁹¹⁾ Access to these avenues is subject to the showing of 'standing'. This standard, which applies to any individual regardless of nationality, stems from the 'case or controversy' requirement of the U.S. Const., Article III. According to the Supreme Court, this requires that (1) the individual has suffered an 'injury in fact' (i.e. an injury of a legally protected interest that is concrete and particularised and actual or imminent), (2) there is a causal connection between the injury and the conduct challenged before the court, and (3) it is likely, rather than speculative, that a favourable decision by the court will address the injury (see *Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992)).

⁽³⁹²⁾ 18 U.S.C. § 2712.

⁽³⁹³⁾ 50 U.S.C. § 1810.

⁽³⁹⁴⁾ 50 U.S.C. § 1806.

⁽³⁹⁵⁾ See, respectively, *Brady v. Maryland*, 373 U.S. 83 (1963) and the Jencks Act, 18 U.S.C. § 3500.

⁽³⁹⁶⁾ 18 U.S.C. § 1030.

⁽³⁹⁷⁾ 18 U.S.C. §§ 2701-2712.

⁽³⁹⁸⁾ 12 U.S.C. § 3417.

⁽³⁹⁹⁾ 5 U.S.C. § 702.

⁽⁴⁰⁰⁾ Generally, only "final" agency action — rather than "preliminary, procedural, or intermediate" agency action — is subject to judicial review. See 5 U.S.C. § 704.

⁽⁴⁰¹⁾ 5 U.S.C. § 706(2)(A).

⁽⁴⁰²⁾ *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015), The bulk telephony collection program challenged in these cases was terminated by the USA FREEDOM Act in 2015.

- (199) Finally, in addition to the redress avenues mentioned in recitals 176-198, any individual has the right to seek access to existing federal agency records under FOIA, including where these contain the individual's personal data ⁽⁴⁰³⁾. Gaining such access can also facilitate bringing proceedings before ordinary courts, including in support of showing standing. Agencies may withhold information that falls within certain enumerated exceptions, including access to classified national security information and information concerning law enforcement investigations ⁽⁴⁰⁴⁾, but complainants who are dissatisfied with the response have the possibility to challenge it by seeking administrative and, subsequently, judicial review (before federal courts) ⁽⁴⁰⁵⁾.
- (200) It follows from the above that when U.S. law enforcement and national security authorities access personal data falling within the scope of this Decision, such access is governed by a legal framework that lays down the conditions under which access can take place and ensures that access and further use of the data is limited to what is necessary and proportionate to the public interest objective pursued. These safeguards can be invoked by individuals who enjoy effective redress rights.

4. CONCLUSION

- (201) The Commission considers that the United States – through the Principles issued by the U.S. DoC – ensures a level of protection for personal data transferred from the Union to certified organisations in the United States under the EU-U.S. Data Privacy Framework that is essentially equivalent to the one guaranteed by Regulation (EU) 2016/679.
- (202) Moreover, the Commission considers that the effective application of the Principles is guaranteed by transparency obligations and the administration of the DPF by the DoC. In addition, taken as a whole, the oversight mechanisms and redress avenues in U.S. law enable infringements of the data protection rules to be identified and punished in practice and offer legal remedies to the data subject to obtain access to personal data relating to him/her and, eventually, the rectification or erasure of such data.
- (203) Finally, on the basis of the available information about the U.S. legal order, including the information contained in Annexes VI and VII, the Commission considers that any interference in the public interest, in particular for criminal law enforcement and national security purposes, by U.S. public authorities with the fundamental rights of the individuals whose personal data are transferred from the Union to the United States under the EU-U.S. Data Privacy Framework, will be limited to what is strictly necessary to achieve the legitimate objective in question, and that effective legal protection against such interference exists. Therefore, in the light of the above findings, it should be decided that the United States ensures an adequate level of protection within the meaning of Article 45 of Regulation (EU) 2016/679, interpreted in light of the Charter of Fundamental Rights of the European Union, for personal data transferred from the European Union to organisations certified under the EU-U.S. Data Privacy Framework.
- (204) Given that the limitations, safeguards and redress mechanism established by EO 14086 are essential elements of the U.S. legal framework on which the Commission's assessment is based, the adoption of this Decision is notably based on the adoption of updated policies and procedures to implement EO 14086 by all U.S. intelligence agencies and the designation of the Union as a qualifying organisation for the purpose of the redress mechanism that have taken place respectively on 3 July 2023 (see recital 126) and 30 June 2023 (see recital 176).

⁽⁴⁰³⁾ 5 U.S.C. § 552. Similar laws exist at State level.

⁽⁴⁰⁴⁾ If this is the case, the individual will normally only receive a standard reply by which the agency declines either to confirm or deny the existence of any records. See *ACLU v CIA*, 710 F.3d 422 (D.C. Cir. 2014). The criteria for and duration of classification are laid down in Executive Order 13526, which provides, as a general rule, that a specific date or event for declassification must be established based on the duration of the national security sensitivity of the information, at which time the information must be automatically declassified (see Section 1.5 of EO 13526).

⁽⁴⁰⁵⁾ The court makes a de novo determination of whether records are lawfully withheld and can compel the government to provide access to records (5 U.S.C. § 552(a)(4)(B)).

5. EFFECTS OF THIS DECISION AND ACTION OF DATA PROTECTION AUTHORITIES

- (205) Member States and their organs are required to take the measures necessary to comply with acts of the Union institutions, as the latter are presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality.
- (206) Consequently, a Commission adequacy decision adopted pursuant to Article 45(3) of Regulation (EU) 2016/679 is binding on all organs of the Member States to which it is addressed, including their independent supervisory authorities. In particular, transfers from a controller or processor in the Union to certified organisations in the United States may take place without the need to obtain any further authorisation.
- (207) It should be recalled that, pursuant to Article 58(5) of Regulation (EU) 2016/679 and as explained by the Court of Justice in the *Schrems* judgment ⁽⁴⁰⁶⁾, where a national data protection authority questions, including upon a complaint, the compatibility of a Commission adequacy decision with the fundamental rights of the individual to privacy and data protection, national law must provide it with a legal remedy to put those objections before a national court which may be required to make a reference for a preliminary ruling to the Court of Justice ⁽⁴⁰⁷⁾.

6. MONITORING AND REVIEW OF THIS DECISION

- (208) According to the case law of the Court of Justice ⁽⁴⁰⁸⁾, and as recognised in Article 45(4) of Regulation (EU) 2016/679, the Commission should continuously monitor relevant developments in the third country after the adoption of an adequacy decision in order to assess whether the third country still ensures an essentially equivalent level of protection. Such a check is required, in any event, when the Commission receives information giving rise to a justified doubt in that respect.
- (209) Therefore, the Commission should on an on-going basis monitor the situation in the United States as regards the legal framework and actual practice for the processing of personal data as assessed in this Decision. To facilitate this process, the U.S. authorities should promptly inform the Commission of material developments in the U.S. legal order that have an impact on the legal framework that is the object of this Decision, as well as any evolution in practices related to the processing of the personal data assessed in this Decision, both as regards the processing of personal data by certified organisations in the United States and the limitations and safeguards applicable to access to personal data by public authorities.
- (210) Moreover, in order to allow the Commission to effectively carry out its monitoring function, the Member States should inform the Commission about any relevant action undertaken by the national data protection authorities, in particular regarding queries or complaints by Union data subjects concerning the transfer of personal data from the Union to certified organisations in the United States. The Commission should also be informed about any indications that the actions of U.S. public authorities responsible for the prevention, investigation, detection or prosecution of criminal offences, or for national security, including any oversight bodies, do not ensure the required level of protection.

⁽⁴⁰⁶⁾ *Schrems*, paragraph 65.

⁽⁴⁰⁷⁾ *Schrems*, paragraph 65: "It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity."

⁽⁴⁰⁸⁾ *Schrems*, paragraph 76.

- (211) In application of Article 45(3) of Regulation (EU) 2016/679 ⁽⁴⁰⁹⁾, the Commission, following the adoption of this Decision, should periodically review whether the findings relating to the adequacy of the level of protection ensured by the United States under the EU-U.S. DPF are still factually and legally justified. Since in particular EO 14086 and the AG Regulation require the creation of new mechanisms and the implementation of new safeguards, this Decision should be subject to a first review within one year after its entry into force, to verify whether all relevant elements have been fully implemented and are functioning effectively in practice. Following that first review, and depending on its outcome, the Commission will decide in close consultation with the Committee established under Article 93(1) of Regulation (EU) 2016/679 and the European Data Protection Board on the periodicity of future reviews ⁽⁴¹⁰⁾.
- (212) To perform the reviews, the Commission should meet with the DoC, FTC and DoT accompanied, if appropriate, by other departments and agencies involved in the implementation of the EU-U.S. DPF, as well as, for matters pertaining to government access to data, representatives of the DoJ, ODNI (including the CLPO), other Intelligence Community elements, the DPRC as well as the Special Advocates. The participation in this meeting should be open to representatives of the members of the European Data Protection Board.
- (213) The reviews should cover all aspects of the functioning of this Decision with respect to the processing of personal data in the United States, and in particular the application and implementation of the Principles, with special attention paid to protections afforded in case of onward transfers; relevant case law developments; the effectiveness of the exercise of individual rights; the monitoring and enforcement of compliance with the Principles; as well as the limitations and safeguards with respect to government access, notably the implementation and application of the safeguards introduced by EO 14086, including through policies and procedures developed by intelligence agencies; the interplay between the EO 14086 and Section 702 FISA and EO 12333; and the effectiveness of the oversight mechanisms and redress avenues (including the functioning of the new redress mechanism established under EO 14086). In the context of such reviews, attention will also be paid to cooperation between the DPAs and competent authorities of the United States, including the development of guidance and other interpretative tools on the application of the Principles as well as on other aspects of the functioning of the Framework.
- (214) On the basis of the review, the Commission should prepare a public report to be submitted to the European Parliament and the Council.

7. SUSPENSION, REPEAL OR AMENDMENT OF THIS DECISION

- (215) Where available information, in particular information resulting from the monitoring of this Decision or provided by U.S. or Member States' authorities, reveals that the level of protection afforded to data transferred under this Decision may no longer be adequate, the Commission should promptly inform the competent U.S. authorities thereof and request that appropriate measures be taken within a specified, reasonable timeframe.
- (216) If, at the expiry of that specified timeframe, the competent U.S. authorities fail to take those measures or otherwise demonstrate satisfactorily that this Decision continues to be based on an adequate level of protection, the Commission will initiate the procedure referred to in Article 93(2) of Regulation (EU) 2016/679 with a view to partially or completely suspend or repeal this Decision.
- (217) Alternatively, the Commission will initiate that procedure with a view to amend the Decision, in particular by subjecting data transfers to additional conditions or by limiting the scope of the adequacy finding only to data transfers for which an adequate level of protection continues to be ensured.

⁽⁴⁰⁹⁾ According to Article 45(3) Regulation (EU) 2016/679, "[t]he implementing act shall provide for a mechanism for a periodic review, [...] which shall take into account all relevant developments in the third country or international organisation."

⁽⁴¹⁰⁾ Article 45(3) Regulation (EU) 2016/679 provides that a periodic review must take place "at least every four years". See also European Data Protection Board, Adequacy Referential, WP 254 rev. 01.

- (218) In particular, the Commission should initiate the procedure for suspension or repeal in case of:
- (a) indications that organisations that have received personal data from the Union under this Decision do not comply with the Principles and that such non-compliance is not effectively addressed by the competent oversight and enforcement bodies;
 - (b) indications that the U.S. authorities do not comply with the applicable conditions and limitations for access by U.S. public authorities for law enforcement and national security purposes to personal data transferred under the EU-U.S. DPF ; or
 - (c) failure to effectively address complaints by Union data subjects, including by the ODNI CLPO and/or the DPRC.
- (219) The Commission should also consider initiating the procedure leading to the amendment, suspension or repeal of this Decision if the competent U.S. authorities fail to provide the information or clarifications necessary for the assessment of the level of protection afforded to personal data transferred from the Union to the United States, or as regards compliance with this Decision. In this respect, the Commission should take into account the extent to which the relevant information can be obtained from other sources.
- (220) On duly justified imperative grounds of urgency, for example if EO 14086 or the AG Regulation would be amended in a way that undermines the level of protection described in this Decision or if the Attorney General's designation of the Union as a qualifying organisation for the purpose of the redress mechanism is withdrawn, the Commission will make use of the possibility to adopt, in accordance with the procedure referred to in Article 93(3) of Regulation (EU) 2016/679, immediately applicable implementing acts suspending, repealing or amending this Decision.

8. FINAL CONSIDERATIONS

- (221) The European Data Protection Board published its opinion ⁽⁴¹¹⁾, which has been taken into consideration in the preparation of this Decision.
- (222) The European Parliament adopted a resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework ⁽⁴¹²⁾.
- (223) The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 93(1) Regulation (EU) 2016/679.

HAS ADOPTED THIS DECISION:

Article 1

For the purpose of Article 45 of Regulation (EU) 2016/679, the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States that are included in the 'Data Privacy Framework List', maintained and made publicly available by the U.S. Department of Commerce, in accordance with Section I.3 of Annex I.

Article 2

Whenever the competent authorities in Member States, in order to protect individuals with regard to the processing of their personal data, exercise their powers pursuant to Article 58 of Regulation (EU) 2016/679 with respect to data transfers referred to in Article 1 of this Decision, the Member State concerned shall inform the Commission without delay.

⁽⁴¹¹⁾ Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework of 28 February 2023.

⁽⁴¹²⁾ European Parliament Resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP)).

Article 3

1. The Commission shall continuously monitor the application of the legal framework that is the object of this Decision, including the conditions under which onward transfers are carried out, individual rights are exercised and U.S. public authorities have access to data transferred on the basis of this Decision, with a view to assessing whether the United States continues to ensure an adequate level of protection as referred to in Article 1.
2. The Member States and the Commission shall inform each other of cases where it appears that the bodies in the United States with the statutory power to enforce compliance with the Principles set out in Annex I fail to provide effective detection and supervision mechanisms enabling infringements of the Principles set out in Annex I to be identified and punished in practice.
3. The Member States and the Commission shall inform each other of any indications that the interferences by U.S. public authorities responsible for the pursuit of national security, law enforcement or other public interests with the right of individuals to the protection of their personal data go beyond what is necessary and proportionate, and/or that there is no effective legal protection against such interferences.
4. After one year from the date of the notification of this Decision to the Member States and subsequently at a periodicity that will be decided in close consultation with the Committee established under Article 93(1) of Regulation (EU) 2016/679 and the European Data Protection Board, the Commission shall evaluate the finding referred to in Article 1(1) on the basis of all available information, including information obtained through the review carried out together with the competent authorities of the United States.
5. Where the Commission has indications that an adequate level of protection is no longer ensured, the Commission shall inform the competent U.S. authorities. If necessary, it will decide to suspend, amend or repeal this Decision, or limit its scope, in accordance with Article 45(5) of Regulation (EU) 2016/679. The Commission may also adopt such a decision if the lack of cooperation of the U.S. government prevents the Commission from determining whether the United States continues to ensure an adequate level of protection.

Article 4

This Decision is addressed to the Member States.

Done at Brussels, 10 July 2023.

For the Commission
Didier REYNERS
Member of the Commission

ANNEX I

EU-U.S. DATA PRIVACY FRAMEWORK PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE

I. OVERVIEW

1. While the United States and the European Union (the “EU”) share a commitment to enhancing privacy protection, the rule of law, and a recognition of the importance of transatlantic data flows to our respective citizens, economies, and societies, the United States takes a different approach to privacy protection from that taken by the EU. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. The U.S. Department of Commerce (“the Department”) is issuing the EU-U.S. Data Privacy Framework Principles, including the Supplemental Principles (collectively “the Principles”) and Annex I of the Principles (“Annex I”), under its statutory authority to foster, promote, and develop international commerce (15 U.S.C. § 1512). The Principles were developed in consultation with the European Commission (“the Commission”), industry, and other stakeholders to facilitate trade and commerce between the United States and EU. The Principles, a key component of the EU-U.S. Data Privacy Framework (“EU-U.S. DPF”), provide organizations in the United States with a reliable mechanism for personal data transfers to the United States from the EU while ensuring that EU data subjects continue to benefit from effective safeguards and protection as required by European legislation with respect to the processing of their personal data when they have been transferred to non-EU countries. The Principles are intended for use solely by eligible organizations in the United States receiving personal data from the EU for the purpose of qualifying for the EU-U.S. DPF and thus benefitting from the Commission’s adequacy decision.⁽¹⁾ The Principles do not affect the application of the Regulation (EU) 2016/679 (“the General Data Protection Regulation” or “the GDPR”) ⁽²⁾ that applies to the processing of personal data in the EU Member States. Nor do the Principles limit privacy obligations that otherwise apply under U.S. law.
2. In order to rely on the EU-U.S. DPF to effectuate transfers of personal data from the EU, an organization must self-certify its adherence to the Principles to the Department (or its designee). While decisions by organizations to thus enter the EU-U.S. DPF are entirely voluntary, effective compliance is compulsory: organizations that self-certify to the Department and publicly declare their commitment to adhere to the Principles must comply fully with the Principles. In order to enter the EU-U.S. DPF, an organization must (a) be subject to the investigatory and enforcement powers of the Federal Trade Commission (the “FTC”), the U.S. Department of Transportation (the “DOT”) or another statutory body that will effectively ensure compliance with the Principles (*other U.S. statutory bodies recognized by the EU may be included as an annex in the future*); (b) publicly declare its commitment to comply with the Principles; (c) publicly disclose its privacy policies in line with these Principles; and (d) fully implement them ⁽³⁾. An organization’s failure to comply is enforceable by the FTC under Section 5 of the Federal Trade Commission (FTC) Act prohibiting unfair or deceptive acts in or affecting commerce (15 U.S.C. § 45); by the DOT under 49 U.S.C. § 41712 prohibiting a carrier or ticket agent from engaging in an unfair or deceptive practice in air transportation or the sale of air transportation; or under other laws or regulations prohibiting such acts.

⁽¹⁾ Provided that the Commission Decision on the adequacy of the protection provided by the EU-U.S. DPF applies to Iceland, Liechtenstein and Norway, the EU-U.S. DPF will cover both the EU, as well as these three countries. Consequently, references to the EU and its Member States will be read as including Iceland, Liechtenstein, and Norway.

⁽²⁾ REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

⁽³⁾ The EU-U.S. Privacy Shield Framework Principles have been amended as the “EU-U.S. Data Privacy Framework Principles”. (See Supplemental Principle on Self-Certification).

3. The Department will maintain and make available to the public an authoritative list of U.S. organizations that have self-certified to the Department and declared their commitment to adhere to the Principles ("the Data Privacy Framework List"). EU-U.S. DPF benefits are assured from the date that the Department places the organization on the Data Privacy Framework List. The Department will remove from the Data Privacy Framework List those organizations that voluntarily withdraw from the EU-U.S. DPF or fail to complete their annual re-certification to the Department; these organizations must either continue to apply the Principles to the personal information they received under the EU-U.S. DPF and affirm to the Department on an annual basis their commitment to do so (i.e., for as long as they retain such information), provide "adequate" protection for the information by another authorized means (for example, using a contract that fully reflects the requirements of the relevant standard contractual clauses adopted by the Commission), or return or delete the information. The Department will also remove from the Data Privacy Framework List those organizations that have persistently failed to comply with the Principles; these organizations must return or delete the personal information they received under the EU-U.S. DPF. An organization's removal from the Data Privacy Framework List means it is no longer entitled to benefit from the Commission's adequacy decision to receive personal information from the EU.
4. The Department will also maintain and make available to the public an authoritative record of U.S. organizations that had previously self-certified to the Department, but that have been removed from the Data Privacy Framework List. The Department will provide a clear warning that these organizations are not participants in the EU-U.S. DPF; that removal from the Data Privacy Framework List means that such organizations cannot claim to be EU-U.S. DPF compliant and must avoid any statements or misleading practices implying that they participate in the EU-U.S. DPF; and that such organizations are no longer entitled to benefit from the Commission's adequacy decision to receive personal information from the EU. An organization that continues to claim participation in the EU-U.S. DPF or makes other EU-U.S. DPF-related misrepresentations after it has been removed from the Data Privacy Framework List may be subject to enforcement action by the FTC, the DOT, or other enforcement authorities.
5. Adherence to these Principles may be limited: (a) to the extent necessary to comply with a court order or meet public interest, law enforcement, or national security requirements, including where statute or government regulation create conflicting obligations; (b) by statute, court order, or government regulation that creates explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the GDPR is to allow exceptions or derogations, under the conditions set out therein, provided such exceptions or derogations are applied in comparable contexts. In this context, safeguards in U.S. law to protect privacy and civil liberties include those required by Executive Order 14086 ⁽⁴⁾ under the conditions set out therein (including its requirements on necessity and proportionality). Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently, including by endeavouring to indicate in their privacy policies where exceptions to the Principles permitted by (b) above will apply. For the same reason, where the option is allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection where possible.
6. Organizations are obligated to apply the Principles to all personal data transferred in reliance on the EU-U.S. DPF after they enter the EU-U.S. DPF. An organization that chooses to extend EU-U.S. DPF benefits to human resources personal information transferred from the EU for use in the context of an employment relationship must indicate this when it self-certifies to the Department and conform to the requirements set forth in the Supplemental Principle on Self-Certification.

⁽⁴⁾ Executive Order of October 7, 2022, "Enhancing Safeguards for United States Signals Intelligence Activities."

7. U.S. law will apply to questions of interpretation and compliance with the Principles and relevant privacy policies by organizations participating in the EU-U.S. DPF, except where such organizations have committed to cooperate with EU data protection authorities ("DPAs"). Unless otherwise stated, all provisions of the Principles apply where they are relevant.
8. Definitions:
 - a. "Personal data" and "personal information" are data about an identified or identifiable individual that are within the scope of the GDPR, received by an organization in the United States from the EU, and recorded in any form.
 - b. "Processing" of personal data means any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.
 - c. "Controller" means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of personal data.
9. The effective date of the Principles and Annex I of the Principles is the date of entry into force of the European Commission's adequacy decision.

II. PRINCIPLES

1. NOTICE

- a. An organization must inform individuals about:
 - i. its participation in the EU-U.S. DPF and provide a link to, or the web address for, the Data Privacy Framework List,
 - ii. the types of personal data collected and, where applicable, the U.S. entities or U.S. subsidiaries of the organization also adhering to the Principles,
 - iii. its commitment to subject to the Principles all personal data received from the EU in reliance on the EU-U.S. DPF,
 - iv. the purposes for which it collects and uses personal information about them,
 - v. how to contact the organization with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints,
 - vi. the type or identity of third parties to which it discloses personal information, and the purposes for which it does so,
 - vii. the right of individuals to access their personal data,
 - viii. the choices and means the organization offers individuals for limiting the use and disclosure of their personal data,
 - ix. the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual, and whether it is: (1) the panel established by DPAs, (2) an alternative dispute resolution provider based in the EU, or (3) an alternative dispute resolution provider based in the United States,
 - x. being subject to the investigatory and enforcement powers of the FTC, the DOT or any other U.S. authorized statutory body,
 - xi. the possibility, under certain conditions, for the individual to invoke binding arbitration, ⁽³⁾
 - xii. the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, and
 - xiii. its liability in cases of onward transfers to third parties.

⁽³⁾ See, e.g., section (c) of the Recourse, Enforcement and Liability Principle.

- b. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

2. CHOICE

- a. An organization must offer individuals the opportunity to choose (*i.e.*, opt out) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.
- b. By derogation to the previous paragraph, it is not necessary to provide choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. However, an organization shall always enter into a contract with the agent.
- c. For sensitive information (*i.e.*, personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), organizations must obtain affirmative express consent (*i.e.*, opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice. In addition, an organization should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.

3. ACCOUNTABILITY FOR ONWARD TRANSFER

- a. To transfer personal information to a third party acting as a controller, organizations must comply with the Notice and Choice Principles. Organizations must also enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles and will notify the organization if it makes a determination that it can no longer meet this obligation. The contract shall provide that when such a determination is made the third party controller ceases processing or takes other reasonable and appropriate steps to remediate.
- b. To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

4. SECURITY

- a. Organizations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

5. DATA INTEGRITY AND PURPOSE LIMITATION

- a. Consistent with the Principles, personal information must be limited to the information that is relevant for the purposes of processing. ⁽⁶⁾ An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. An organization must adhere to the Principles for as long as it retains such information.
- b. Information may be retained in a form identifying or making identifiable ⁽⁷⁾ the individual only for as long as it serves a purpose of processing within the meaning of 5(a). This obligation does not prevent organizations from processing personal information for longer periods for the time and to the extent such processing reasonably serves the purposes of archiving in the public interest, journalism, literature and art, scientific or historical research, and statistical analysis. In these cases, such processing shall be subject to the other principles and provisions of the EU-U.S. DPF. Organizations should take reasonable and appropriate measures in complying with this provision.

6. ACCESS

- a. Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

7. RECOURSE, ENFORCEMENT AND LIABILITY

- a. Effective privacy protection must include robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum such mechanisms must include:
 - i. readily available independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual and by reference to the Principles, and damages awarded where the applicable law or private-sector initiatives so provide;
 - ii. follow-up procedures for verifying that the attestations and assertions organizations make about their privacy practices are true and that privacy practices have been implemented as presented and, in particular, with regard to cases of non-compliance; and
 - iii. obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.
- b. Organizations and their selected independent recourse mechanisms will respond promptly to inquiries and requests by the Department for information relating to the EU-U.S. DPF. All organizations must respond expeditiously to complaints regarding compliance with the Principles referred by EU Member State authorities through the Department. Organizations that have chosen to cooperate with DPAs, including organizations that process human resources data, must respond directly to such authorities with regard to the investigation and resolution of complaints.

⁽⁶⁾ Depending on the circumstances, examples of compatible processing purposes may include those that reasonably serve customer relations, compliance and legal considerations, auditing, security and fraud prevention, preserving or defending the organization's legal rights, or other purposes consistent with the expectations of a reasonable person given the context of the collection.

⁽⁷⁾ In this context, if, given the means of identification reasonably likely to be used (considering, among other things, the costs of and the amount of time required for identification and the available technology at the time of the processing) and the form in which the data is retained, an individual could reasonably be identified by the organization, or a third party if it would have access to the data, then the individual is "identifiable."

- c. Organizations are obligated to arbitrate claims and follow the terms as set forth in Annex I, provided that an individual has invoked binding arbitration by delivering notice to the organization at issue and following the procedures and subject to conditions set forth in Annex I.
- d. In the context of an onward transfer, a participating organization has responsibility for the processing of personal information it receives under the EU-U.S. DPF and subsequently transfers to a third party acting as an agent on its behalf. The participating organization shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage.
- e. When an organization becomes subject to a court order that is based on non-compliance or an order from a U.S. statutory body (e.g., FTC or DOT) listed in the Principles or in a future annex to the Principles that is based on non-compliance, the organization shall make public any relevant EU-U.S. DPF-related sections of any compliance or assessment report submitted to the court or U.S. statutory body to the extent consistent with confidentiality requirements. The Department has established a dedicated point of contact for DPAs for any problems of compliance by participating organizations. The FTC and the DOT will give priority consideration to referrals of non-compliance with the Principles from the Department and EU Member State authorities, and will exchange information regarding referrals with the referring state authorities on a timely basis, subject to existing confidentiality restrictions.

III. SUPPLEMENTAL PRINCIPLES

1. Sensitive Data

- a. An organization is not required to obtain affirmative, express consent (*i.e.*, opt in) with respect to sensitive data where the processing is:
 - i. in the vital interests of the data subject or another person;
 - ii. necessary for the establishment of legal claims or defenses;
 - iii. required to provide medical care or diagnosis;
 - iv. carried out in the course of legitimate activities by a foundation, association or any other non-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects;
 - v. necessary to carry out the organization's obligations in the field of employment law; or
 - vi. related to data that are manifestly made public by the individual.

2. Journalistic Exceptions

- a. Given U.S. constitutional protections for freedom of the press, where the rights of a free press embodied in the First Amendment of the U.S. Constitution intersect with privacy protection interests, the First Amendment must govern the balancing of these interests with regard to the activities of U.S. persons or organizations.
- b. Personal information that is gathered for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives, is not subject to the requirements of the Principles.

3. Secondary Liability

- a. Internet Service Providers ("ISPs"), telecommunications carriers, and other organizations are not liable under the Principles when on behalf of another organization they merely transmit, route, switch, or cache information. The EU-U.S. DPF does not create secondary liability. To the extent that an organization is acting as a mere conduit for data transmitted by third parties and does not determine the purposes and means of processing those personal data, it would not be liable.

4. Performing Due Diligence and Conducting Audits

- a. The activities of auditors and investment bankers may involve processing personal data without the consent or knowledge of the individual. This is permitted by the Notice, Choice, and Access Principles under the circumstances described below.
- b. Public stock corporations and closely held companies, including participating organizations, are regularly subject to audits. Such audits, particularly those looking into potential wrongdoing, may be jeopardized if disclosed prematurely. Similarly, a participating organization involved in a potential merger or takeover will need to perform, or be the subject of, a “due diligence” review. This will often entail the collection and processing of personal data, such as information on senior executives and other key personnel. Premature disclosure could impede the transaction or even violate applicable securities regulation. Investment bankers and attorneys engaged in due diligence, or auditors conducting an audit, may process information without knowledge of the individual only to the extent and for the period necessary to meet statutory or public interest requirements and in other circumstances in which the application of these Principles would prejudice the legitimate interests of the organization. These legitimate interests include the monitoring of organizations’ compliance with their legal obligations and legitimate accounting activities, and the need for confidentiality connected with possible acquisitions, mergers, joint ventures, or other similar transactions carried out by investment bankers or auditors.

5. The Role of the Data Protection Authorities

- a. Organizations will implement their commitment to cooperate with DPAs as described below. Under the EU-U.S. DPF, U.S. organizations receiving personal data from the EU must commit to employ effective mechanisms for assuring compliance with the Principles. More specifically as set out in the Recourse, Enforcement and Liability Principle, participating organizations must provide: (a)(i) recourse for individuals to whom the data relate; (a)(ii) follow-up procedures for verifying that the attestations and assertions they have made about their privacy practices are true; and (a)(iii) obligations to remedy problems arising out of failure to comply with the Principles and consequences for such organizations. An organization may satisfy points (a)(i) and (a)(iii) of the Recourse, Enforcement and Liability Principle if it adheres to the requirements set forth here for cooperating with the DPAs.
- b. An organization commits to cooperate with the DPAs by declaring in its EU-U.S. DPF self-certification submission to the Department (*see* Supplemental Principle on Self-Certification) that the organization:
 - i. elects to satisfy the requirement in points (a)(i) and (a)(iii) of the Recourse, Enforcement and Liability Principle by committing to cooperate with the DPAs;
 - ii. will cooperate with the DPAs in the investigation and resolution of complaints brought under the Principles; and
 - iii. will comply with any advice given by the DPAs where the DPAs take the view that the organization needs to take specific action to comply with the Principles, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Principles, and will provide the DPAs with written confirmation that such action has been taken.
- c. Operation of DPA Panels
 - i. The cooperation of the DPAs will be provided in the form of information and advice in the following way:
 1. The advice of the DPAs will be delivered through an informal panel of DPAs established at the EU level, which will *inter alia* help ensure a harmonized and coherent approach.
 2. The panel will provide advice to the U.S. organizations concerned on unresolved complaints from individuals about the handling of personal information that has been transferred from the EU under the EU-U.S. DPF. This advice will be designed to ensure that the Principles are being correctly applied and will include any remedies for the individual(s) concerned that the DPAs consider appropriate.

3. The panel will provide such advice in response to referrals from the organizations concerned and/or to complaints received directly from individuals against organizations which have committed to cooperate with DPAs for EU-U.S. DPF purposes, while encouraging and if necessary helping such individuals in the first instance to use the in-house complaint handling arrangements that the organization may offer.
 4. Advice will be issued only after both sides in a dispute have had a reasonable opportunity to comment and to provide any evidence they wish. The panel will seek to deliver advice as quickly as this requirement for due process allows. As a general rule, the panel will aim to provide advice within 60 days after receiving a complaint or referral and more quickly where possible.
 5. The panel will make public the results of its consideration of complaints submitted to it, if it sees fit.
 6. The delivery of advice through the panel will not give rise to any liability for the panel or for individual DPAs.
- ii. As noted above, organizations choosing this option for dispute resolution must undertake to comply with the advice of the DPAs. If an organization fails to comply within 25 days of the delivery of the advice and has offered no satisfactory explanation for the delay, the panel will give notice of its intention either to refer the matter to the FTC, the DOT, or other U.S. federal or state body with statutory powers to take enforcement action in cases of deception or misrepresentation, or to conclude that the agreement to cooperate has been seriously breached and must therefore be considered null and void. In the latter case, the panel will inform the Department so that the Data Privacy Framework List can be duly amended. Any failure to fulfill the undertaking to cooperate with the DPAs, as well as failures to comply with the Principles, will be actionable as a deceptive practice under Section 5 of the FTC Act (15 U.S.C. § 45), 49 U.S.C. § 41712, or other similar statute.
- d. An organization that wishes its EU-U.S. DPF benefits to cover human resources data transferred from the EU in the context of the employment relationship must commit to cooperate with the DPAs with regard to such data (see Supplemental Principle on Human Resources Data).
 - e. Organizations choosing this option will be required to pay an annual fee, which will be designed to cover the operating costs of the panel. They may additionally be asked to meet any necessary translation expenses arising out of the panel's consideration of referrals or complaints against them. The amount of the fee will be determined by the Department after consultation with the Commission. The collection of the fee may be conducted by a third party selected by the Department to serve as the custodian of the funds collected for this purpose. The Department will closely cooperate with the Commission and the DPAs on the establishment of appropriate procedures for the distribution of funds collected through the fee, as well as other procedural and administrative aspects of the panel. The Department and the Commission may agree to alter how often the fee is collected.

6. Self-Certification

- a. EU-U.S. DPF benefits are assured from the date on which the Department places the organization on the Data Privacy Framework List. The Department will only place an organization on the Data Privacy Framework List after having determined that the organization's initial self-certification submission is complete, and will remove the organization from that list if it voluntarily withdraws, fails to complete its annual re-certification, or if it persistently fails to comply with the Principles (see Supplemental Principle on Dispute Resolution and Enforcement).
- b. To initially self-certify or subsequently re-certify for the EU-U.S. DPF, an organization must on each occasion provide to the Department a submission by a corporate officer on behalf of the organization that is self-certifying or re-certifying (as applicable) its adherence to the Principles ⁽⁸⁾, that contains at least the following information:

⁽⁸⁾ The submission must be made via the Department's Data Privacy Framework website by an individual within the organization who is authorized to make representations on behalf of the organization and any of its covered entities regarding its adherence to the Principles.

- i. the name of the self-certifying or re-certifying U.S. organization, as well as the name(s) of any of its U.S. entities or U.S. subsidiaries also adhering to the Principles that the organization wishes to cover;
- ii. a description of the activities of the organization with respect to personal information that would be received from the EU under the EU-U.S. DPF;
- iii. a description of the organization's relevant privacy policy/ies for such personal information, including:
 - 1. if the organization has a public website, the relevant web address where the privacy policy is available, or if the organization does not have a public website, where the privacy policy is available for viewing by the public; and
 - 2. its effective date of implementation;
- iv. a contact office within the organization for the handling of complaints, access requests, and any other issues arising under the Principles ⁽⁹⁾, including:
 - 1. the name(s), job title(s) (as applicable), e-mail address(es), and telephone number(s) of the relevant individual(s) or relevant contact office(s) within the organization; and
 - 2. the relevant U.S. mailing address for the organization;
- v. the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the Principles or a future annex to the Principles);
- vi. the name of any privacy program in which the organization is a member;
- vii. the method of verification (*i.e.*, self-assessment; or outside compliance reviews, including the third party that completes such reviews); ⁽¹⁰⁾ and
- viii. the relevant independent recourse mechanism(s) available to investigate unresolved Principles-related complaints. ⁽¹¹⁾
- c. Where the organization wishes its EU-U.S. DPF benefits to cover human resources information transferred from the EU for use in the context of the employment relationship, it may do so where a statutory body listed in the Principles or a future annex to the Principles has jurisdiction to hear claims against the organization arising out of the processing of human resources information. In addition, the organization must indicate this in its initial self-certification submission, as well as in any re-certification submissions, and declare its commitment to cooperate with the EU authority or authorities concerned in conformity with the Supplemental Principles on Human Resources Data and the Role of the Data Protection Authorities (as applicable) and that it will comply with the advice given by such authorities. The organization must also provide the Department with a copy of its human resources privacy policy and provide information where the privacy policy is available for viewing by its affected employees.

⁽⁹⁾ The primary "organization contact" or the "organization corporate officer" cannot be external to the organization (*e.g.*, outside counsel or an external consultant).

⁽¹⁰⁾ See Supplemental Principle on Verification.

⁽¹¹⁾ See Supplemental Principle on Dispute Resolution and Enforcement.

- d. The Department will maintain and make publicly available the Data Privacy Framework List of organizations that have filed completed, initial self-certification submissions and will update that list on the basis of completed, annual re-certification submissions, as well as notifications received pursuant to the Supplemental Principle on Dispute Resolution and Enforcement. Such re-certification submissions must be provided not less than annually; otherwise the organization will be removed from the Data Privacy Framework List and EU-U.S. DPF benefits will no longer be assured. All organizations that are placed on the Data Privacy Framework List by the Department must have relevant privacy policies that comply with the Notice Principle and state in those privacy policies that they adhere to the Principles.⁽¹²⁾ If available online, an organization's privacy policy must include a hyperlink to the Department's Data Privacy Framework website and a hyperlink to the website or complaint submission form of the independent recourse mechanism that is available to investigate unresolved, Principles-related complaints free of charge to the individual.
- e. The Principles apply immediately upon self-certification. Participating organizations that previously self-certified to the EU-U.S. Privacy Shield Framework Principles will need to update their privacy policies to instead refer to the "EU-U.S. Data Privacy Framework Principles". Such organizations shall include this reference as soon as possible, and in any event no later than three months from the effective date for the EU-U.S. Data Privacy Framework Principles.
- f. An organization must subject to the Principles all personal data received from the EU in reliance on the EU-U.S. DPF. The undertaking to adhere to the Principles is not time-limited in respect of personal data received during the period in which the organization enjoys the benefits of the EU-U.S. DPF; its undertaking means that it will continue to apply the Principles to such data for as long as the organization stores, uses or discloses them, even if it subsequently leaves the EU-U.S. DPF for any reason. An organization that wishes to withdraw from the EU-U.S. DPF must notify the Department of this in advance. This notification must also indicate what the organization will do with the personal data that it received in reliance on the EU-U.S. DPF (i.e., retain, return, or delete the data, and if it will retain the data, the authorized means by which it will provide protection to the data). An organization that withdraws from the EU-U.S. DPF, but wants to retain such data must either affirm to the Department on an annual basis its commitment to continue to apply the Principles to the data or provide "adequate" protection for the data by another authorized means (for example, using a contract that fully reflects the requirements of the relevant standard contractual clauses adopted by the Commission); otherwise, the organization must return or delete the information.⁽¹³⁾ An organization that withdraws from the EU-U.S. DPF must remove from any relevant privacy policy any references to the EU-U.S. DPF that imply that the organization continues to participate in the EU-U.S. DPF and is entitled to its benefits.

⁽¹²⁾ An organization self-certifying for the first time may not claim EU-U.S. DPF participation in its final privacy policy until the Department notifies the organization that it may do so. The organization must provide the Department with a draft privacy policy, which is consistent with the Principles, when it submits its initial self-certification. Once the Department has determined that the organization's initial self-certification submission is otherwise complete, the Department will notify the organization that it should finalize (e.g., publish where applicable) its EU-U.S. DPF-consistent privacy policy. The organization must promptly notify the Department as soon as the relevant privacy policy is finalized, at which time the Department will place the organization on the Data Privacy Framework List.

⁽¹³⁾ If an organization elects at the time of its withdrawal to retain the personal data that it received in reliance on the EU-U.S. DPF and affirm to the Department on an annual basis that it continues to apply the Principles to such data, the organization must verify to the Department once a year following its withdrawal (i.e., unless and until the organization provides "adequate" protection for such data by another authorized means, or returns or deletes all such data and notifies the Department of this action) what it has done with that personal data, what it will do with any of that personal data that it continues to retain, and who will serve as an ongoing point of contact for Principles-related questions.

- g. An organization that will cease to exist as a separate legal entity due to a change in corporate status, such as a result of a merger, takeover, bankruptcy, or dissolution must notify the Department of this in advance. The notification should also indicate whether the entity resulting from the change in corporate status will (i) continue to participate in the EU-U.S. DPF through an existing self-certification; (ii) self-certify as a new participant in the EU-U.S. DPF (*e.g.*, where the new entity or surviving entity does not already have an existing self-certification through which it could participate in the EU-U.S. DPF); or (iii) put in place other safeguards, such as a written agreement that will ensure continued application of the Principles to any personal data that the organization received under the EU-U.S. DPF and will be retained. Where neither (i), (ii), nor (iii) applies, any personal data that has been received under the EU-U.S. DPF must be promptly returned or deleted.
- h. When an organization leaves the EU-U.S. DPF for any reason, it must remove all statements implying that the organization continues to participate in the EU-U.S. DPF or is entitled to the benefits of the EU-U.S. DPF. The EU-U.S. DPF certification mark, if used, must also be removed. Any misrepresentation to the general public concerning an organization's adherence to the Principles may be actionable by the FTC, DOT, or other relevant government body. Misrepresentations to the Department may be actionable under the False Statements Act (18 U.S.C. § 1001).

7. Verification

- a. Organizations must provide follow-up procedures for verifying that the attestations and assertions they make about their EU-U.S. DPF privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Principles.
- b. To meet the verification requirements of the Recourse, Enforcement and Liability Principle, an organization must verify such attestations and assertions either through self-assessment or outside compliance reviews.
- c. Where the organization has chosen self-assessment, such verification must demonstrate that its privacy policy regarding personal information received from the EU is accurate, comprehensive, readily available, conforms to the Principles, and is completely implemented (*i.e.*, is being complied with). It must also indicate that individuals are informed of any in-house arrangements for handling complaints and of the independent recourse mechanism(s) through which they may pursue complaints; that it has in place procedures for training employees in its implementation, and disciplining them for failure to follow it; and that it has in place internal procedures for periodically conducting objective reviews of compliance with the above. A statement verifying that the self-assessment has been completed must be signed by a corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about non-compliance.
- d. Where the organization has chosen outside compliance review, such verification must demonstrate that its privacy policy regarding personal information received from the EU is accurate, comprehensive, readily available, conforms to the Principles, and is completely implemented (*i.e.*, is being complied with). It must also indicate that individuals are informed of mechanism(s) through which they may pursue complaints. The methods of review may include, without limitation, auditing, random reviews, use of "decoys", or use of technology tools as appropriate. A statement verifying that an outside compliance review has been successfully completed must be signed either by the reviewer or by the corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about compliance.
- e. Organizations must retain their records on the implementation of their EU-U.S. DPF privacy practices and make them available upon request in the context of an investigation or a complaint about non-compliance to the independent dispute resolution body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction. Organizations must also respond promptly to inquiries and other requests for information from the Department relating to the organization's adherence to the Principles.

8. Access

a. The Access Principle in Practice

- i. Under the Principles, the right of access is fundamental to privacy protection. In particular, it allows individuals to verify the accuracy of information held about them. The Access Principle means that individuals have the right to:
 1. obtain from an organization confirmation of whether or not the organization is processing personal data relating to them; ⁽¹⁴⁾
 2. have communicated to them such data so that they could verify its accuracy and the lawfulness of the processing; and
 3. have the data corrected, amended or deleted where it is inaccurate or processed in violation of the Principles.
- ii. Individuals do not have to justify requests for access to their personal data. In responding to individuals' access requests, organizations should first be guided by the concern(s) that led to the requests in the first place. For example, if an access request is vague or broad in scope, an organization may engage the individual in a dialogue so as to better understand the motivation for the request and to locate responsive information. The organization might inquire about which part(s) of the organization the individual interacted with or about the nature of the information or its use that is the subject of the access request.
- iii. Consistent with the fundamental nature of access, organizations should always make good faith efforts to provide access. For example, where certain information needs to be protected and can be readily separated from other personal information subject to an access request, the organization should redact the protected information and make available the other information. If an organization determines that access should be restricted in any particular instance, it should provide the individual requesting access with an explanation of why it has made that determination and a contact point for any further inquiries.

b. Burden or Expense of Providing Access

- i. The right of access to personal data may be restricted in exceptional circumstances where the legitimate rights of persons other than the individual would be violated or where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question. Expense and burden are important factors and should be taken into account but they are not controlling factors in determining whether providing access is reasonable.
- ii. For example, if the personal information is used for decisions that will significantly affect the individual (e.g., the denial or grant of important benefits, such as insurance, a mortgage, or a job), then consistent with the other provisions of these Supplemental Principles, the organization would have to disclose that information even if it is relatively difficult or expensive to provide. If the personal information requested is not sensitive or not used for decisions that will significantly affect the individual, but is readily available and inexpensive to provide, an organization would have to provide access to such information.

c. Confidential Commercial Information

- i. Confidential commercial information is information that an organization has taken steps to protect from disclosure, where disclosure would help a competitor in the market. Organizations may deny or limit access to the extent that granting full access would reveal its own confidential commercial information, such as marketing inferences or classifications generated by the organization, or the confidential commercial information of another that is subject to a contractual obligation of confidentiality.

⁽¹⁴⁾ The organization should answer requests from an individual concerning the purposes of the processing, the categories of personal data concerned, and the recipients or categories of recipients to whom the personal data is disclosed.

- ii. Where confidential commercial information can be readily separated from other personal information subject to an access request, the organization should redact the confidential commercial information and make available the non-confidential information.

d. Organization of Data Bases

- i. Access can be provided in the form of disclosure of the relevant personal information by an organization to the individual and does not require access by the individual to an organization's data base.
- ii. Access needs to be provided only to the extent that an organization stores the personal information. The Access Principle does not itself create any obligation to retain, maintain, reorganize, or restructure personal information files.

e. When Access May be Restricted

- i. As organizations must always make good faith efforts to provide individuals with access to their personal data, the circumstances in which organizations may restrict such access are limited, and any reasons for restricting access must be specific. As under the GDPR, an organization can restrict access to information to the extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security; defense; or public security. In addition, where personal information is processed solely for research or statistical purposes, access may be denied. Other reasons for denying or limiting access are:
 - 1. interference with the execution or enforcement of the law or with private causes of action, including the prevention, investigation or detection of offenses or the right to a fair trial;
 - 2. disclosure where the legitimate rights or important interests of others would be violated;
 - 3. breaching a legal or other professional privilege or obligation;
 - 4. prejudicing employee security investigations or grievance proceedings or in connection with employee succession planning and corporate re-organizations; or
 - 5. prejudicing the confidentiality necessary in monitoring, inspection or regulatory functions connected with sound management, or in future or ongoing negotiations involving the organization.
- ii. An organization which claims an exception has the burden of demonstrating its necessity, and the reasons for restricting access and a contact point for further inquiries should be given to individuals.

f. Right to Obtain Confirmation and Charging a Fee to Cover the Costs for Providing Access

- i. An individual has the right to obtain confirmation of whether or not this organization has personal data relating to him or her. An individual also has the right to have communicated to him or her personal data relating to him or her. An organization may charge a fee that is not excessive.
- ii. Charging a fee may be justified, for example, where requests for access are manifestly excessive, in particular because of their repetitive character.
- iii. Access may not be refused on cost grounds if the individual offers to pay the costs.

g. Repetitious or Vexatious Requests for Access

- i. An organization may set reasonable limits on the number of times within a given period that access requests from a particular individual will be met. In setting such limitations, an organization should consider such factors as the frequency with which information is updated, the purpose for which the data are used, and the nature of the information.

h. Fraudulent Requests for Access

- i. An organization is not required to provide access unless it is supplied with sufficient information to allow it to confirm the identity of the person making the request.

i. Timeframe for Responses

- i. Organizations should respond to access requests within a reasonable time period, in a reasonable manner, and in a form that is readily intelligible to the individual. An organization that provides information to data subjects at regular intervals may satisfy an individual access request with its regular disclosure if it would not constitute an excessive delay.

9. Human Resources Data

a. Coverage by the EU-U.S. DPF

- i. Where an organization in the EU transfers personal information about its employees (past or present) collected in the context of the employment relationship, to a parent, affiliate, or unaffiliated service provider in the United States participating in the EU-U.S. DPF, the transfer enjoys the benefits of the EU-U.S. DPF. In such cases, the collection of the information and its processing prior to transfer will have been subject to the national laws of the EU Member State where it was collected, and any conditions for or restrictions on its transfer according to those laws will have to be respected.
- ii. The Principles are relevant only when individually identified or identifiable records are transferred or accessed. Statistical reporting relying on aggregate employment data and containing no personal data or the use of anonymized data does not raise privacy concerns.

b. Application of the Notice and Choice Principles

- i. A U.S. organization that has received employee information from the EU under the EU-U.S. DPF may disclose it to third parties or use it for different purposes only in accordance with the Notice and Choice Principles. For example, where an organization intends to use personal information collected through the employment relationship for non-employment-related purposes, such as marketing communications, the U.S. organization must provide the affected individuals with the requisite choice before doing so, unless they have already authorized the use of the information for such purposes. Such use must not be incompatible with the purposes for which the personal information has been collected or subsequently authorized by the individual. Moreover, such choices must not be used to restrict employment opportunities or take any punitive action against such employees.
- ii. It should be noted that certain generally applicable conditions for transfer from some EU Member States may preclude other uses of such information even after transfer outside the EU and such conditions will have to be respected.
- iii. In addition, employers should make reasonable efforts to accommodate employee privacy preferences. This could include, for example, restricting access to the personal data, anonymizing certain data, or assigning codes or pseudonyms when the actual names are not required for the management purpose at hand.
- iv. To the extent and for the period necessary to avoid prejudicing the ability of the organization in making promotions, appointments, or other similar employment decisions, an organization does not need to offer notice and choice.

c. Application of the Access Principle

- i. The Supplemental Principle on Access provides guidance on reasons which may justify denying or limiting access on request in the human resources context. Of course, employers in the EU must comply with local regulations and ensure that EU employees have access to such information as is required by law in their home countries, regardless of the location of data processing and storage. The EU-U.S. DPF requires that an organization processing such data in the United States will cooperate in providing such access either directly or through the EU employer.

d. Enforcement

- i. In so far as personal information is used only in the context of the employment relationship, primary responsibility for the data vis-à-vis the employee remains with the organization in the EU. It follows that, where European employees make complaints about violations of their data protection rights and are not satisfied with the results of internal review, complaint, and appeal procedures (or any applicable grievance procedures under a contract with a trade union), they should be directed to the state or national data protection or labor authority in the jurisdiction where the employees work. This includes cases where the alleged mishandling of their personal information is the responsibility of the U.S. organization that has received the information from the employer and thus involves an alleged breach of the Principles. This will be the most efficient way to address the often overlapping rights and obligations imposed by local labor law and labor agreements as well as data protection law.
- ii. A U.S. organization participating in the EU-U.S. DPF that uses EU human resources data transferred from the EU in the context of the employment relationship and that wishes such transfers to be covered by the EU-U.S. DPF must therefore commit to cooperate in investigations by and to comply with the advice of competent EU authorities in such cases.

e. Application of the Accountability for Onward Transfer Principle

- i. For occasional employment-related operational needs of the participating organization with respect to personal data transferred under the EU-U.S. DPF, such as the booking of a flight, hotel room, or insurance coverage, transfers of personal data of a small number of employees can take place to controllers without application of the Access Principle or entering into a contract with the third-party controller, as otherwise required under the Accountability for Onward Transfer Principle, provided that the participating organization has complied with the Notice and Choice Principles.

10. **Obligatory Contracts for Onward Transfers**

a. Data Processing Contracts

- i. When personal data is transferred from the EU to the United States only for processing purposes, a contract will be required, regardless of participation by the processor in the EU-U.S. DPF.
- ii. Data controllers in the EU are always required to enter into a contract when a transfer for mere processing is made, whether the processing operation is carried out inside or outside the EU, and whether or not the processor participates in the EU-U.S. DPF. The purpose of the contract is to make sure that the processor:
 1. acts only on instructions from the controller;
 2. provides appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and understands whether onward transfer is allowed; and
 3. taking into account the nature of the processing, assists the controller in responding to individuals exercising their rights under the Principles.

- iii. Because adequate protection is provided by participating organizations, contracts with such organizations for mere processing do not require prior authorization.

b. Transfers within a Controlled Group of Corporations or Entities

- i. When personal information is transferred between two controllers within a controlled group of corporations or entities, a contract is not always required under the Accountability for Onward Transfer Principle. Data controllers within a controlled group of corporations or entities may base such transfers on other instruments, such as EU Binding Corporate Rules or other intra-group instruments (*e.g.*, compliance and control programs), ensuring the continuity of protection of personal information under the Principles. In case of such transfers, the participating organization remains responsible for compliance with the Principles.

c. Transfers between Controllers

- i. For transfers between controllers, the recipient controller need not be a participating organization or have an independent recourse mechanism. The participating organization must enter into a contract with the recipient third-party controller that provides for the same level of protection as is available under the EU-U.S. DPF, not including the requirement that the third party controller be a participating organization or have an independent recourse mechanism, provided it makes available an equivalent mechanism.

11. **Dispute Resolution and Enforcement**

- a. The Recourse, Enforcement and Liability Principle sets out the requirements for EU-U.S. DPF enforcement. How to meet the requirements of point (a)(ii) of the Principle is set out in the Supplemental Principle on Verification. This Supplemental Principle addresses points (a)(i) and (a)(iii), both of which require independent recourse mechanisms. These mechanisms may take different forms, but they must meet the Recourse, Enforcement and Liability Principle's requirements. Organizations satisfy the requirements through the following: (i) compliance with private sector developed privacy programs that incorporate the Principles into their rules and that include effective enforcement mechanisms of the type described in the Recourse, Enforcement and Liability Principle; (ii) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or (iii) commitment to cooperate with DPAs located in the EU or their authorized representatives.
- b. This list is intended to be illustrative and not limiting. The private sector may design additional mechanisms to provide enforcement, so long as they meet the requirements of the Recourse, Enforcement and Liability Principle and the Supplemental Principles. Please note that the Recourse, Enforcement and Liability Principle's requirements are additional to the requirement that self-regulatory efforts must be enforceable under Section 5 of the FTC Act (15 U.S.C. § 45) prohibiting unfair or deceptive acts, 49 U.S.C. § 41712 prohibiting a carrier or ticket agent from engaging in an unfair or deceptive practice in air transportation or the sale of air transportation, or another law or regulation prohibiting such acts.
- c. In order to help ensure compliance with their EU-U.S. DPF commitments and to support the administration of the program, organizations, as well as their independent recourse mechanisms, must provide information relating to the EU-U.S. DPF when requested by the Department. In addition, organizations must respond expeditiously to complaints regarding their compliance with the Principles referred through the Department by DPAs. The response should address whether the complaint has merit and, if so, how the organization will rectify the problem. The Department will protect the confidentiality of information it receives in accordance with U.S. law.

d. Recourse Mechanisms

- i. Individuals should be encouraged to raise any complaints they may have with the relevant organization before proceeding to independent recourse mechanisms. Organizations must respond to an individual within 45 days of receiving a complaint. Whether a recourse mechanism is independent is a factual question that can be demonstrated notably by impartiality, transparent composition and financing, and a proven track record. As required by the Recourse, Enforcement and Liability Principle, the recourse available to individuals must be readily available and free of charge to individuals. Independent dispute resolution bodies should look into each complaint received from individuals unless they are obviously unfounded or frivolous. This does not preclude the establishment of eligibility requirements by the independent dispute resolution body operating the recourse mechanism, but such requirements should be transparent and justified (for example, to exclude complaints that fall outside the scope of the program or are for consideration in another forum), and should not have the effect of undermining the commitment to look into legitimate complaints. In addition, recourse mechanisms should provide individuals with full and readily available information about how the dispute resolution procedure works when they file a complaint. Such information should include notice about the mechanism's privacy practices, in conformity with the Principles. They should also cooperate in the development of tools, such as standard complaint forms to facilitate the complaint resolution process.
- ii. Independent recourse mechanisms must include on their public websites information regarding the Principles and the services that they provide under the EU-U.S. DPF. This information must include: (1) information on or a link to the Principles' requirements for independent recourse mechanisms; (2) a link to the Department's Data Privacy Framework website; (3) an explanation that their dispute resolution services under the EU-U.S. DPF are free of charge to individuals; (4) a description of how a Principles-related complaint can be filed; (5) the timeframe in which Principles-related complaints are processed; and (6) a description of the range of potential remedies.
- iii. Independent recourse mechanisms must publish an annual report providing aggregate statistics regarding their dispute resolution services. The annual report must include: (1) the total number of Principles-related complaints received during the reporting year; (2) the types of complaints received; (3) dispute resolution quality measures, such as the length of time taken to process complaints; and (4) the outcomes of the complaints received, notably the number and types of remedies or sanctions imposed.
- iv. As set forth in Annex I, an arbitration option is available to an individual to determine, for residual claims, whether a participating organization has violated its obligations under the Principles as to that individual, and whether any such violation remains fully or partially unremedied. This option is available only for these purposes. This option is not available, for example, with respect to the exceptions to the Principles⁽¹⁵⁾ or with respect to an allegation about the adequacy of the EU-U.S. DPF. Under this arbitration option, the "EU-U.S. Data Privacy Framework Panel" (consisting of one or three arbitrators, as agreed by the parties) has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return of the individual's data in question) necessary to remedy the violation of the Principles only with respect to the individual. Individuals and participating organizations will be able to seek judicial review and enforcement of the arbitral decisions pursuant to U.S. law under the Federal Arbitration Act.

e. Remedies and Sanctions

- i. The result of any remedies provided by the independent dispute resolution body should be that the effects of non-compliance are reversed or corrected by the organization, insofar as feasible, and that future processing by the organization will be in conformity with the Principles and, where appropriate, that processing of the personal data of the individual who brought the complaint will cease. Sanctions need to be rigorous enough to ensure compliance by the organization with the Principles. A range of sanctions of varying degrees of severity will allow dispute resolution bodies to respond appropriately to varying degrees of non-compliance. Sanctions should include both publicity for findings of non-compliance and

⁽¹⁵⁾ The Principles, Overview, para. 5.

the requirement to delete data in certain circumstances. ⁽¹⁶⁾ Other sanctions could include suspension and removal of a seal, compensation for individuals for losses incurred as a result of non-compliance and injunctive awards. Private-sector independent dispute resolution bodies and self-regulatory bodies must notify failures of participating organizations to comply with their rulings to the governmental body with applicable jurisdiction or the courts, as appropriate, and the Department.

f. FTC Action

- i. The FTC has committed to reviewing on a priority basis referrals alleging non-compliance with the Principles received from: (i) privacy self-regulatory bodies and other independent dispute resolution bodies; (ii) EU Member States; and (iii) the Department, to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated. If the FTC concludes that it has reason to believe Section 5 has been violated, it may resolve the matter by seeking an administrative cease and desist order prohibiting the challenged practices or by filing a complaint in a federal district court, which if successful could result in a federal court order to same effect. This includes false claims of adherence to the Principles or participation in the EU-U.S. DPF by organizations, which either are no longer on the Data Privacy Framework List or have never self-certified to the Department. The FTC may obtain civil penalties for violations of an administrative cease and desist order and may pursue civil or criminal contempt for violation of a federal court order. The FTC will notify the Department of any such actions it takes. The Department encourages other government bodies to notify it of the final disposition of any such referrals or other rulings determining adherence to the Principles.

g. Persistent Failure to Comply

- i. If an organization persistently fails to comply with the Principles, it is no longer entitled to benefit from the EU-U.S. DPF. Organizations that have persistently failed to comply with the Principles will be removed from the Data Privacy Framework List by the Department and must return or delete the personal information they received under the EU-U.S. DPF.
- ii. Persistent failure to comply arises where an organization that has self-certified to the Department refuses to comply with a final determination by any privacy self-regulatory, independent dispute resolution, or government body, or where such a body, including the Department, determines that an organization frequently fails to comply with the Principles to the point where its claim to comply is no longer credible. In cases where such a determination is made by a body other than the Department the organization must promptly notify the Department of such facts. Failure to do so may be actionable under the False Statements Act (18 U.S.C. § 1001). An organization's withdrawal from a private-sector privacy self-regulatory program or independent dispute resolution mechanism does not relieve it of its obligation to comply with the Principles and would constitute a persistent failure to comply.
- iii. The Department will remove an organization from the Data Privacy Framework List for persistent failure to comply, including in response to any notification it receives of such non-compliance from the organization itself, a privacy self-regulatory body or another independent dispute resolution body, or a government body, but only after first providing the organization with 30 days' notice and an opportunity to respond ⁽¹⁷⁾. Accordingly, the Data Privacy Framework List maintained by the Department will make clear which organizations are assured and which organizations are no longer assured of EU-U.S. DPF benefits.
- iv. An organization applying to participate in a self-regulatory body for the purposes of requalifying for the EU-U.S. DPF must provide that body with full information about its prior participation in the EU-U.S. DPF.

⁽¹⁶⁾ Independent dispute resolution bodies have discretion about the circumstances in which they use these sanctions. The sensitivity of the data concerned is one factor to be taken into consideration in deciding whether deletion of data should be required, as is whether an organization has collected, used, or disclosed information in blatant contravention of the Principles.

⁽¹⁷⁾ The Department will indicate within the notice the amount of time, which will necessarily be less than 30 days, the organization has to respond to the notice.

12. Choice – Timing of Opt Out

- a. Generally, the purpose of the Choice Principle is to ensure that personal information is used and disclosed in ways that are consistent with the individual's expectations and choices. Accordingly, an individual should be able to exercise "opt out" choice of having personal information used for direct marketing at any time subject to reasonable limits established by the organization, such as giving the organization time to make the opt out effective. An organization may also require sufficient information to confirm the identity of the individual requesting the "opt out." In the United States, individuals may be able to exercise this option through the use of a central "opt out" program. In any event, an individual should be given a readily available and affordable mechanism to exercise this option.
- b. Similarly, an organization may use information for certain direct marketing purposes when it is impracticable to provide the individual with an opportunity to opt out before using the information, if the organization promptly gives the individual such opportunity at the same time (and upon request at any time) to decline (at no cost to the individual) to receive any further direct marketing communications and the organization complies with the individual's wishes.

13. Travel Information

- a. Airline passenger reservation and other travel information, such as frequent flyer or hotel reservation information and special handling needs, such as meals to meet religious requirements or physical assistance, may be transferred to organizations located outside the EU in several different circumstances. Under the GDPR, personal data may, in the absence of an adequacy decision, be transferred to a third country if appropriate data protection safeguards are provided pursuant to Article 46 GDPR or, in specific situations, if one of the conditions of Article 49 GDPR is fulfilled (e.g., where the data subject has explicitly consented to the transfer). U.S. organizations subscribing to the EU-U.S. DPF provide adequate protection for personal data and may therefore receive data transfers from the EU on the basis of Article 45 GDPR, without having to put in place a transfer instrument pursuant to Article 46 GDPR or meet the conditions of Article 49 GDPR. Since the EU-U.S. DPF includes specific rules for sensitive information, such information (which may need to be collected, for example, in connection with customers' needs for physical assistance) may be included in transfers to participating organizations. In all cases, however, the organization transferring the information has to respect the law in the EU Member State in which it is operating, which may *inter alia* impose special conditions for the handling of sensitive data.

14. Pharmaceutical and Medical Products

- a. Application of EU/Member State Laws or the Principles
 - i. EU/Member State law applies to the collection of the personal data and to any processing that takes place prior to the transfer to the United States. The Principles apply to the data once they have been transferred to the United States. Data used for pharmaceutical research and other purposes should be anonymized when appropriate.
- b. Future Scientific Research
 - i. Personal data developed in specific medical or pharmaceutical research studies often play a valuable role in future scientific research. Where personal data collected for one research study are transferred to a U.S. organization in the EU-U.S. DPF, the organization may use the data for a new scientific research activity if appropriate notice and choice have been provided in the first instance. Such notice should provide information about any future specific uses of the data, such as periodic follow up, related studies, or marketing.

- ii. It is understood that not all future uses of the data can be specified, since a new research use could arise from new insights on the original data, new medical discoveries and advances, and public health and regulatory developments. Where appropriate, the notice should therefore include an explanation that personal data may be used in future medical and pharmaceutical research activities that are unanticipated. If the use is not consistent with the general research purpose(s) for which the personal data were originally collected, or to which the individual has consented subsequently, new consent must be obtained.
- c. Withdrawal from a Clinical Trial
 - i. Participants may decide or be asked to withdraw from a clinical trial at any time. Any personal data collected previous to withdrawal may still be processed along with other data collected as part of the clinical trial, however, if this was made clear to the participant in the notice at the time he or she agreed to participate.
- d. Transfers for Regulatory and Supervision Purposes
 - i. Pharmaceutical and medical device companies are allowed to provide personal data from clinical trials conducted in the EU to regulators in the United States for regulatory and supervision purposes. Similar transfers are allowed to parties other than regulators, such as company locations and other researchers, consistent with the Principles of Notice and Choice.
- e. "Blinded" Studies
 - i. To ensure objectivity in many clinical trials, participants, and often investigators as well, cannot be given access to information about which treatment each participant may be receiving. Doing so would jeopardize the validity of the research study and results. Participants in such clinical trials (referred to as "blinded" studies) do not have to be provided access to the data on their treatment during the trial if this restriction has been explained when the participant entered the trial and the disclosure of such information would jeopardize the integrity of the research effort.
 - ii. Agreement to participate in the trial under these conditions is a reasonable forgoing of the right of access. Following the conclusion of the trial and analysis of the results, participants should have access to their data if they request it. They should seek it primarily from the physician or other health care provider from whom they received treatment within the clinical trial, or secondarily from the sponsoring organization.
- f. Product Safety and Efficacy Monitoring
 - i. A pharmaceutical or medical device company does not have to apply the Principles with respect to the Notice, Choice, Accountability for Onward Transfer, and Access Principles in its product safety and efficacy monitoring activities, including the reporting of adverse events and the tracking of patients/subjects using certain medicines or medical devices, to the extent that adherence to the Principles interferes with compliance with regulatory requirements. This is true both with respect to reports by, for example, health care providers to pharmaceutical and medical device companies, and with respect to reports by pharmaceutical and medical device companies to government agencies like the Food and Drug Administration.
- g. Key-coded Data
 - i. Invariably, research data are uniquely key-coded at their origin by the principal investigator so as not to reveal the identity of individual data subjects. Pharmaceutical companies sponsoring such research do not receive the key. The unique key code is held only by the researcher, so that he or she can identify the research subject under special circumstances (e.g., if follow-up medical attention is required). A transfer from the EU to the United States of data coded in this way that is EU personal data under EU law would be covered by the Principles.

15. Public Record and Publicly Available Information

- a. An organization must apply the Principles of Security, Data Integrity and Purpose Limitation, and Recourse, Enforcement and Liability to personal data from publicly available sources. These Principles shall apply also to personal data collected from public records (*i.e.*, those records kept by government agencies or entities at any level that are open to consultation by the public in general).
- b. It is not necessary to apply the Notice, Choice, or Accountability for Onward Transfer Principles to public record information, as long as it is not combined with non-public record information, and any conditions for consultation established by the relevant jurisdiction are respected. Also, it is generally not necessary to apply the Notice, Choice, or Accountability for Onward Transfer Principles to publicly available information unless the European transferor indicates that such information is subject to restrictions that require application of those Principles by the organization for the uses it intends. Organizations will have no liability for how such information is used by those obtaining such information from published materials.
- c. Where an organization is found to have intentionally made personal information public in contravention of the Principles so that it or others may benefit from these exceptions, it will cease to qualify for the benefits of the EU-U.S. DPF.
- d. It is not necessary to apply the Access Principle to public record information as long as it is not combined with other personal information (apart from small amounts used to index or organize the public record information); however, any conditions for consultation established by the relevant jurisdiction are to be respected. In contrast, where public record information is combined with other non-public record information (other than as specifically noted above), an organization must provide access to all such information, assuming it is not subject to other permitted exceptions.
- e. As with public record information, it is not necessary to provide access to information that is already publicly available to the public at large, as long as it is not combined with non-publicly available information. Organizations that are in the business of selling publicly available information may charge the organization's customary fee in responding to requests for access. Alternatively, individuals may seek access to their information from the organization that originally compiled the data.

16. Access Requests by Public Authorities

- a. In order to provide transparency in respect of lawful requests by public authorities to access personal information, participating organizations may voluntarily issue periodic transparency reports on the number of requests for personal information they receive by public authorities for law enforcement or national security reasons, to the extent such disclosures are permissible under applicable law.
 - b. The information provided by the participating organizations in these reports together with information that has been released by the intelligence community, along with other information, can be used to inform the periodic joint review of the functioning of the EU-U.S. DPF in accordance with the Principles.
 - c. Absence of notice in accordance with point (a)(xii) of the Notice Principle shall not prevent or impair an organization's ability to respond to any lawful request.
-

ANNEX I: ARBITRAL MODEL

This Annex I provides the terms under which organizations participating in the EU-U.S. DPF are obligated to arbitrate claims, pursuant to the Recourse, Enforcement and Liability Principle. The binding arbitration option described below applies to certain “residual” claims as to data covered by the EU-U.S. DPF. The purpose of this option is to provide a prompt, independent, and fair mechanism, at the option of individuals, for resolution of any claimed violations of the Principles not resolved by any of the other EU-U.S. DPF mechanisms.

A. Scope

This arbitration option is available to an individual to determine, for residual claims, whether a participating organization has violated its obligations under the Principles as to that individual, and whether any such violation remains fully or partially unremedied. This option is available only for these purposes. This option is not available, for example, with respect to the exceptions to the Principles ⁽¹⁾ or with respect to an allegation about the adequacy of the EU-U.S. DPF.

B. Available Remedies

Under this arbitration option, the “EU-U.S. Data Privacy Framework Panel” (the arbitration panel consisting of one or three arbitrators, as agreed by the parties) has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return of the individual's data in question) necessary to remedy the violation of the Principles only with respect to the individual. These are the only powers of the EU-U.S. Data Privacy Framework Panel with respect to remedies. In considering remedies, the EU-U.S. Data Privacy Framework Panel is required to consider other remedies that already have been imposed by other mechanisms under the EU-U.S. DPF. No damages, costs, fees, or other remedies are available. Each party bears its own attorney's fees.

C. Pre-Arbitration Requirements

An individual who decides to invoke this arbitration option must take the following steps prior to initiating an arbitration claim: (1) raise the claimed violation directly with the organization and afford the organization an opportunity to resolve the issue within the timeframe set forth in section (d)(i) of the Supplemental Principle on Dispute Resolution and Enforcement; (2) make use of the independent recourse mechanism under the Principles, at no cost to the individual; and (3) raise the issue through the individual's DPA to the Department and afford the Department an opportunity to use best efforts to resolve the issue within the timeframes set forth in the Letter from the Department's International Trade Administration, at no cost to the individual.

This arbitration option may not be invoked if the individual's same claimed violation of the Principles (1) has previously been subject to binding arbitration; (2) was the subject of a final judgment entered in a court action to which the individual was a party; or (3) was previously settled by the parties. In addition, this option may not be invoked if a DPA (1) has authority under the Supplemental Principle on the Role of the Data Protection Authorities or the Supplemental Principle on Human Resources Data; or (2) has the authority to resolve the claimed violation directly with the organization. A DPA's authority to resolve the same claim against an EU data controller does not alone preclude invocation of this arbitration option against a different legal entity not bound by the DPA authority.

D. Binding Nature of Decisions

An individual's decision to invoke this binding arbitration option is entirely voluntary. Arbitral decisions will be binding on all parties to the arbitration. Once invoked, the individual forgoes the option to seek relief for the same claimed violation in another forum, except that if non-monetary equitable relief does not fully remedy the claimed violation, the individual's invocation of arbitration will not preclude a claim for damages that is otherwise available in the courts.

⁽¹⁾ The Principles, Overview, para. 5.

E. Review and Enforcement

Individuals and participating organizations will be able to seek judicial review and enforcement of the arbitral decisions pursuant to U.S. law under the Federal Arbitration Act. ⁽²⁾ Any such cases must be brought in the federal district court whose territorial coverage includes the primary place of business of the participating organization.

This arbitration option is intended to resolve individual disputes, and arbitral decisions are not intended to function as persuasive or binding precedent in matters involving other parties, including in future arbitrations or in EU or U.S. courts, or FTC proceedings.

F. The Arbitration Panel

The parties will select arbitrators for the EU-U.S. Data Privacy Framework Panel from the list of arbitrators discussed below.

Consistent with applicable law, the Department and the Commission will develop a list of at least 10 arbitrators, chosen on the basis of independence, integrity, and expertise. The following shall apply in connection with this process:

Arbitrators:

- (1) will remain on the list for a period of 3 years, absent exceptional circumstances or removal for cause, renewable by the Department, with prior notification to the Commission, for additional 3-year terms;
- (2) shall not be subject to any instructions from, or be affiliated with, either party, or any participating organization, or the U.S., EU, or any EU Member State or any other governmental authority, public authority, or enforcement authority; and
- (3) must be admitted to practice law in the United States and be experts in U.S. privacy law, with expertise in EU data protection law.

⁽²⁾ Chapter 2 of the Federal Arbitration Act ("FAA") provides that "[a]n arbitration agreement or arbitral award arising out of a legal relationship, whether contractual or not, which is considered as commercial, including a transaction, contract, or agreement described in [section 2 of the FAA], falls under the Convention [on the Recognition and Enforcement of Foreign Arbitral Awards of June 10, 1958, 21 U.S.T. 2519, T.I.A.S. No. 6997 ("New York Convention")." 9 U.S.C. § 202. The FAA further provides that "[a]n agreement or award arising out of such a relationship which is entirely between citizens of the United States shall be deemed not to fall under the [New York] Convention unless that relationship involves property located abroad, envisages performance or enforcement abroad, or has some other reasonable relation with one or more foreign states." *Id.* Under Chapter 2, "any party to the arbitration may apply to any court having jurisdiction under this chapter for an order confirming the award as against any other party to the arbitration. The court shall confirm the award unless it finds one of the grounds for refusal or deferral of recognition or enforcement of the award specified in the said [New York] Convention." *Id.* § 207. Chapter 2 further provides that "[t]he district courts of the United States . . . shall have original jurisdiction over . . . an action or proceeding [under the New York Convention], regardless of the amount in controversy." *Id.* § 203.

Chapter 2 also provides that "Chapter 1 applies to actions and proceedings brought under this chapter to the extent that chapter is not in conflict with this chapter or the [New York] Convention as ratified by the United States." *Id.* § 208. Chapter 1, in turn, provides that "[a] written provision in . . . a contract evidencing a transaction involving commerce to settle by arbitration a controversy thereafter arising out of such contract or transaction, or the refusal to perform the whole or any part thereof, or an agreement in writing to submit to arbitration an existing controversy arising out of such a contract, transaction, or refusal, shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract." *Id.* § 2. Chapter 1 further provides that "any party to the arbitration may apply to the court so specified for an order confirming the award, and thereupon the court must grant such an order unless the award is vacated, modified, or corrected as prescribed in sections 10 and 11 of [the FAA]." *Id.* § 9.

G. Arbitration Procedures

The Department and the Commission have agreed, consistent with applicable law, to the adoption of arbitration rules that govern proceedings before the EU-U.S. Data Privacy Framework Panel. ⁽⁷⁾ In the event the rules governing the proceedings need to be changed, the Department and the Commission will agree to amend those rules or adopt a different set of existing, well-established U.S. arbitral procedures, as appropriate, subject to each of the following considerations:

1. An individual may initiate binding arbitration, subject to the pre-arbitration requirements provision above, by delivering a "Notice" to the organization. The Notice shall contain a summary of steps taken under Paragraph C to resolve the claim, a description of the alleged violation, and, at the choice of the individual, any supporting documents and materials and/or a discussion of law relating to the alleged claim.
2. Procedures will be developed to ensure that an individual's same claimed violation does not receive duplicative remedies or procedures.
3. FTC action may proceed in parallel with arbitration.
4. No representative of the U.S., EU, or any EU Member State or any other governmental authority, public authority, or enforcement authority may participate in these arbitrations, provided, that at the request of an EU individual, DPAs may provide assistance in the preparation only of the Notice but DPAs may not have access to discovery or any other materials related to these arbitrations.
5. The location of the arbitration will be the United States, and the individual may choose video or telephone participation, which will be provided at no cost to the individual. In-person participation will not be required.
6. The language of the arbitration will be English unless otherwise agreed by the parties. Upon a reasoned request, and taking into account whether the individual is represented by an attorney, interpretation at the arbitral hearing, as well as translation of arbitral materials will be provided at no cost to the individual, unless the EU-U.S. Data Privacy Framework Panel finds that, under the circumstances of the specific arbitration, this would lead to unjustified or disproportionate costs.
7. Materials submitted to arbitrators will be treated confidentially and will only be used in connection with the arbitration.
8. Individual-specific discovery may be permitted if necessary, and such discovery will be treated confidentially by the parties and will only be used in connection with the arbitration.
9. Arbitrations should be completed within 90 days of the delivery of the Notice to the organization at issue, unless otherwise agreed to by the parties.

⁽⁷⁾ The International Centre for Dispute Resolution ("ICDR"), the international division of the American Arbitration Association ("AAA") (collectively "ICDR-AAA"), was selected by the Department to administer arbitrations pursuant to and manage the arbitral fund identified in Annex I of the Principles. On September 15, 2017, the Department and the Commission agreed to the adoption of a set of arbitration rules to govern binding arbitration proceedings described in Annex I of the Principles, as well as a code of conduct for arbitrators that is consistent with generally accepted ethical standards for commercial arbitrators and Annex I of the Principles. The Department and the Commission agreed to adapt the arbitration rules and code of conduct to reflect the updates under the EU-U.S. DPF, and the Department will work with the ICDR-AAA to make those updates.

H. Costs

Arbitrators should take reasonable steps to minimize the costs or fees of the arbitrations.

The Department will, consistent with applicable law, facilitate the maintenance of a fund, to which participating organizations will be required to contribute, based in part on the size of the organization, which will cover the arbitral cost, including arbitrator fees, up to maximum amounts ("caps"). The fund will be managed by a third party, which will report regularly to the Department on the operations of the fund. The Department will work with the third party to periodically review the operation of the fund, including the need to adjust the amount of the contributions or of the caps on the arbitral cost, and consider, among other things, the number of arbitrations and the costs and timing of the arbitrations, with the understanding that there will be no excessive financial burden imposed on participating organizations. The Department will notify the Commission of the outcome of such reviews with the third party and will provide the Commission with prior notification of any adjustments of the amount of the contributions. Attorney's fees are not covered by this provision or any fund under this provision.

ANNEX II



UNITED STATES DEPARTMENT OF COMMERCE
Secretary of Commerce
Washington, D.C. 20230

July 6, 2023

The Honorable Didier Reynders
Commissioner for Justice
European Commission
Rue de la Loi/ Weststraat 200
1049 Brussels
Belgium

Dear Commissioner Reynders:

On behalf of the United States, I am pleased to transmit herewith a package of EU-U.S. Data Privacy Framework materials that, combined with Executive Order 14086, “Enhancing Safeguards for United States Signals Intelligence Activities” and 28 CFR part 201 amending Department of Justice regulations to establish the “Data Protection Review Court”, reflects important and detailed negotiations to strengthen privacy and civil liberties protections. These negotiations have resulted in new safeguards to ensure that U.S. signals intelligence activities are necessary and proportionate in the pursuit of defined national security objectives and a new mechanism for European Union (“EU”) individuals to seek redress if they believe they are unlawfully targeted by signals intelligence activities, which together will ensure the privacy of EU personal data. The EU-U.S. Data Privacy Framework will underpin an inclusive and competitive digital economy. We should both be proud of the improvements reflected in that Framework, which will enhance the protection of privacy around the world. This package, along with the Executive Order, Regulations, and other materials available from public sources, provides a very strong basis for a new adequacy finding by the European Commission. ⁽¹⁾

The following materials are attached:

- The EU-U.S. Data Privacy Framework Principles, including the Supplemental Principles (collectively “the Principles”) and Annex I of the Principles (i.e., an annex providing the terms under which Data Privacy Framework organizations are obligated to arbitrate certain residual claims as to personal data covered by the Principles);
- A letter from the Department’s International Trade Administration, which administers the Data Privacy Framework program, describing the commitments that our Department has made to ensure that the EU-U.S. Data Privacy Framework operates effectively;
- A letter from the Federal Trade Commission describing its enforcement of the Principles;
- A letter from the Department of Transportation describing its enforcement of the Principles;
- A letter prepared by the Office of the Director of National Intelligence regarding safeguards and limitations applicable to U.S. national security authorities; and
- A letter prepared by the Department of Justice regarding safeguards and limitations on U.S. Government access for law enforcement and public interest purposes.

⁽¹⁾ Provided that the Commission Decision on the adequacy of the protection provided by the EU-U.S. Data Privacy Framework applies to Iceland, Liechtenstein and Norway, the EU-U.S. Data Privacy Framework Package will cover both the European Union, as well as these three countries.

The full EU-U.S. Data Privacy Framework Package will be published on the Department's Data Privacy Framework website and the Principles and Annex I of the Principles will be effective on the date of entry into force of the European Commission's adequacy decision.

You can be assured that the United States takes these commitments seriously. We look forward to working with you as the EU-U.S. Data Privacy Framework is implemented and as we embark on the next phase of this process together.

Sincerely,



Gina M. RAIMONDO

ANNEX III



UNITED STATES DEPARTMENT OF COMMERCE
International Trade Administration
Washington, D C 20230

December 12, 2022

The Honorable Didier Reynders
Commissioner for Justice
European Commission
Rue de la Loi/Westraat 200
1049 Brussels
Belgium

Dear Commissioner Reynders:

On behalf of the International Trade Administration ("ITA"), I am pleased to describe the commitments the Department of Commerce ("the Department") has made to ensure the protection of personal data through its administration and supervision of the Data Privacy Framework program. Finalizing the EU-U.S. Data Privacy Framework ("EU-U.S. DPF") is a major achievement for privacy and for businesses on both sides of the Atlantic, as it will offer confidence to EU individuals that their data will be protected and that they will have legal remedies to address concerns related to their data, and will enable thousands of businesses to continue to invest and otherwise engage in trade and commerce across the Atlantic to the benefit of our respective economies and citizens. The EU-U.S. DPF reflects years of hard work and collaboration with you and your colleagues in the European Commission ("the Commission"). We look forward to continuing to work with the Commission to ensure that this collaborative effort functions effectively.

The EU-U.S. DPF will yield significant benefits for both individuals and businesses. First, it provides an important set of privacy protections for the data of EU individuals transferred to the United States. It requires participating U.S. organizations to develop a conforming privacy policy; publicly commit to comply with the "EU-U.S. Data Privacy Framework Principles", including the Supplemental Principles (collectively "the Principles"), and Annex I of the Principles (i.e., an annex providing the terms under which EU-U.S. DPF organizations are obligated to arbitrate certain residual claims as to personal data covered by the Principles), so that the commitment becomes enforceable under U.S. law ⁽¹⁾; annually re-certify their compliance to the Department; provide free, independent dispute resolution to EU individuals; and be subject to the investigatory and enforcement authority of a U.S. statutory body listed in the Principles (e.g., the Federal Trade Commission (the "FTC") and Department of Transportation (the "DOT")), or a U.S. statutory body listed in a future annex to the Principles. While an organization's decision to self-certify is voluntary, once an organization publicly commits to the EU-U.S. DPF, its commitment is enforceable under U.S. law by the FTC, DOT, or another U.S. statutory body depending on which body has jurisdiction over the participating organization. Second, the EU-U.S. DPF will enable businesses in the United States, including subsidiaries of European businesses located in the United States, to receive personal data from the European Union to facilitate data flows that support transatlantic trade. Data flows between the

⁽¹⁾ Organizations that self-certified their commitment to comply with the EU-U.S. Privacy Shield Framework Principles and wish to enjoy the benefits of participating in the EU-U.S. DPF must comply with the "EU-U.S. Data Privacy Framework Principles". This commitment to comply with the "EU-U.S. Data Privacy Framework Principles" shall be reflected in the privacy policies of such participating organizations as soon as possible, and in any event no later than three months from the effective date for the "EU-U.S. Data Privacy Framework Principles". (See section (e) of the Supplemental Principle on Self-Certification).

United States and the European Union are the largest in the world and underpin the \$7.1 trillion U.S.-EU economic relationship, which supports millions of jobs on both sides of the Atlantic. Businesses that rely on transatlantic data flows come from all industry sectors and include major Fortune 500 firms, as well as many small and medium-sized enterprises. Transatlantic data flows allow U.S. organizations to process data required to offer goods, services, and employment opportunities to European individuals.

The Department is committed to working closely and productively with our EU counterparts to effectively administer and supervise the Data Privacy Framework program. This commitment is reflected in the Department's development and continued refinement of a variety of resources to assist organizations with the self-certification process, creation of a website to provide targeted information to stakeholders, collaboration with the Commission and European data protection authorities ("DPAs") to develop guidance that clarifies important elements of the EU-U.S. DPF, outreach to facilitate increased understanding of organizations' data protection obligations, and oversight and monitoring of organizations' compliance with the program's requirements.

Our ongoing cooperation with valued EU counterparts will enable the Department to ensure that the EU-U.S. DPF functions effectively. The United States Government has a long history of working with the Commission to promote shared data protection principles, bridging the differences in our respective legal approaches while furthering trade and economic growth in the European Union and the United States. We believe that the EU-U.S. DPF, which is an example of this cooperation, will allow the Commission to issue a new adequacy decision that will permit organizations to use the EU-U.S. DPF to transfer personal data from the European Union to the United States consistent with EU law.

Administration and Supervision of the Data Privacy Framework Program by the Department of Commerce

The Department is firmly committed to the effective administration and supervision of the Data Privacy Framework program and will undertake appropriate efforts and dedicate appropriate resources to ensure that outcome. The Department will maintain and make available to the public an authoritative list of U.S. organizations that have self-certified to the Department and declared their commitment to adhere to the Principles ("the Data Privacy Framework List"), which it will update on the basis of annual re-certification submissions made by participating organizations and by removing organizations when they voluntarily withdraw, fail to complete the annual re-certification in accordance with the Department's procedures, or are found to persistently fail to comply. The Department will also maintain and make available to the public an authoritative record of U.S. organizations that have been removed from the Data Privacy Framework List and will identify the reason each organization was removed. The aforementioned authoritative list and record will remain available to the public on the Department's Data Privacy Framework website. The Data Privacy Framework website will include a prominently placed explanation indicating that any organization removed from the Data Privacy Framework List must cease making claims that it participates in or complies with the EU-U.S. DPF and that it may receive personal information pursuant to the EU-U.S. DPF. Such an organization must nevertheless continue to apply the Principles to the personal information that it received while it participated in the EU-U.S. DPF for as long as it retains such information. The Department, in furtherance of its overarching, ongoing commitment to the effective administration and supervision of the Data Privacy Framework program, specifically undertakes to do the following:

Verify Self-Certification Requirements

- The Department will, prior to finalizing an organization's initial self-certification or annual re-certification (collectively "self-certification") and placing or maintaining an organization on the Data Privacy Framework List, verify that the organization has, at a minimum, met the relevant requirements set forth in the Supplemental Principle on Self-Certification concerning what information an organization must provide in its self-certification submission to the Department and provided at an appropriate time a relevant privacy policy that informs individuals about all 13 of the enumerated elements set forth in the Notice Principle. The Department will verify that the organization has:

- identified the organization that is submitting its self-certification, as well as any U.S. entities or U.S. subsidiaries of the self-certifying organization that are also adhering to the Principles that the organization wishes to be covered by its self-certification;
- provided required organization contact information (e.g., contact information for specific individual(s) and/or office(s) within the self-certifying organization responsible for handling complaints, access requests, and any other issues arising under the EU-U.S. DPF);
- described the purpose(s) for which the organization would collect and use personal information received from the European Union;
- indicated what personal information would be received from the European Union in reliance on the EU-U.S. DPF and therefore be covered by its self-certification;
- if the organization has a public website, provided the web address where the relevant privacy policy is readily available on that website, or if the organization does not have a public website, provided the Department with a copy of the relevant privacy policy and where that privacy policy is available for viewing by affected individuals (i.e., affected employees if the relevant privacy policy is a human resources privacy policy or the public if the relevant privacy policy is not a human resources privacy policy);
- included in its relevant privacy policy at the appropriate time (i.e., initially only in a draft privacy policy provided along with the submission if that submission is an initial self-certification; otherwise, in a final and where applicable published privacy policy) a statement that it adheres to the Principles and a hyperlink to or the web address for the Department's Data Privacy Framework website (e.g., the homepage or the Data Privacy Framework List web page);
- included in its relevant privacy policy at the appropriate time all of the 12 other enumerated elements set forth in the Notice Principle (e.g., the possibility, under certain conditions, for the affected EU individual to invoke binding arbitration; the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements; and its liability in cases of onward transfers to third parties);
- identified the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the Principles or a future annex to the Principles);
- identified any privacy program in which the organization is a member;
- identified whether the relevant method (i.e., follow-up procedures that it must provide) for verifying its compliance with the Principles is "self-assessment" (i.e., in-house verification) or "outside compliance review" (i.e., third-party verification) and if it identified the relevant method as outside compliance review, also identified the third party that has completed that review;
- identified the appropriate independent recourse mechanism that is available to address complaints brought under the Principles and provide appropriate recourse free of charge to the affected individual.
- If the organization has selected an independent recourse mechanism provided by a private-sector alternative dispute resolution body, it included in its relevant privacy policy a hyperlink to or the web address for the relevant website or complaint submission form of the mechanism that is available to investigate unresolved complaints brought under the Principles.
- If the organization either is required to (i.e., with respect to human resources data transferred from the European Union in the context of the employment relationship) or has elected to cooperate with the appropriate DPAs in the investigation and resolution of complaints brought under the Principles, it declared its commitment to such cooperation with the DPAs and compliance with their related advice to take specific action to comply with the Principles.

- The Department will also verify that the organization's self-certification submission is consistent with its relevant privacy policy/ies. Where a self-certifying organization wishes to cover any of its U.S. entities or U.S. subsidiaries that have separate, relevant privacy policies, the Department will also review the relevant privacy policies of such covered entities or subsidiaries to ensure that they include all of the required elements set forth in the Notice Principle.
- The Department will work with statutory bodies (*e.g.*, FTC and DOT) to verify that the organizations are subject to the jurisdiction of the relevant statutory body identified in their self-certification submissions, where the Department has reason to doubt that they are subject to that jurisdiction.
- The Department will work with private-sector alternative dispute resolution bodies to verify that the organizations are actively registered for the independent recourse mechanism identified in their self-certification submissions; and work with those bodies to verify that the organizations are actively registered for the outside compliance review identified in their self-certification submissions, where those bodies may offer both types of services.
- The Department will work with the third party selected by the Department to serve as the custodian of the funds collected through the DPA panel fee (*i.e.*, the annual fee designed to cover the operating costs of the DPA panel) to verify that the organizations have paid that fee for the relevant year, where the organizations have identified the DPAs as the relevant independent recourse mechanism.
- The Department will work with the third party selected by the Department to administer arbitrations pursuant to and manage the arbitral fund identified in Annex I of the Principles to verify that the organizations have contributed to that arbitral fund.
- Where the Department identifies any issues during its review of organizations' self-certification submissions, it will inform them that they must address all such issues within the appropriate timeframe designated by the Department. ⁽²⁾ The Department will also inform them that failure to respond within timeframes designated by the Department or other failure to complete their self-certification in accordance with the Department's procedures will lead to those self-certification submissions being considered abandoned, and that any misrepresentation about an organization's participation in or compliance with the EU-U.S. DPF may be subject to enforcement action by the FTC, the DOT, or other relevant government body. The Department will inform the organizations through the means of contact that the organizations provided to the Department.

Facilitate Cooperation with Alternative Dispute Resolution Bodies That Provide Principles-Related Services

- The Department will work with private-sector alternative dispute resolution bodies providing independent recourse mechanisms, which are available to investigate unresolved complaints brought under the Principles, to verify that they meet, at a minimum, the requirements set forth in the Supplemental Principle on Dispute Resolution and Enforcement. The Department will verify that they:
 - include information on their public websites regarding the Principles and the services that they provide under the EU-U.S. DPF, which must include: (1) information on or a hyperlink to the Principles' requirements for independent recourse mechanisms; (2) a hyperlink to the Department's Data Privacy Framework website; (3) an explanation that their dispute resolution services under the EU-U.S. DPF are free of charge to individuals; (4) a description of how a Principles-related complaint can be filed; (5) the timeframe in which Principles-related complaints are processed; and (6) a description of the range of potential remedies. The Department will provide the bodies with timely notice of material changes to the Department's supervision and administration of the Data Privacy Framework program, where such changes are imminent or have already been made and such changes are relevant to the role that the bodies play under the EU-U.S. DPF;

⁽²⁾ *E.g.*, As regards re-certification, the expectation would be that organizations address all such issues within 45 days; subject to the designation by the Department of a different, appropriate timeframe.

- publish an annual report providing aggregate statistics regarding their dispute resolution services, which must include: (1) the total number of Principles-related complaints received during the reporting year; (2) the types of complaints received; (3) dispute resolution quality measures, such as the length of time taken to process complaints; and (4) the outcomes of the complaints received, notably the number and types of remedies or sanctions imposed. The Department will provide the bodies with specific, complementary guidance on what information they should provide in those annual reports elaborating upon those requirements (*e.g.*, listing the specific criteria that a complaint must meet to be considered a Principles-related complaint for purposes of the annual report), as well as identifying other types of information they should provide (*e.g.*, if the body also provides a Principles-related verification service, a description of how the body avoids any actual or potential conflicts of interest in situations when it provides an organization with both verification services and dispute resolution services). The additional guidance provided by the Department will also specify the date by which the bodies' annual reports should be published for the relevant reporting period.

Follow Up with Organizations That Wish to Be or Have Been Removed from the Data Privacy Framework List

- If an organization wishes to withdraw from the EU-U.S. DPF, the Department will require that the organization remove from any relevant privacy policy any references to EU-U.S. DPF that imply that it continues to participate in the EU-U.S. DPF and that it may receive personal data pursuant to the EU-U.S. DPF (*see* description of the Department's commitment to search for false claims of participation). The Department will also require that the organization complete and submit to the Department an appropriate questionnaire to verify:
 - its wish to withdraw;
 - which of the following it will do with the personal data that it received in reliance on the EU-U.S. DPF while it participated in the EU-U.S. DPF: (a) retain such data, continue to apply the Principles to such data, and affirm to the Department on an annual basis its commitment to apply the Principles to such data; (b) retain such data and provide "adequate" protection for such data by another authorized means; or (c) return or delete all such data by a specified date; and
 - who within the organization will serve as an ongoing point of contact for Principles-related questions.
- If an organization elected (a) as described immediately above, the Department will also require that it complete and submit to the Department each year after its withdrawal (*i.e.*, by the first anniversary of its withdrawal, as well as by every subsequent anniversary unless and until the organization either provides "adequate" protection for such data by another authorized means or returns or deletes all such data and notifies the Department of this action) an appropriate questionnaire to verify what it has done with that personal data, what it will do with any of that personal data that it continues to retain, and who within the organization will serve as an ongoing point of contact for Principles-related questions.
- If an organization has allowed its self-certification to lapse (*i.e.*, neither completed its annual re-certification of its adherence to the Principles nor was removed from the Data Privacy Framework List for some other reason, such as withdrawal), the Department will direct it to complete and submit to the Department an appropriate questionnaire to verify whether it wishes to withdraw or re-certify:
 - and if it wishes to withdraw, further verify what it will do with the personal data that it received in reliance on the EU-U.S. DPF while it participated in the EU-U.S. DPF (*see* previous description of what an organization must verify if it wishes to withdraw);
 - and if it intends to re-certify, further verify that during the lapse of its certification status it applied the Principles to personal data received under the EU-U.S. DPF and clarify what steps it will take to address the outstanding issues that have delayed its re-certification.

- If an organization is removed from the Data Privacy Framework List for any of the following reasons: (a) withdrawal from the EU-U.S. DPF, (b) failure to complete the annual re-certification of its adherence to the Principles (*i.e.*, either started, but failed to complete the annual re-certification process in a timely manner or did not even start the annual re-certification process), or (c) “persistent failure to comply”, the Department will send a notification to the contact(s) identified in the organization’s self-certification submission specifying the reason for the removal and explaining that it must cease making any explicit or implicit claims that it participates in or complies with the EU-U.S. DPF and that it may receive personal data pursuant to the EU-U.S. DPF. The notification, which may also include other content tailored to fit the reason for the removal, will indicate that organizations misrepresenting their participation in or compliance with the EU-U.S. DPF, including where they represent that they are participating in the EU-U.S. DPF after having been removed from the Data Privacy Framework List, may be subject to enforcement action by the FTC, the DOT, or other relevant government body.

Search for and Address False Claims of Participation

- On an ongoing basis, when an organization: (a) withdraws from participation in the EU-U.S. DPF, (b) fails to complete the annual re-certification of its adherence to the Principles (*i.e.*, either started, but failed to complete the annual re-certification process in a timely manner or did not even start the annual re-certification process), (c) is removed as a participant in the EU-U.S. DPF notably for “persistent failure to comply,” or (d) fails to complete an initial self-certification of its adherence to the Principles (*i.e.*, started, but failed to complete the initial self-certification process in a timely manner), the Department will undertake, on an *ex officio* basis action to verify that any relevant published privacy policy of the organization does not contain references to the EU-U.S. DPF that imply that the organization participates in the EU-U.S. DPF and that it may receive personal data pursuant to the EU-U.S. DPF. Where the Department finds such references, the Department will inform the organization that the Department will, as appropriate, refer the matter to the relevant agency for potential enforcement action if the organization continues to misrepresent its participation in the EU-U.S. DPF. The Department will inform the organization through the means of contact the organization provided to the Department or where necessary other appropriate means. If the organization neither removes the references nor self-certifies its compliance under the EU-U.S. DPF in accordance with the Department’s procedures, the Department will *ex officio*, refer the matter to the FTC, DOT, or other appropriate enforcement agency, or take other appropriate action to ensure proper use of the EU-U.S. DPF certification mark;
- The Department will undertake other efforts to identify false claims of EU-U.S. DPF participation and improper use of the EU-U.S. DPF certification mark, including by organizations that unlike the organizations described immediately above have never even started the self-certification process (*e.g.*, conducting appropriate Internet searches to identify references to EU-U.S. DPF in organizations’ privacy policies). Where through such efforts the Department identifies false claims of EU-U.S. DPF participation and improper use of the EU-U.S. DPF certification mark, the Department will inform the organization that the Department will, as appropriate, refer the matter to the relevant agency for potential enforcement action if the organization continues to misrepresent its participation in the EU-U.S. DPF. The Department will inform the organization through the means of contact, if any, the organization provided to the Department or where necessary other appropriate means. If the organization neither removes the references nor self-certifies its compliance under the EU-U.S. DPF in accordance with the Department’s procedures, the Department will *ex officio*, refer the matter to the FTC, DOT, or other appropriate enforcement agency, or take other appropriate action to ensure proper use of the EU-U.S. DPF certification mark;
- The Department will promptly review and address specific, non-frivolous complaints about false claims of EU-U.S. DPF participation that the Department receives (*e.g.*, complaints received from the DPAs, independent recourse mechanisms provided by private-sector alternative dispute resolution bodies, data subjects, EU and U.S. businesses, and other types of third parties); and
- The Department may take other appropriate corrective action. Misrepresentations to the Department may be actionable under the False Statements Act (18 U.S.C. § 1001).

Conduct Periodic *ex officio* Compliance Reviews and Assessments of the Data Privacy Framework Program

- On an ongoing basis, the Department will undertake efforts to monitor effective compliance by EU-U.S. DPF organizations to identify issues that may warrant follow-up action. In particular, the Department will conduct, on an *ex officio* basis routine spot checks of randomly selected EU-U.S. DPF organizations, as well as *ad hoc* spot checks of specific EU-U.S. DPF organizations when potential compliance deficiencies are identified (e.g., potential compliance deficiencies brought to the attention of the Department by third parties) to verify: (a) that the point(s) of contact responsible for the handling of complaints, access requests, and other issues arising under the EU-U.S. DPF are available; (b) where applicable, that the organization's public-facing privacy policy is readily available for viewing by the public both on the organization's public website and via a hyperlink on the Data Privacy Framework List; (c) that the organization's privacy policy continues to comply with the self-certification requirements described in the Principles; and (d) that the independent recourse mechanism identified by the organization is available to address complaints brought under the EU-U.S. DPF. The Department will also actively monitor the news for reports that provide credible evidence of non-compliance by EU-U.S. DPF organizations;
- As part of the compliance review, the Department will require that a EU-U.S. DPF organization complete and submit to the Department a detailed questionnaire when: (a) the Department has received any specific, non-frivolous complaints about the organization's compliance with the Principles, (b) the organization does not respond satisfactorily to inquiries by the Department for information relating to the EU-U.S. DPF, or (c) there is credible evidence that the organization does not comply with its commitments under the EU-U.S. DPF. Where the Department has sent such a detailed questionnaire to an organization and the organization fails to satisfactorily reply to the questionnaire, the Department will inform the organization that the Department will, as appropriate, refer the matter to the relevant agency for potential enforcement action if the Department does not receive a timely and satisfactory response from the organization. The Department will inform the organization through the means of contact the organization provided to the Department or where necessary other appropriate means. If the organization does not provide a timely and satisfactory response, the Department will *ex officio* refer the matter to the FTC, DOT, or other appropriate enforcement agency, or take other appropriate action towards ensuring compliance. The Department shall, when appropriate, consult with the competent data protection authorities about such compliance reviews; and
- The Department will assess periodically the administration and supervision of the Data Privacy Framework program to ensure that its monitoring efforts, including any such efforts undertaken through the use of search tools (e.g., to check for broken links to EU-U.S. DPF organizations' privacy policies), are appropriate to address existing issues and any new issues as they arise.

Tailor the Data Privacy Framework Website to Targeted Audiences

The Department will tailor the Data Privacy Framework website to focus on the following target audiences: EU individuals, EU businesses, U.S. businesses, and DPAs. The inclusion of material targeted directly to EU individuals and EU businesses will facilitate transparency in a number of ways. With regard to EU individuals, the website will clearly explain: (1) the rights the EU-U.S. DPF provides to EU individuals; (2) the recourse mechanisms available to EU individuals when they believe an organization has breached its commitment to comply with the Principles; and (3) how to find information pertaining to an organization's EU-U.S. DPF self-certification. With regard to EU businesses, it will facilitate verification of: (1) whether an organization is a participant in the EU-U.S. DPF; (2) the type of information covered by an organization's EU-U.S. DPF self-certification; (3) the privacy policy that applies to the covered information; and (4) the method the organization uses to verify its adherence to the Principles. With regard to U.S. businesses, it will clearly explain: (1) the benefits of EU-U.S. DPF participation; (2) how to join the EU-U.S. DPF, as well as how to re-certify to and withdraw from the EU-U.S. DPF; and (3) how the United States administers and enforces the EU-U.S. DPF. The inclusion of material targeted directly to DPAs (e.g., information about the Department's dedicated point of contact for DPAs and a hyperlink to Principles-related content on the FTC website) will facilitate both cooperation and transparency. The Department will also work on an *ad hoc* basis with the Commission and the European Data Protection Board ("EDPB") to develop additional, topical material (e.g., answers to frequently asked questions) for use on the Data Privacy Framework website, where such information would facilitate the efficient administration and supervision of the Data Privacy Framework program.

Facilitate Cooperation with DPAs

To increase opportunities for cooperation with DPAs, the Department will maintain a dedicated point of contact at the Department to act as a liaison with DPAs. In instances where a DPA believes that a EU-U.S. DPF organization is not complying with the Principles, including following a complaint from an EU individual, the DPA will be able to reach out to the dedicated point of contact at the Department to refer the organization for further review. The Department will make its best effort to facilitate resolution of the complaint with the EU-U.S. DPF organization. Within 90 days after receipt of the complaint, the Department will provide an update to the DPA. The dedicated point of contact will also receive referrals regarding organizations that falsely claim to participate in the EU-U.S. DPF. The dedicated point of contact will track all referrals from DPAs received by the Department, and the Department will provide in the joint review described below a report analyzing in aggregate the complaints it receives each year. The dedicated point of contact will assist DPAs seeking information related to a specific organization's self-certification or previous participation in the EU-U.S. DPF, and the dedicated point of contact will respond to DPA inquiries regarding the implementation of specific EU-U.S. DPF requirements. The Department will also cooperate with the Commission and the EDPB on procedural and administrative aspects of the DPA panel, including the establishment of appropriate procedures for the distribution of funds collected through the DPA panel fee. We understand that the Commission will work with the Department to facilitate resolution of any issues that may arise regarding those procedures. In addition, the Department will provide DPAs with material regarding the EU-U.S. DPF for inclusion on their own websites to increase transparency for EU individuals and EU businesses. Increased awareness regarding the EU-U.S. DPF and the rights and responsibilities it creates should facilitate the identification of issues as they arise, so that these can be appropriately addressed.

Fulfill Its Commitments under Annex I of the Principles

The Department will fulfill its commitments under Annex I of the Principles, including maintaining a list of arbitrators chosen with the Commission on the basis of independence, integrity, and expertise; and supporting, as appropriate, the third party selected by the Department to administer arbitrations pursuant to and manage the arbitral fund identified in Annex I of the Principles. ⁽³⁾ The Department will work with the third party to, among other things, verify that the third party maintains a website with guidance on the arbitration process, including: (1) how to initiate proceedings and submit documents; (2) the list of arbitrators maintained by the Department and how to select arbitrators from that list; (3) the governing arbitral procedures and arbitrator code of conduct adopted by the Department and the Commission; ⁽⁴⁾ and (4) the collection and payment of arbitrator fees. In addition, the Department will work with the third party to periodically review the operation of the arbitral fund, including the need to adjust the amount of the contributions or the caps (*i.e.*, maximum amounts) on the arbitral cost, and consider, among other things, the number of arbitrations and the costs and timing of the arbitrations, with the understanding that there will be no excessive financial burden imposed on EU-U.S. DPF organizations. The Department will notify the Commission of the outcome of such reviews with the third party and will provide the Commission with prior notification of any adjustments of the amount of the contributions.

Conduct Joint Reviews of the Functioning of the EU-U.S. DPF

The Department and other agencies, as appropriate, will hold meetings on a periodic basis with the Commission, interested DPAs, and appropriate representatives from the EDPB, where the Department will provide updates on the EU-U.S. DPF. The meetings will include discussion of current issues related to the functioning, implementation, supervision, and enforcement of the Data Privacy Framework program. The meetings may, as appropriate, include discussion of related topics, such as other data transfer mechanisms that benefit from the safeguards under the EU-U.S. DPF.

⁽³⁾ The International Centre for Dispute Resolution ("ICDR"), the international division of the American Arbitration Association ("AAA") (collectively "ICDR-AAA"), was selected by the Department to administer arbitrations pursuant to and manage the arbitral fund identified in Annex I of the Principles.

⁽⁴⁾ On September 15, 2017, the Department and the Commission agreed to the adoption of a set of arbitral rules to govern binding arbitration proceedings described in Annex I of the Principles, as well as a code of conduct for arbitrators that is consistent with generally accepted ethical standards for commercial arbitrators and Annex I of the Principles. The Department and the Commission agreed to adapt the arbitration rules and code of conduct to reflect the updates under the EU-U.S. DPF, and the Department will work with the ICDR-AAA to make those updates.

Update of Laws

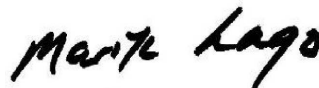
The Department will make reasonable efforts to inform the Commission of material developments in the law in the United States so far as they are relevant to the EU-U.S. DPF in the field of data privacy protection and the limitations and safeguards applicable to access to personal data by U.S. authorities and its subsequent use.

U.S. Government Access to Personal Data

The United States has issued Executive Order 14086, "Enhancing Safeguards for United States Signals Intelligence Activities" and 28 CFR part 201 amending Department of Justice regulations to establish the Data Protection Review Court (the "DPRC"), which provide strong protection for personal data with respect to government access to data for national security purposes. The protection provided includes: strengthening privacy and civil liberties safeguards to ensure that U.S. signals intelligence activities are necessary and proportionate in the pursuit of defined national security objectives; establishing a new redress mechanism with independent and binding authority; and enhancing the existing rigorous and layered oversight of U.S. signals intelligence activities. Through these protections, EU individuals may seek redress from a new multi-layer redress mechanism that includes an independent DPRC that would consist of individuals chosen from outside the U.S. Government who would have full authority to adjudicate claims and direct remedial measures as needed. The Department will maintain a record of EU individuals who submit a qualifying complaint pursuant to Executive Order 14086 and 28 CFR part 201. Five years after the date of this letter, and on a five-year basis thereafter, the Department will contact relevant agencies regarding whether information pertaining to the review of qualifying complaints or review of any applications for review submitted to the DPRC has been declassified. If such information has been declassified, the Department will work with the relevant DPA to inform the EU individual. These enhancements confirm that EU personal data transferred to the United States will be treated in a manner consistent with EU legal requirements with respect to government access to data.

On the basis of the Principles, Executive Order 14086, 28 CFR part 201, and the accompanying letters and materials, including the Department's commitments regarding the administration and supervision of the Data Privacy Framework program, our expectation is that the Commission will determine that the EU-U.S. DPF provides adequate protection for the purposes of EU law and data transfers from the European Union will continue to organizations that participate in the EU-U.S. DPF. We also expect that transfers to U.S. organizations made in reliance on EU Standard Contractual Clauses or EU Binding Corporate Rules will be further facilitated by the terms of those arrangements.

Sincerely,



Marisa LAGO

ANNEX IV



UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of the Chair

June 9, 2023

Didier Reynders
Commissioner for Justice
European Commission
Rue de la Loi / Wetstraat 200
1049 Brussels
Belgium

Dear Commissioner Reynders:

The United States Federal Trade Commission ("FTC") appreciates the opportunity to address its enforcement role in connection with the EU-U.S. Data Privacy Framework ("EU-U.S. DPF") Principles. The FTC has long committed to protecting consumers and privacy across borders, and we are committed to enforcement of the commercial sector aspects of this framework. The FTC has performed such a role since the year 2000, in connection with the U.S.-EU Safe Harbor Framework, and most recently since 2016, in connection with the EU-U.S. Privacy Shield Framework. ⁽¹⁾ On July 16, 2020, the Court of Justice of the European Union ("CJEU") invalidated the European Commission's adequacy decision underlying the EU-U.S. Privacy Shield Framework, on the basis of issues other than the commercial principles that the FTC enforced. The U.S. and the European Commission have since negotiated the EU-U.S. Data Privacy Framework to address that CJEU ruling.

I write to confirm the FTC's commitment to vigorous enforcement of the EU-U.S. DPF Principles. Notably, we affirm our commitment in three key areas: (1) referral prioritization and investigations; (2) seeking and monitoring orders; and (3) enforcement cooperation with EU data protection authorities ("DPAs").

I. Introduction

a. FTC Privacy Enforcement and Policy Work

The FTC has broad civil enforcement authority to promote consumer protection and competition in the commercial sphere. As part of its consumer protection mandate, the FTC enforces a wide range of laws to protect the privacy and security of consumers and their data. The primary law enforced by the FTC, the FTC Act, prohibits "unfair" or "deceptive"

⁽¹⁾ Letter from Chairwoman Edith Ramirez to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission, Describing Federal Trade Commission Enforcement of the New EU-U.S. Privacy Shield Framework (February 29, 2016), available at <https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european>. The FTC also previously committed to enforce the U.S.-EU Safe Harbor Program. Letter from Robert Pitofsky, FTC Chairman, to John Mogg, Director DG Internal Market, European Commission (July 14, 2000), available at <https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission>. This letter replaces those earlier commitments.

acts or practices in or affecting commerce. ⁽²⁾ The FTC also enforces targeted statutes that protect information relating to health, credit, and other financial matters, as well as children's online information, and has issued regulations implementing each of these statutes. ⁽³⁾

The FTC has also recently pursued numerous initiatives to strengthen our privacy work. In August of 2022 the FTC announced it is considering rules to crack down on harmful commercial surveillance and lax data security. ⁽⁴⁾ The goal of the project is to build a robust public record to inform whether the FTC should issue rules to address commercial surveillance and data security practices, and what those rules should potentially look like. We have welcomed comments from EU stakeholders on this and other initiatives.

Our "PrivacyCon" conferences continue to gather leading researchers to discuss the latest research and trends related to consumer privacy and data security. We also have increased our agency's ability to keep pace with the technology developments at the center of much of our privacy work, building a growing team of technologists and interdisciplinary researchers. We also, as you know, announced a joint dialogue with you and your colleagues at the European Commission, which includes addressing such privacy-related topics as dark patterns and business models characterized by pervasive data collection. ⁽⁵⁾ We also recently issued a report to Congress warning about harms associated with using artificial intelligence ("AI") to address online harms identified by Congress. This report raised concerns regarding inaccuracy, bias, discrimination, and commercial surveillance creep. ⁽⁶⁾

b. U.S. Legal Protections Benefitting EU Consumers

The EU-U.S. DPF operates in the context of the larger U.S. privacy landscape, which also protects EU consumers in a number of ways. The FTC Act's prohibition on unfair or deceptive acts or practices is not limited to protecting U.S. consumers from U.S. companies, as it includes those practices that (1) cause or are likely to cause reasonably foreseeable injury in the United States, or (2) involve material conduct in the United States. Further, the FTC can use all remedies that are available to protect domestic consumers when protecting foreign consumers. ⁽⁷⁾

The FTC also enforces other targeted laws whose protections extend to non-U.S. consumers, such as the Children's Online Privacy Protection Act ("COPPA"). Among other things, COPPA requires that operators of child-directed websites and online services, or general audience sites that knowingly collect personal information from children under the age of 13, provide parental notice and obtain verifiable parental consent. U.S.-based websites and services that are subject to COPPA and collect personal information from foreign children are required to comply with COPPA. Foreign-based websites and

⁽²⁾ 15 U.S.C. § 45(a). The FTC does not have jurisdiction over criminal law enforcement or national security matters. Nor can the FTC reach most other governmental actions. In addition, there are exceptions to the FTC's jurisdiction over commercial activities, including with respect to banks, airlines, the business of insurance, and the common carrier activities of telecommunications service providers. The FTC also does not have jurisdiction over most non-profit organizations, though it does have jurisdiction over sham charities or other non-profits that in fact operate for profit. The FTC also has jurisdiction over non-profit organizations that operate for the profit of their for-profit members, including by providing substantial economic benefits to those members. In some instances, the FTC's jurisdiction is concurrent with that of other law enforcement agencies. We have developed strong working relationships with federal and state authorities, and work closely with them to coordinate investigations or make referrals where appropriate.

⁽³⁾ See FTC, Privacy and Security, <https://www.ftc.gov/business-guidance/privacy-security>.

⁽⁴⁾ See Press Release, Fed. Trade Comm'n, FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices (Aug. 11, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices>.

⁽⁵⁾ See Joint Press Statement by Didier Reynnders, Commissioner for Justice of the European Commission and Lina Khan, Chair of the United States Federal Trade Commission (March 30, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf.

⁽⁶⁾ See Press Release, Fed. Trade Comm'n, FTC Report Warns About Using Artificial Intelligence to Combat Online Problems (June 16, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems>.

⁽⁷⁾ 15 U.S.C. § 45(a)(4)(B). Further, "unfair or deceptive acts or practices" includes such acts or practices involving foreign commerce that (i) cause or are likely to cause reasonably foreseeable injury within the United States; or (ii) involve material conduct occurring within the United States. 15 U.S.C. § 45(a)(4)(A).

online services must also comply with COPPA if they are directed to children in the United States, or if they knowingly collect personal information from children in the United States. Moreover, in addition to the U.S. federal laws enforced by the FTC, other federal and state consumer protection, data breach, and privacy laws may provide additional benefits to EU consumers.

c. FTC Enforcement Activity

The FTC brought cases under both the U.S.-EU Safe Harbor and EU-U.S. Privacy Shield frameworks and continued to enforce the EU-U.S. Privacy Shield even after the CJEU invalidation of the adequacy decision underlying the EU-U.S. Privacy Shield Framework.⁽⁸⁾ Several of the FTC's recent complaints have included counts alleging that firms violated EU-U.S. Privacy Shield provisions, including in proceedings against Twitter,⁽⁹⁾ CafePress,⁽¹⁰⁾ and Flo.⁽¹¹⁾ In the enforcement action against Twitter, the FTC secured \$150 million from Twitter for its violation of an earlier FTC order with practices affecting more than 140 million customers, including violating EU-U.S. Privacy Shield Principle 5 (Data Integrity and Purpose Limitation). Further, the agency's order requires that Twitter allow users to employ secure multifactor authentication methods that do not require users to provide their telephone numbers.

In *CafePress*, the FTC alleged that the company failed to secure consumers' sensitive information, covered up a major data breach, and violated EU-U.S. Privacy Shield Principles 2 (Choice), 4 (Security), and 6 (Access). The FTC's order requires the company to replace inadequate authentication measures with multifactor authentication, substantively limit the amount of data it collects and retains, encrypt Social Security numbers, and have a third party assess its information security programs and provide the FTC with a copy that can be publicized.

In *Flo*, the FTC alleged that the fertility-tracking app disclosed user health information to third-party data analytics providers after commitments to keep such information private. The FTC complaint specifically notes the company's interactions with EU consumers and that Flo violated EU-U.S. Privacy Shield Principles 1 (Notice), 2 (Choice), 3 (Accountability for Onward Transfer), and 5 (Data Integrity and Purpose Limitation). Among other things, the agency's order requires Flo to notify affected users about the disclosure of their personal information and to instruct any third party that received users' health information to destroy that data. Importantly, FTC orders protect all consumers worldwide who interact with a U.S. business, not just those consumers who have lodged complaints.

Many past U.S.-EU Safe Harbor and EU-U.S. Privacy Shield enforcement cases involved organizations that completed an initial self-certification through the Department of Commerce, but failed to maintain their annual self-certification while they continued to represent themselves as current participants. Other cases involved false claims of participation by organizations that never completed an initial self-certification through the Department of Commerce. Going forward, we expect to focus our proactive enforcement efforts on the types of substantive violations of the EU-U.S. DPF Principles alleged in cases such as Twitter, CafePress, and Flo. Meanwhile, the Department of Commerce will administer and supervise the self-certification process, maintain the authoritative list of EU-U.S. DPF participants, and address other program participation claim issues.⁽¹²⁾ Importantly, organizations claiming EU-U.S. DPF participation may be subject to substantive enforcement of the EU-U.S. DPF Principles even if they fail to make or maintain their self-certification through the Department of Commerce.

⁽⁸⁾ See Appendix A for a list of FTC Safe Harbor and Privacy Shield matters.

⁽⁹⁾ See Press Release, Fed. Trade Comm'n, FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads (May 25, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads>.

⁽¹⁰⁾ See Press Release, Fed. Trade Comm'n, FTC Takes Action Against CafePress for Data Breach Cover Up (March 15, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover>.

⁽¹¹⁾ See Press Release, Fed. Trade Comm'n, FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others (June 22, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google>.

⁽¹²⁾ Letter from Marisa Lago, Under Secretary of Commerce for International Trade, to the Honorable Didier Reynders, Commissioner for Justice, European Commission (December 12, 2022).

II. Referral Prioritization and Investigations

As we did under the U.S.-EU Safe Harbor Framework and the EU-U.S. Privacy Shield Framework, the FTC commits to give priority consideration to EU-U.S. DPF Principles referrals from the Department of Commerce and EU Member States. We will also prioritize consideration of referrals for non-compliance with the EU-U.S. DPF Principles from privacy self-regulatory organizations and other independent dispute resolution bodies.

To facilitate referrals under the EU-U.S. DPF from EU Member States, the FTC has created a standardized referral process and has provided guidance to EU Member States on the type of information that would best assist the FTC in its inquiry into a referral. As part of this effort, the FTC has designated an agency point of contact for EU Member State referrals. It is most useful when the referring authority has conducted a preliminary inquiry into the alleged violation and can cooperate with the FTC in an investigation.

Upon receipt of such a referral from the Department of Commerce, an EU Member State, or self-regulatory organization or other independent dispute resolution bodies the FTC can take a range of actions to address the issues raised. For example, we may review the organization's privacy policies, obtain further information directly from the organization or from third parties, follow up with the referring entity, assess whether there is a pattern of violations or significant number of consumers affected, determine whether the referral implicates issues within the purview of the Department of Commerce, assess whether additional efforts to put market participants on notice would be helpful, and, as appropriate, initiate an enforcement proceeding.

In addition to prioritizing EU-U.S. DPF Principles referrals from the Department of Commerce, EU Member States, and privacy self-regulatory organizations or other independent dispute resolution bodies, ⁽¹³⁾ the FTC will continue to investigate significant EU-U.S. DPF Principles violations on its own initiative where appropriate, using a range of tools. As part of the FTC's program of investigating privacy and security issues involving commercial organizations, the agency has routinely examined whether the entity at issue was making EU-U.S. Privacy Shield representations. If the entity made such representations and the investigation revealed apparent violations of the EU-U.S. Privacy Shield Principles, the FTC included allegations of EU-U.S. Privacy Shield violations in its enforcement actions. We will continue this proactive approach, now with respect to the EU-U.S. DPF Principles.

III. Seeking and Monitoring Orders

The FTC also affirms its commitment to seek and monitor enforcement orders to ensure compliance with the EU-U.S. DPF Principles. We will require compliance with the EU-U.S. DPF Principles through a variety of appropriate injunctive provisions in future FTC EU-U.S. DPF Principles orders. Violations of the FTC's administrative orders can lead to civil penalties of up to \$50,120 per violation, or \$50,120 per day for a continuing violation, ⁽¹⁴⁾ which, in the case of practices affecting many consumers, can amount to millions of dollars. Each consent order also has reporting and compliance provisions. The entities under order must retain documents demonstrating their compliance for a specified number of years. The orders must also be disseminated to employees responsible for ensuring order compliance.

The FTC systematically monitors compliance with existing EU-U.S. Privacy Shield Principles orders, as it does with all of its orders, and brings actions to enforce them when necessary. ⁽¹⁵⁾ Importantly, FTC orders will continue to protect all consumers worldwide who interact with a business, not just those consumers who have lodged complaints. Finally, the FTC will maintain an online list of companies subject to orders obtained in connection with enforcement of the EU-U.S. DPF Principles. ⁽¹⁶⁾

⁽¹³⁾ Although the FTC does not resolve or mediate individual consumer complaints, the FTC affirms that it will prioritize EU-U.S. DPF Principles referrals from EU DPAs. In addition, the FTC uses complaints in its Consumer Sentinel database, which is accessible by many other law enforcement agencies, to identify trends, determine enforcement priorities, and identify potential investigative targets. EU individuals can use the same complaint system available to U.S. consumers to submit a complaint to the FTC at <https://reportfraud.ftc.gov/>. For individual EU-U.S. DPF Principles complaints, however, it may be most useful for EU individuals to submit complaints to their Member State DPA or independent dispute resolution body.

⁽¹⁴⁾ 15 U.S.C. § 45(m); 16 C.F.R. § 1.98. This amount is periodically adjusted for inflation.

⁽¹⁵⁾ Last year the FTC voted to streamline the process for investigating repeat offenders. See Press Release, Fed. Trade Comm'n, FTC Authorizes Investigations into Key Enforcement Priorities (Jul. 1, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities>.

⁽¹⁶⁾ Cf. FTC, Privacy Shield, <https://www.ftc.gov/business-guidance/privacy-security/privacy-shield>.

IV. Enforcement Cooperation with EU DPAs

The FTC recognizes the important role that EU DPAs can play with respect to EU-U.S. DPF Principles compliance and encourages increased consultation and enforcement cooperation. Indeed, a coordinated approach to the challenges posed by current digital market developments, and data-intensive business models, is increasingly critical. The FTC will exchange information on referrals with referring enforcement authorities, including the status of referrals, subject to confidentiality laws and restrictions. To the extent feasible given the number and type of referrals received, the information provided will include an evaluation of the referred matters, including a description of significant issues raised and any action taken to address law violations within the jurisdiction of the FTC. The FTC will also provide feedback to the referring authority on the types of referrals received in order to increase the effectiveness of efforts to address unlawful conduct. If a referring enforcement authority seeks information about the status of a particular referral for purposes of pursuing its own enforcement proceeding, the FTC will respond, taking into account the number of referrals under consideration and subject to confidentiality and other legal requirements.

The FTC will also work closely with EU DPAs to provide enforcement assistance. In appropriate cases, this could include information sharing and investigative assistance pursuant to the U.S. SAFE WEB Act, which authorizes FTC assistance to foreign law enforcement agencies when the foreign agency is enforcing laws prohibiting practices that are substantially similar to those prohibited by laws the FTC enforces.⁽¹⁷⁾ As part of this assistance, the FTC can share information obtained in connection with an FTC investigation, issue compulsory process on behalf of the EU DPA conducting its own investigation, and seek oral testimony from witnesses or defendants in connection with the DPA's enforcement proceeding, subject to the requirements of the U.S. SAFE WEB Act. The FTC regularly uses this authority to assist other authorities around the world in privacy and consumer protection cases.

In addition to any consultation with referring EU DPAs on case-specific matters, the FTC will participate in periodic meetings with designated representatives of the European Data Protection Board ("EDPB") to discuss in general terms how to improve enforcement cooperation. The FTC will also participate, along with the Department of Commerce, the European Commission, and EDPB representatives, in the periodic review of EU-U.S. DPF to discuss its implementation. The FTC also encourages the development of tools that will enhance enforcement cooperation with EU DPAs, as well as other privacy enforcement authorities around the world. The FTC is pleased to affirm its commitment to enforcing the commercial sector aspects of the EU-U.S. DPF. We see our partnership with EU colleagues as a critical part of providing privacy protection for both our citizens and yours.

Sincerely,



Lina M. KHAN

Chair, Federal Trade Commission

⁽¹⁷⁾ In determining whether to exercise its U.S. SAFE WEB Act authority, the FTC considers, *inter alia*: "(A) whether the requesting agency has agreed to provide or will provide reciprocal assistance to the Commission; (B) whether compliance with the request would prejudice the public interest of the United States; and (C) whether the requesting agency's investigation or enforcement proceeding concerns acts or practices that cause or are likely to cause injury to a significant number of persons." 15 U.S.C. § 46(j)(3). This authority does not apply to enforcement of competition laws.

Appendix A

Privacy Shield and Safe Harbor Enforcement

	Docket/FTC File No.	Case	Link
1	FTC File No. 2023062 Case No. 3:22-cv-03070 (N.D. Cal.)	US v. Twitter, Inc.	Twitter
2	FTC File No. 192 3209	In the Matter of Residual Pumpkin Entity, LLC, formerly d/b/a CafePress , and PlanetArt, LLC, d/b/a CafePress	CafePress
3	FTC File No. 192 3133 Docket No. C-4747	In the Matter of Flo Health, Inc.	Flo Health
4	FTC File No. 192 3050 Docket No. C-4723	In the Matter of Ortho-Clinical Diagnostics, Inc.	Ortho-Clinical
5	FTC File No. 192 3092 Docket No. C-4709	In the Matter of T&M Protection, LLC	T&M Protection
6	FTC File No. 192 3084 Docket No. C-4704	In the Matter of TDARX, Inc.	TDARX
7	FTC File No. 192 3093 Docket No. C-4706	In the Matter of Global Data Vault, LLC	Global Data
8	FTC File No. 192 3078 Docket No. C-4703	In the Matter of Incentive Services, Inc.	Incentive Services
9	FTC File No. 192 3090 Docket No. C-4705	In the Matter of Click Labs, Inc.	Click Labs
10	FTC File No. 182 3192 Docket No. C-4697	In the Matter of Medable, Inc.	Medable
11	FTC File No. 182 3189 Docket No. 9386	In the Matter of NTT Global Data Centers Americas, Inc., as successor in interest to RagingWire Data Centers, Inc.	RagingWire
12	FTC File No. 182 3196 Docket No. C-4702	In the Matter of Thru, Inc.	Thru
13	FTC File No. 182 3188 Docket No. C-4698	In the Matter of DCR Workforce, Inc.	DCR Workforce
14	FTC File No. 182 3194 Docket No. C-4700	In the Matter of LotaData, Inc.	LotaData
15	FTC File No. 182 3195 Docket No. C-4701	In the Matter of EmpiriStat, Inc.	EmpiriStat

16	FTC File No. 182 3193 Docket No. C-4699	In the Matter of 214 Technologies, Inc., also d/b/a Trueface.ai	Trueface.ai
17	FTC File No. 182 3107 Docket No. 9383	In the Matter of Cambridge Analytica, LLC	Cambridge Analytica
18	FTC File No. 182 3152 Docket No. C-4685	In the Matter of SecureTest, Inc.	SecurTest
19	FTC File No. 182 3144 Docket No. C-4664	In the Matter of VenPath, Inc.	VenPath
20	FTC File No. 182 3154 Docket No. C-4666	In the Matter of SmartStart Employment Screening, Inc.	SmartStart
21	FTC File No. 182 3143 Docket No. C-4663	In the Matter of mResourceLLC , d/b/a Loop Works LLC	mResource
22	FTC File No. 182 3150 Docket No. C-4665	In the Matter of IDmission LLC	IDmission
23	FTC File No. 182 3100 Docket No. C-4659	In the Matter of ReadyTech Corporation	ReadyTech
24	FTC File No. 172 3173 Docket No. C-4630	In the Matter of Decusoft, LLC	Decusoft
25	FTC File No. 172 3171 Docket No. C-4628	In the Matter of Tru Communication, Inc.	Tru
26	FTC File No. 172 3172 Docket No. C-4629	In the Matter of Md7, LLC	Md7
30	FTC File No. 152 3198 Docket No. C-4543	In the Matter of Jhayrmaine Daniels (d/b/a California Skate-Line)	Jhayrmaine Daniels
31	FTC File No. 152 3190 Docket No. C-4545	In the Matter of Dale Jarrett Racing Adventure, Inc.	Dale Jarrett
32	FTC File No. 152 3141 Docket No. C-4540	In the Matter of Golf Connect, LLC	Golf Connect
33	FTC File No. 152 3202 Docket No. C-4546	In the Matter of Inbox Group, LLC	Inbox Group
34	File No. 152 3187 Docket No. C-4542	In the Matter of IOActive, Inc.	IOActive
35	FTC File No. 152 3140 Docket No. C-4549	In the Matter of Jubilant Clinsys, Inc.	Jubilant
36	FTC File No. 152 3199 Docket No. C-4547	In the Matter of Just Bagels Manufacturing, Inc.	Just Bagels

37	FTC File No. 152 3138 Docket No. C-4548	In the Matter of NAICS Association, LLC	NAICS
38	FTC File No. 152 3201 Docket No. C-4544	In the Matter of One Industries Corp.	One Industries
39	FTC File No. 152 3137 Docket No. C-4550	In the Matter of Pinger, Inc.	Pinger
40	FTC File No. 152 3193 Docket No. C-4552	In the Matter of SteriMed Medical Waste Solutions	SteriMed
41	FTC File No. 152 3184 Docket No. C-4541	In the Matter of Contract Logix, LLC	Contract Logix
42	FTC File No. 152 3185 Docket No. C-4551	In the Matter of Forensics Consulting Solutions, LLC	Forensics Consulting
43	FTC File No. 152 3051 Docket No. C-4526	In the Matter of American Int'l Mailing, Inc.	AIM
44	FTC File No. 152 3015 Docket No. C-4525	In the Matter of TES Franchising, LLC	TES
45	FTC File No. 142 3036 Docket No. C-4459	In the Matter of American Apparel, Inc.	American Apparel
46	FTC File No. 142 3026 Docket No. C-4469	In the Matter of Fantage.com, Inc.	Fantage
47	FTC File No. 142 3017 Docket No. C-4461	In the Matter of Apperian, Inc.	Apperian
48	FTC File No. 142 3018 Docket No. C-4462	In the Matter of Atlanta Falcons Football Club, LLC	Atlanta Falcons
49	FTC File No. 142 3019 Docket No. C-4463	In the Matter of Baker Tilly Virchow Krause, LLP	Baker Tilly
50	FTC File No. 142 3020 Docket No. C-4464	In the Matter of BitTorrent, Inc.	BitTorrent
51	FTC File No. 142 3022 Docket No. C-4465	In the Matter of Charles River Laboratories, Int'l	Charles River
52	FTC File No. 142 3023 Docket No. C-4466	In the Matter of DataMotion, Inc.	DataMotion
53	FTC File No. 142 3024 Docket No. C-4467	In the Matter of DDC Laboratories, Inc., d/b/a DNA Diagnostics Center	DDC
54	FTC File No. 142 3028 Docket No. C-4470	In the Matter of Level 3 Communications, LLC	Level 3

55	FTC File No. 142 3025 Docket No. C-4468	In the Matter of PDB Sports, Ltd. , d/b/a the Denver Broncos Football Club, LLP	Broncos
56	FTC File No. 142 3030 Docket No. C-4471	In the Matter of Reynolds Consumer Products, Inc.	Reynolds
57	FTC File No. 142 3031 Docket No. C-4472	In the Matter of Receivable Management Services Corporation	Receivable Mgmt
58	FTC File No. 142 3032 Docket No. C-4473	In the Matter of Tennessee Football, Inc.	Tennessee Football
59	FTC File No. 102 3058 Docket No. C-4369	In the Matter of Myspace LLC	Myspace
60	FTC File No. 092 3184 Docket No. C-4365	In the Matter of Facebook, Inc.	Facebook
61	FTC File No. 092 3081 Civil Action No. 09-CV-5276 (C.D. Cal.)	FTC v. Javian Karnani, and Balls of Kryptonite, LLC , d/b/a Bite Size Deals, LLC, and Best Priced Brands, LLC	Balls of Kryptonite
62	FTC File No. 102 3136 Docket No. C-4336	In the Matter of Google, Inc.	Google
63	FTC File No. 092 3137 Docket No. C-4282	In the Matter of World Innovators, Inc.	World Innovators
64	FTC File No. 092 3141 Docket No. C-4271	In the Matter of Progressive Gaitways LLC	Progressive Gaitways
65	FTC File No. 092 3139 Docket No. C-4270	In the Matter of Onyx Graphics, Inc.	Onyx Graphics
66	FTC File No. 092 3138 Docket No. C-4269	In the Matter of ExpatEdge Partners, LLC	ExpatEdge
67	FTC File No. 092 3140 Docket No. C-4281	In the Matter of Directors Desk LLC	Directors Desk
68	FTC File No. 092 3142 Docket No. C-4272	In the Matter of Collectify LLC	Collectify

ANNEX V



THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

July 6, 2023

Commissioner Didier Reynders
European Commission
Rue de la Loi / Wetstraat 200
1049 1049 Brussels
Belgium

Dear Commissioner Reynders:

The United States Department of Transportation ("Department" or "DOT") appreciates the opportunity to describe its role in enforcing the EU-U.S. Data Privacy Framework ("EU-U.S. DPF") Principles. The EU-U.S. DPF will play a critical role in protecting personal data provided during commercial transactions in an increasingly interconnected world. It will enable businesses to conduct important operations in the global economy, while at the same time ensuring that EU consumers retain important privacy protections.

The DOT first publicly expressed its commitment to enforcement of the U.S.-EU Safe Harbor Framework in a letter sent to the European Commission over 22 years ago, commitments that were repeated and expanded upon in a 2016 letter regarding the EU-U.S. Privacy Shield Framework. The DOT pledged to vigorously enforce the U.S.-EU Safe Harbor Privacy Principles, and then the EU-U.S. Privacy Shield Principles, in those letters. The DOT extends this commitment to the EU-U.S. DPF Principles and this letter memorializes that commitment.

Notably, the DOT confirms its commitment in the following key areas: (1) prioritizing investigation of alleged EU-U.S. DPF Principles violations; (2) appropriate enforcement action against entities making false or deceptive claims of EU-U.S. DPF participation; and (3) monitoring and making public enforcement orders concerning EU-U.S. DPF Principles violations. We provide information about each of these commitments and, for necessary context, pertinent background about the DOT's role in protecting consumer privacy and enforcing the EU-U.S. DPF Principles.

1. Background

A. DOT's Privacy Authority

The Department is strongly committed to ensuring the privacy of information provided by

consumers to airlines and ticket agents. The DOT's authority to take action in this area is found in 49 U.S.C. 41712, which prohibits a carrier or ticket agent from engaging in "an unfair or deceptive practice" in air transportation or the sale of air transportation. Section 41712 is

patterned after Section 5 of the Federal Trade Commission (FTC) Act (15 U.S.C. 45). Recently, DOT issued regulations defining unfair and deceptive practices, consistent with both DOT and FTC precedent (14 CFR § 399.79). Specifically, a practice is "unfair" if it causes or is likely to cause substantial injury, which is not reasonably avoidable, and the harm is not outweighed by

benefits to consumers or competition. A practice is “deceptive” to consumers if it is likely to mislead a consumer, acting reasonably under the circumstances, with respect to a material matter. A matter is material if it is likely to have affected the consumer’s conduct or decision with respect to a product or service. Aside from these general principles, DOT specifically interprets section 41712 as prohibiting carriers and ticket agents from: (1) violating the terms of its privacy policy; (2) violating any rule issued by the Department that identifies specific privacy practices as unfair or deceptive; or (3) violating the Children’s Online Privacy Protection Act (COPPA) or FTC rules implementing COPPA; or (4) failing, as a participant in the EU-U.S. DPF, to comply with the EU-U.S. DPF Principles. ⁽¹⁾

As noted above, under federal law, the DOT has exclusive authority to regulate the privacy practices of airlines, and it shares jurisdiction with the FTC with respect to the privacy practices of ticket agents in the sale of air transportation.

As such, once a carrier or seller of air transportation publicly commits to the EU-U.S. DPF Principles, the Department is able to use the statutory powers of section 41712 to ensure compliance with those principles. Therefore, once a passenger provides information to a carrier or ticket agent that has committed to honoring the EU-U.S. DPF Principles, any failure to do so by the carrier or ticket agent would be a violation of section 41712.

B. Enforcement Practices

The Department’s Office of Aviation Consumer Protection (“OACP”) ⁽²⁾ investigates and prosecutes cases under 49 U.S.C. 41712. It enforces the statutory prohibition in section 41712 against unfair and deceptive practices primarily through negotiation, preparing cease and desist orders, and drafting orders assessing civil penalties. The office learns of potential violations largely from complaints it receives from individuals, travel agents, airlines, and U.S. and foreign government agencies. Consumers may use the DOT’s website to file privacy complaints against airlines and ticket agents. ⁽³⁾

If a reasonable and appropriate settlement in a case is not reached, OACP has the authority to institute an enforcement proceeding involving an evidentiary hearing before a DOT administrative law judge (“ALJ”). The ALJ has the authority to issue cease-and-desist orders and civil penalties. Violations of section 41712 can result in the issuance of cease and desist orders and the imposition of civil penalties of up to \$ 37 377 for each violation of section 41712.

The Department does not have the authority to award damages or provide pecuniary relief to individual complainants. However, the Department does have the authority to approve settlements resulting from investigations brought by its OACP that directly benefit consumers (e.g., cash, vouchers) as an offset to monetary penalties otherwise payable to the U.S. Government. This has occurred in the past, and may also occur in the context of the EU-U.S. DPF Principles when circumstances warrant. Repeated violations of section 41712 by an airline would also raise questions regarding the airline’s compliance disposition which could, in egregious situations, result in an airline being found to be no longer fit to operate and, therefore, losing its economic operating authority.

To date, the DOT has received relatively few complaints involving alleged privacy violations by ticket agents or airlines. When they arise, they are investigated according to the principles set forth above.

C. DOT Legal Protections Benefiting EU Consumers

Under section 41712, the prohibition on unfair or deceptive practices in air transportation or the sale of air transportation applies to U.S. and foreign air carriers as well as ticket agents. The DOT frequently takes action against U.S. and foreign airlines for practices that affect both foreign and U.S. consumers on the basis that the airline’s practices took place in the course of providing transportation to or from the United States. The DOT does and will continue to use all remedies that are available to protect both foreign and U.S. consumers from unfair or deceptive practices in air transportation by regulated entities.

⁽¹⁾ <https://www.transportation.gov/individuals/aviation-consumer-protection/privacy>.

⁽²⁾ Formerly known as the Office of Aviation Enforcement and Proceedings.

⁽³⁾ <http://www.transportation.gov/airconsumer/privacy-complaints>.

The DOT also enforces, with respect to airlines, other targeted laws whose protections extend to non-U.S. consumers such as the Children's Online Privacy Act ("COPPA"). Among other things, COPPA requires that operators of child-directed websites and online services, or general audience sites that knowingly collect personal information from children under 13 provide parental notice and obtain verifiable parental consent. U.S.-based websites and services that are subject to COPPA and collect personal information from foreign children are required to comply with COPPA. Foreign-based websites and online services must also comply with COPPA if they are directed to children in the United States, or if they knowingly collect personal information from children in the United States. To the extent that U.S. or foreign airlines doing business in the United States violate COPPA, the DOT would have jurisdiction to take enforcement action.

II. EU-U.S. DPF Principles Enforcement

If an airline or ticket agent chooses to participate in the EU-U.S. DPF and the Department receives a complaint that such an airline or ticket agent had allegedly violated the EU-U.S. DPF Principles, the Department would take the following steps to vigorously enforce the EU-U.S. DPF Principles.

A. Prioritizing Investigation of Alleged Violations

The Department's OACP will investigate each complaint alleging EU-U.S. DPF Principles

violations, including complaints received from EU data protection authorities ("DPAs") and take enforcement action where there is evidence of a violation. Further, OACP will cooperate with the FTC and Department of Commerce and place a priority on allegations that the regulated entities are not complying with privacy commitments made as part of the EU-U.S. DPF.

Upon receipt of an allegation of a violation of the EU-U.S. DPF Principles, OACP may take a range of actions as part of its investigation. For example, it may review the ticket agent or airline's privacy policies, obtain further information from the ticket agent or airline or from third parties, follow up with the referring entity, and assess whether there is a pattern of violations or significant number of consumers affected. In addition, it would determine whether the issue implicates matters within the purview of the Department of Commerce or FTC, assess whether consumer education and business education would be helpful, and as appropriate, initiate an enforcement proceeding.

If the Department becomes aware of potential EU-U.S. DPF Principles violations by ticket agents, it will coordinate with the FTC on the matter. We will also advise the FTC and the Department of Commerce of the outcome of any EU-U.S. DPF Principles enforcement action.

B. Addressing False or Deceptive Participation Claims

The Department remains committed to investigating EU-U.S. DPF Principles violations, including false or deceptive claims of participation in the EU-U.S. DPF. We will give priority consideration to referrals from the Department of Commerce regarding organizations that it identifies as improperly holding themselves out to be EU-U.S. DPF participants or using the EU-U.S. DPF certification mark without authorization.

In addition, we note that if an organization's privacy policy promises that it complies with the EU-U.S. DPF Principles, its failure to make or maintain a self-certification through the Department of Commerce likely will not, by itself, excuse the organization from DOT enforcement of those commitments.

C. Monitoring and Making Public Enforcement Orders Concerning EU-U.S. DPF Violations

The Department's OACP also remains committed to monitoring enforcement orders as needed to ensure compliance with the EU-U.S. DPF Principles. Specifically, if the office issues an order directing an airline or ticket agent to cease and desist from future violations of the EU-U.S. DPF Principles and section 41712, it will monitor the entity's compliance with the cease-and-desist provision in the order. In addition, the office will ensure that orders resulting from EU-U.S. DPF Principles cases are available on its website.

We look forward to our continued work with our federal partners and EU stakeholders on EU-U.S. DPF matters.

I hope that this information proves helpful. If you have any questions or need further information, please feel free to contact me.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Pete Buttigieg', with a stylized, cursive script.

Pete BUTTIGIEG

ANNEX VI



U.S. Department of Justice

Criminal Division

Office of Assistant Attorney General

Washington, D.C. 20530

June 23, 2023

Ms. Ana Gallego Torres
Director-General for Justice and Consumers
European Commission
Rue Montoyer/Montoyerstraat 59
1049 Brussels
Belgium

Dear Ms. Director-General Gallego Torres:

This letter provides a brief overview of the primary investigative tools used to obtain commercial data and other record information from corporations in the United States for criminal law enforcement or public interest (civil and regulatory) purposes, including the access limitations set forth in those authorities. ⁽¹⁾ All the legal processes described in this letter are nondiscriminatory in that they are used to obtain information from corporations in the United States, including from companies that will self-certify through the EU-U.S. Data Privacy Framework, without regard to the nationality or place of residence of the data subject. Further, corporations that receive legal process in the United States may challenge it in court as discussed below. ⁽²⁾

Of particular note with respect to the seizure of data by public authorities is the Fourth Amendment to the United States Constitution, which provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. As the United States Supreme Court stated in *Berger v. State of New York*, "[t]he basic purpose of this Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." 388 U.S. 41, 53 (1967) (citing *Camara v. Mun. Court of San Francisco*, 387 U.S. 523, 528 (1967)). In domestic criminal investigations, the Fourth Amendment generally requires law enforcement officers to obtain a court-issued warrant before conducting a search. See *Katz v. United States*, 389 U.S. 347, 357 (1967). Standards for the issuance of a warrant, such as the probable cause and particularity requirements, apply to warrants for physical searches and seizures as well as to warrants for the stored content of electronic communications

⁽¹⁾ This overview does not describe the national security investigative tools used by law enforcement in terrorism and other national security investigations, including National Security Letters (NSLs) for certain record information in credit reports, financial records, and electronic subscriber and transaction records, 12 U.S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, 50 U.S.C. § 3162, and for electronic surveillance, search warrants, business records, and other collection of information pursuant to the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 et seq.

⁽²⁾ This letter discusses federal law enforcement and regulatory authorities. Violations of state law are investigated by state law enforcement authorities and are tried in state courts. State law enforcement authorities use warrants and subpoenas issued under state law in essentially the same manner as described herein, but with the possibility that state legal process may be subject to additional protections provided by state constitutions or statutes that exceed those of the U.S. Constitution. State law protections must be at least equal to those of the U.S. Constitution, including but not limited to the Fourth Amendment.

issued under the Stored Communications Act as discussed below. When the warrant requirement does not apply, government activity is still subject to a "reasonableness" test under the Fourth Amendment. The Constitution itself, therefore, ensures that the U.S. government does not have limitless, or arbitrary, power to seize private information. ⁽³⁾

Criminal Law Enforcement Authorities:

Federal prosecutors, who are officials of the Department of Justice (DOJ), and federal investigative agents including agents of the Federal Bureau of Investigation (FBI), a law enforcement agency within DOJ, are able to compel production of documents and other record information from corporations in the United States for criminal investigative purposes through several types of compulsory legal processes, including grand jury subpoenas, administrative subpoenas, and search warrants, and may acquire other communications pursuant to federal criminal wiretap and pen register authorities.

Grand Jury or Trial Subpoenas: Criminal subpoenas are used to support targeted law enforcement investigations. A grand jury subpoena is an official request issued from a grand jury (usually at the request of a federal prosecutor) to support a grand jury investigation into a particular suspected violation of criminal law. Grand juries are an investigative arm of the court and are empaneled by a judge or magistrate. A subpoena may require someone to testify at a proceeding, or to produce or make available business records, electronically stored information, or other tangible items. The information must be relevant to the investigation and the subpoena cannot be unreasonable because it is overbroad, or because it is oppressive or burdensome. A recipient can file a motion to challenge a subpoena based on those grounds. See Fed. R. Crim. P. 17. In limited circumstances, trial subpoenas for documents may be used after the case has been indicted by the grand jury.

Administrative Subpoena Authority: Administrative subpoena authorities may be exercised in criminal or civil investigations. In the criminal law enforcement context, several federal statutes authorize the use of administrative subpoenas to produce or make available business records, electronically stored information, or other tangible items relevant to investigations involving health care fraud, child abuse, Secret Service protection, controlled substance cases, and Inspector General investigations implicating government agencies. If the government seeks to enforce an administrative subpoena in court, the recipient of the administrative subpoena, like the recipient of a grand jury subpoena, can argue that the subpoena is unreasonable because it is overbroad, or because it is oppressive or burdensome.

Court Orders For Pen Register and Trap and Traces: Under criminal pen register and trap-and-trace provisions, law enforcement may obtain a court order to acquire real-time, non-content dialing, routing, addressing, and signaling information about a phone number or email upon certification that the information provided is relevant to a pending criminal investigation. See 18 U.S.C. §§ 3121-3127. The use or installation of such a device outside the law is a federal crime.

Electronic Communications Privacy Act (ECPA): Additional rules govern the government's access to subscriber information, traffic data, and stored content of communications held by internet service providers (also known as "ISPs"), telephone companies, and other third-party service providers, pursuant to Title II of ECPA, also called the Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2712. The SCA sets forth a system of statutory privacy rights that limit law enforcement access to data beyond what is required under Constitutional law from customers and subscribers of ISPs. The SCA provides for increasing levels of privacy protections depending on the intrusiveness of the collection. For subscriber registration information, Internet Protocol (IP) addresses and associated time stamps, filed billing information, criminal law enforcement authorities must obtain a subpoena. For most other stored, non-content information, such as

⁽³⁾ With respect to the Fourth Amendment principles on safeguarding privacy and security interests that are discussed above, U.S. courts regularly apply those principles to new types of law enforcement investigative tools that are enabled by developments in technology. For example, in 2018 the Supreme Court ruled that the government's acquisition in a law enforcement investigation of historical cell-site location information from a cell phone company for an extended period of time is a "search" subject to the Fourth Amendment warrant requirement. *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

email holders without the subject line, law enforcement must present specific facts to a judge demonstrating that the requested information is relevant and material to an ongoing criminal investigation. To obtain the stored content of electronic communications, generally, criminal law enforcement authorities must obtain a warrant from a judge based on probable cause to believe the account in question contains evidence of a crime. The SCA also provides for civil liability and criminal penalties. ⁽⁴⁾

Court Orders for Surveillance Pursuant to Federal Wiretap Law: Additionally, law enforcement may intercept in real time wire, oral, or electronic communications for criminal investigative purposes pursuant to the federal wiretap law. See 18 U.S.C. §§ 2510-2523. This authority is available only pursuant to a court order in which a judge finds, inter alia, that there is probable cause to believe that the wiretap or electronic interception will produce evidence of a federal crime, or the whereabouts of a fugitive fleeing from prosecution. The statute provides for civil liability and criminal penalties for violations of the wiretapping provisions.

Search Warrant-Fed. R. Crim. P. Rule 41: Law enforcement can physically search premises in the United States when authorized to do so by a judge. Law enforcement must demonstrate to the judge based on a showing of probable cause that a crime was committed or is about to be committed and that items connected to the crime are likely to be found in the place specified by the warrant. This authority is often used when a physical search by police of a premise is needed due to the danger that evidence may be destroyed if a subpoena or other production order is served on the corporation. A person subject to a search or whose property is subject to a search may move to suppress evidence obtained or derived from an unlawful search if that evidence is introduced against that person during a criminal trial. See *Mapp v. Ohio*, 367 U.S. 643 (1961). When a data holder is required to disclose data pursuant to a warrant, the compelled party may challenge the requirement to disclose as unduly burdensome. See *In re Application of United States*, 610 F.2d 1148, 1157 (3d Cir. 1979) (holding that "due process requires a hearing on the issue of burdensomeness before compelling a telephone company to provide" assistance with a search warrant); *In re Application of United States*, 616 F.2d 1122 (9th Cir. 1980) (reaching same conclusion based on court's supervisory authority).

DOJ Guidelines and Policies: In addition to these Constitutional, statutory, and rule-based limitations on government access to data, the Attorney General has issued guidelines that place further limits on law enforcement access to data, and that also contain privacy and civil liberties protections. For instance, the Attorney General's Guidelines for Domestic FBI Operations (September 2008) (hereinafter AG FBI Guidelines), available at <http://www.justice.gov/archive/opa/docs/guidelines.pdf>, set limits on use of investigative means to seek information related to investigations that involve federal crimes. These guidelines require that the FBI use the least intrusive investigative methods feasible, taking into account the effect on privacy and civil liberties and the potential damage to reputation. Further, they note that "it is axiomatic that the FBI must conduct its investigations and other activities in a lawful and reasonable manner that respects liberty and privacy and avoids unnecessary intrusions into the lives of law-abiding people." AG FBI Guidelines at 5. The FBI has implemented these guidelines through the FBI Domestic Investigations and Operations Guide (DIOG), available at <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29>, a comprehensive manual that includes detailed limits on use of investigative tools and guidance to assure that civil liberties and privacy are protected in every investigation. Additional rules and policies that prescribe limitations on the investigative activities of federal prosecutors are set out in the Justice Manual, also available online at <https://www.justice.gov/jm/justicemanual>.

Civil and Regulatory Authorities (Public Interest):

⁽⁴⁾ In addition, section 2705(b) of the SCA authorizes the government to obtain a court order, based on a demonstrated need for protection from disclosure, prohibiting a communications services provider from voluntarily notifying its users of the receipt of SCA legal process. In October 2017, Deputy Attorney General Rod Rosenstein issued a memorandum to DOJ attorneys and agents setting out guidance to ensure that applications for such protective orders are tailored to the specific facts and concerns of an investigation and establishing a general one-year ceiling on how long an application may seek to delay notice. In May 2022, Deputy Attorney General Lisa Monaco issued supplementary guidance on the topic, which among other matters established internal DOJ approval requirements for applications to extend a protective order beyond the initial one-year period and required the termination of protective orders at the close of an investigation.

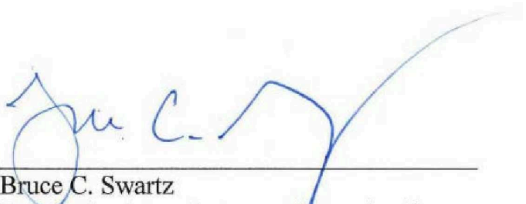
There are also significant limits on civil or regulatory (i.e., "public interest") access to data held by corporations in the United States. Agencies with civil and regulatory responsibilities may issue subpoenas to corporations for business records, electronically stored information, or other tangible items. These agencies are limited in their exercise of administrative or civil subpoena authority not only by their organic statutes, but also by independent judicial review of subpoenas prior to potential judicial enforcement. See, e.g., Fed. R. Civ. P. 45. Agencies may seek access only to data that is relevant to matters within their scope of authority to regulate. Further, a recipient of an administrative subpoena may challenge the enforcement of that subpoena in court by presenting evidence that the agency has not acted in accordance with basic standards of reasonableness, as discussed earlier.

There are other legal bases for companies to challenge data requests from administrative agencies based on their specific industries and the types of data they possess. For example, financial institutions can challenge administrative subpoenas seeking certain types of information as violations of the Bank Secrecy Act and its implementing regulations. 31 U.S.C. § 5318; 31 C.F.R. Chapter X. Other businesses can rely on the Fair Credit Reporting Act, 15 U.S.C. § 1681b, or a host of other sector specific laws. Misuse of an agency's subpoena authority can result in agency liability, or personal liability for agency officers. See, e.g., Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3423. Courts in the United States thus stand as the guardians against improper regulatory requests and provide independent oversight of federal agency actions.

Finally, any statutory power that administrative authorities have to physically seize records from a company in the United States pursuant to an administrative search must meet requirements based on the Fourth Amendment. See *See v. City of Seattle*, 387 U.S. 541 (1967).

Conclusion:

All law enforcement and regulatory activities in the United States must conform to applicable law, including the U.S. Constitution, statutes, rules, and regulations. Such activities must also comply with applicable policies, including any Attorney General Guidelines governing federal law enforcement activities. The legal framework described above limits the ability of U.S. law enforcement and regulatory agencies to acquire information from corporations in the United States-whether the information concerns U.S. persons or citizens of foreign countries-and in addition permits judicial review of any government requests for data pursuant to these authorities.



Bruce C. Swartz
Deputy Assistant Attorney General and
Counselor for International Affairs

ANNEX VII

**OFFICE OF THE DIRECTOR OF NATIONAL
INTELLIGENCE OFFICE OF GENERAL
COUNSEL****WASHINGTON, DC 20511**

December 9, 2022

Leslie B. Kiernan
General Counsel
U.S. Department of
Commerce 1401 Constitution
Ave., NW Washington, DC 20230

Dear Ms. Kiernan,

On October 7, 2022, President Biden signed Executive Order 14086, *Enhancing Safeguards for United States Signals Intelligence Activities*, which bolsters the rigorous array of privacy and civil liberties safeguards that apply to U.S. signals intelligence activities. These safeguards include: requiring signals intelligence activities to meet enumerated legitimate objectives; explicitly barring such activities for the purpose of specific prohibited objectives; putting in place novel procedures for ensuring that signals intelligence activities further these legitimate objectives and do not further prohibited objectives; requiring that signals intelligence activities be conducted only following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority and only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized; and directing Intelligence Community (IC) elements to update their policies and procedures to reflect the Executive Order's required signals intelligence safeguards. Most significantly, the Executive Order also introduces an independent and binding mechanism enabling individuals from "qualifying states," as designated pursuant to the Executive Order, to seek redress if they believe they were subjected to unlawful U.S. signals intelligence activities, including activities violating the protections found in the Executive Order.

President Biden's issuance of Executive Order 14086 marked the culmination of well over a year of detailed negotiations between representatives from the European Commission (EC) and the United States and directs the steps the United States will take to implement its commitments under the EU-U.S. Data Privacy Framework. Consistent with the cooperative spirit that produced the Framework, it is my understanding that you have received two sets of questions from the EC about how the IC will implement the Executive Order. I am happy to address these questions with this letter.

Section 702 of the Foreign Intelligence Surveillance Act of 1978 (FISA Section 702)

The first set of questions concerns FISA Section 702, which allows the collection of foreign intelligence information through the targeting of non-U.S. persons reasonably believed to be located outside the United States with the compelled assistance of electronic communication service providers. Specifically, the questions concern the interplay between that provision and Executive Order 14086, as well as the other safeguards that apply to activities conducted pursuant to FISA Section 702.

To begin, we can confirm that the IC will apply the safeguards set forth in Executive Order 14086 to activities conducted pursuant to FISA Section 702.

In addition, numerous other safeguards apply to the Government's use of FISA Section 702. For example, all FISA Section 702 certifications must be signed by both the Attorney General and Director of National Intelligence (DNI), and the Government must submit all such certifications for approval by the Foreign Intelligence Surveillance Court (FISC), which is comprised of independent, life-tenured judges who serve non-renewable seven-year terms. The certifications identify categories of foreign intelligence information to be collected, which must meet the statutory definition of foreign intelligence information, through the targeting of non-U.S. persons reasonably believed to be located outside the United States. The certifications have included information concerning international terrorism and other topics, such as the acquisition of information concerning weapons of mass destruction. Each annual certification must be submitted to the FISC for approval in a certification application package that includes the Attorney General's and DNI's certifications, affidavits by certain heads of intelligence agencies, and targeting procedures, minimization procedures, and querying procedures that are binding on the Government. The targeting procedures require, among other things, that the IC reasonably assess, based on the totality of the circumstances, that the targeting will likely lead to the collection of foreign intelligence information identified in a FISA Section 702 certification.

Moreover, when collecting information pursuant to FISA Section 702, the IC must: provide a written explanation of the basis for their assessment, at the time of targeting, that the target is expected to possess, is expected to receive, or is likely to communicate foreign intelligence information identified in a FISA Section 702 certification; confirm that the targeting standard as set forth in FISA Section 702 targeting procedures remains satisfied; and cease collection if the standard is no longer satisfied. *See U.S. Government Submission to Foreign Intelligence Surveillance Court, 2015 Summary of Notable Section 702 Requirements*, at 2-3 (July 15, 2015).

Requiring the IC to record in writing, and regularly affirm the validity of, its assessment that FISA Section 702 targets meet the applicable targeting standards facilitates the FISC's supervision of the IC's targeting activities. Each recorded targeting assessment and rationale is reviewed on a bimonthly basis by intelligence oversight attorneys in the Department of Justice (DOJ), who conduct this oversight function independently from foreign intelligence operations. The DOJ section performing this function is then responsible under a long-established FISC rule to report to the FISC any violations of the applicable procedures. This reporting, along with regular meetings between the FISC and this DOJ section regarding oversight of FISA Section 702 targeting, enables the FISC to enforce compliance with the FISA Section 702 targeting and other procedures and otherwise ensure that the Government's activities are lawful. In particular, the FISC can do this in a number of ways, including by issuing binding remedial decisions to terminate the Government's authority to collect against a particular target, or to modify or delay FISA Section 702 data collection. The FISC also can require the Government to provide further reporting or briefing on its compliance with targeting and other procedures or require changes to those procedures.

The "Bulk" Collection of Signals Intelligence

The second set of questions concerns the "bulk" collection of signals intelligence, which is defined by Executive Order 14086 as "the authorized collection of large quantities of signals intelligence data that, due to technical or operational considerations, is acquired without the use of discriminants (for example, without the use of specific identifiers or selection terms)."

With respect to these questions, we first note that neither FISA nor National Security Letters authorize bulk collection. With respect to FISA:

- Titles I and III of FISA, which respectively authorize electronic surveillance and physical searches, require a court order (with limited exceptions, such as emergency circumstances) and always require probable cause to believe that the target is a foreign power or an agent of a foreign power. *See* 50 U.S.C. §§ 1805, 1824.
- The USA FREEDOM Act of 2015 amended Title IV of FISA, which authorizes the use of pen registers and trap and trace devices, pursuant to court order (except in emergency circumstances), to require the Government to base requests on a "specific selection term." *See* 50 U.S.C. § 1842(c)(3).

- Title V of FISA, which permits the Federal Bureau of Investigation (FBI) to obtain certain types of business records, requires a court order based on an application that specifies that “there are specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power.” See 50 U.S.C. § 1862(b)(2)(B). ⁽¹⁾
- Finally, FISA Section 702 authorizes the “targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.” See 50 U.S.C. § 1881a(a). Thus, as the Privacy and Civil Liberties Oversight Board has noted, the Government’s collection of data under FISA Section 702 “consists entirely of targeting individual persons and acquiring communications associated with those persons, from whom the government has reason to expect it will obtain certain types of foreign intelligence,” such that the “program does not operate by collecting communications in bulk.” Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, at 103 (July 2, 2014). ⁽²⁾

With respect to National Security Letters, the USA FREEDOM Act of 2015 imposes a “specific selection term” requirement on the use of such letters. See 12 U.S.C. § 3414(a)(2); 15 U.S.C. § 1681u; 15 U.S.C. § 1681v(a); 18 U.S.C. § 2709(b).

Further, Executive Order 14086 provides that “[t]argeted collection shall be prioritized” and that, when the IC does conduct bulk collection, the “bulk collection of signals intelligence shall be authorized only based on a determination ... that the information necessary to advance a validated intelligence priority cannot reasonably be obtained by targeted collection.” See Executive Order 14086, § 2(c)(ii)(A).

Moreover, when the IC determines that bulk collection satisfies these standards, Executive Order 14086 provides additional safeguards. Specifically, the Executive Order requires the IC, when conducting bulk collection, to “apply reasonable methods and technical measures in order to limit the data collected to only what is necessary to advance a validated intelligence priority, while minimizing the collection of non-pertinent information.” See *id.* The Order also states that “signals intelligence activities,” which include the querying of signals intelligence obtained by bulk collection, “shall be conducted only following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority.” See *id.* § 2(a)(ii)(A). The Order further implements this principle by stating that the IC may only query unminimized signals intelligence obtained in bulk in pursuit of six permissible objectives, and that such queries must be conducted according to policies and procedures that “appropriately take into account the impact [of the queries] on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.” See *id.* § 2(c)(iii)(D). Lastly, the Order provides for handling, security, and access controls for data collected. See *id.* § 2(c)(iii)(A) and § 2(c)(iii)(B).

We hope these clarifications are of assistance. Please do not hesitate to contact us if you have further questions about how the U.S. IC plans to implement Executive Order 14086.

⁽¹⁾ From 2001 until 2020, Title V of FISA permitted the FBI to seek authorization from the FISC to obtain “tangible things” that are relevant to certain authorized investigations. See USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, § 215 (2001). This language, which has sunset and is thus no longer the law, provided the authority pursuant to which the Government at one time collected telephony metadata in bulk. Even before the provision sunset, however, the USA FREEDOM Act had amended it to require the Government to base an application to the FISC on a “specific selection term.” See USA FREEDOM Act, Pub. L. No. 114-23, 129 Stat. 268, § 103 (2015).

⁽²⁾ Sections 703 and 704, which authorize the IC to target U.S. persons located overseas, require a court order (except in emergency circumstances) and always require probable cause to believe that the target is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power. See 50 U.S.C. §§ 1881b, 1881c.

Sincerely,

A handwritten signature in black ink, appearing to read 'C. FONZONE', followed by a horizontal line extending to the right and ending in a vertical line.

Christopher C. FONZONE
General Counsel

ANNEX VIII

List of abbreviations

The following abbreviations appear in this Decision:

AAA	American Arbitration Association
AG Regulation	Attorney General Regulation on the Data Protection Review Court
AGG-DOM	Attorney General Guidelines for Domestic FBI Operations
APA	Administrative Procedure Act
CIA	Central Intelligence Agency
CNSS	Committee on National Security Systems
Court of Justice	Court of Justice of the European Union
Decision	Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DoC	U.S. Department of Commerce
DoJ	U.S. Department of Justice
DoT	U.S. Department of Transportation
DPA	Data Protection Authority
DPF List	Data Privacy Framework List
DPRC	Data Protection Review Court
ECOA	Equal Credit Opportunity Act
ECPA	Electronic Communications Privacy Act
EEA	European Economic Area
EO 12333	Executive Order 12333 'United States Intelligence Activities'
EO 14086, the EO	Executive Order 14086 'Enhancing Safeguards for US Signals Intelligence Activities'
EU-U.S. DPF or DPF	EU-U.S. Data Privacy Framework
EU-U.S. DPF Panel	EU-U.S. Data Privacy Framework Panel
FBI	Federal Bureau of Investigation
FCRA	Fair Credit Reporting Act
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FISCR	Foreign Intelligence Surveillance Court of Review
FOIA	Freedom of Information Act
FRA	Federal Records Act

FTC	U.S. Federal Trade Commission
HIPAA	Health Insurance Portability and Accountability Act
ICDR	International Centre for Dispute Resolution
IOB	Intelligence Oversight Board
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSL	National Security Letter(s)
ODNI	Office of the Director of National Intelligence
ODNI CLPO, CLPO	Civil Liberties Protection Officer of the Director of National Intelligence
OMB	Office of Management and Budget
OPCL	Office of Privacy and Civil Liberties of the Department of Justice
PCLOB	Privacy and Civil Liberties Oversight Board
PIAB	President's Intelligence Advisory Board
PPD 28	Presidential Policy Directive 28
Regulation (EU) 2016/679	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
SAOP	Senior Agency Official for Privacy
The Principles	EU-U.S. Data Privacy Framework Principles
U.S.	United States
Union	European Union

ISSN 1977-0677 (electronic edition)
ISSN 1725-2555 (paper edition)



Publications Office
of the European Union
L-2985 Luxembourg
LUXEMBOURG

EN