

Official Journal of the European Union

L 313



English edition

Legislation

Volume 61

10 December 2018

Contents

II *Non-legislative acts*

INTERNATIONAL AGREEMENTS

- ★ **Notice concerning the provisional application of the Framework Agreement between the European Union and its Member States, of the one part, and Australia, of the other part** 1

REGULATIONS

- ★ **Commission Regulation (EU) 2018/1923 of 7 December 2018 amending Regulation (EU) No 360/2012 as regards its period of application ⁽¹⁾** 2
- ★ **Commission Implementing Regulation (EU) 2018/1924 of 7 December 2018 on cancelling the registration of protected geographical indication ‘Mostviertler Birnmost’ (PGI)** 4

DECISIONS

- ★ **Council Decision (EU) 2018/1925 of 18 September 2018 on the position to be taken on behalf of the European Union position within the Association Council set up by the Euro-Mediterranean Agreement establishing an association between the European Community and its Member States, of the one part, and the Republic of Tunisia, of the other part, with regard to the adoption of the EU-Tunisia strategic priorities for the period 2018-2020** 5
- ★ **Council Decision (EU) 2018/1926 of 19 November 2018 on the position to be taken, on behalf of the European Union, in the Group of Experts on the European Agreement concerning the work of crews of vehicles engaged in international road transport of the United Nations Economic Commission for Europe** 13

⁽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.

★ Commission Decision (EU) 2018/1927 of 5 December 2018 laying down internal rules concerning the processing of personal data by the European Commission in the field of competition in relation to the provision of information to data subjects and the restriction of certain rights	39
★ Commission Implementing Decision (EU) 2018/1928 of 6 December 2018 granting a derogation requested by Denmark pursuant to Council Directive 91/676/EEC concerning the protection of waters against pollution caused by nitrates from agricultural sources (notified under document C(2018) 8081)	45

II

(Non-legislative acts)

INTERNATIONAL AGREEMENTS

Notice concerning the provisional application of the Framework Agreement between the European Union and its Member States, of the one part, and Australia, of the other part

The European Union and Australia have notified each other of the completion of the procedures necessary for the provisional application of the Framework Agreement between the European Union and its Member States, of the one part, and Australia, of the other part ⁽¹⁾, on 4 September 2018. Consequently, Australia and the Union may provisionally apply mutually determined provisions of the Agreement in accordance with Article 61(2) of that Agreement as from 4 October 2018.

By virtue of Article 2 of Council Decision (EU) 2017/1546 of 29 September 2016 on the signing, on behalf of the European Union, and provisional application of the Framework Agreement, the following provisions shall be applied provisionally between the Union and Australia, but only to the extent that they cover matters falling within the Union's competence, including matters falling within the Union's competence to define and implement a common foreign and security policy:

- Article 3 (Political Dialogue),
- Article 10 (Cooperation in regional and international organisations),
- Article 56 (Joint Committee), with the exception of points (g) and (h) of paragraph 3 thereof,
- Title X (Final Provisions), with the exception of Article 61(1) and (3), to the extent necessary for the purpose of ensuring the provisional application of the provisions of the Agreement referred to in the first three indents.

⁽¹⁾ OJ L 237, 15.9.2017, p. 7.

REGULATIONS

COMMISSION REGULATION (EU) 2018/1923

of 7 December 2018

amending Regulation (EU) No 360/2012 as regards its period of application

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

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

Having regard to Council Regulation (EU) 2015/1588 of 13 July 2015 on the application of Articles 107 and 108 of the Treaty on the Functioning of the European Union to certain categories of horizontal State aid ⁽¹⁾, and in particular Article 2(1) thereof,

After consulting the Advisory Committee on State Aid,

Whereas:

- (1) Under Commission Regulation (EU) No 360/2012 ⁽²⁾, aid below a certain threshold granted to undertakings for the provision of a service of general economic interest is deemed not to meet all the criteria of Article 107(1) of the Treaty and is therefore exempt from the notification requirement of Article 108(3) of the Treaty, subject to certain conditions.
- (2) Regulation (EU) No 360/2012 will expire on 31 December 2018.
- (3) On the basis of the Commission's experience in applying Regulation (EU) No 360/2012, it appears that the justifications for the exemption of such compensation measures from the notification requirement are still valid and that the conditions on the basis of which the scope and content of Regulation (EU) No 360/2012 were determined have not substantially changed. The Regulation provides legal certainty and reduces the administrative burden in respect of *de minimis* aid measures granted to undertakings providing services of general economic interest. In order to provide continuity and avoid increasing compliance costs for the services concerned changes should thus be avoided at this stage.
- (4) The period of application of Regulation (EU) No 360/2012 should therefore be extended by two years.
- (5) Regulation (EU) No 360/2012 should therefore be amended accordingly,

HAS ADOPTED THIS REGULATION:

Article 1

In Article 5 of Regulation (EU) No 360/2012 '31 December 2018' is replaced by '31 December 2020'.

Article 2

This Regulation shall enter into force on 31 December 2018.

⁽¹⁾ OJ L 248, 24.9.2015, p. 1.

⁽²⁾ Commission Regulation (EU) No 360/2012 of 25 April 2012 on the application of Articles 107 and 108 of the Treaty on the Functioning of the European Union to *de minimis* aid granted to undertakings providing services of general economic interest (OJ L 114, 26.4.2012, p. 8).

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

Done at Brussels, 7 December 2018.

For the Commission

The President

Jean-Claude JUNKER

COMMISSION IMPLEMENTING REGULATION (EU) 2018/1924
of 7 December 2018
on cancelling the registration of protected geographical indication ‘Mostviertler Birnmost’ (PGI)

THE EUROPEAN COMMISSION,

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

Having regard to Regulation (EU) No 1151/2012 of the European Parliament and of the Council of 21 November 2012 on quality schemes for agricultural products and foodstuffs ⁽¹⁾, and in particular Article 54(1) thereof,

Whereas:

- (1) Article 7(1) of Commission Delegated Regulation (EU) No 664/2014 ⁽²⁾ provides that the procedure laid down in Articles 49 to 52 of Regulation (EU) No 1151/2012 apply *mutatis mutandis* to the cancellation of a registration as referred to in Article 54(1) of that Regulation.
- (2) Pursuant to Article 50(2) of Regulation (EU) No 1151/2012 in connection with Article 7(1) of Delegated Regulation (EU) No 664/2014, the application to cancel the registration of the protected geographical indication (PGI) ‘Mostviertler Birnmost’ was published in the *Official Journal of the European Union* ⁽³⁾.
- (3) As no statement of opposition under Article 51 of Regulation (EU) No 1151/2012 has been received by the Commission, the name ‘Mostviertler Birnmost’ (PGI) should therefore be cancelled from the register of protected designations of origin and protected geographical indications.
- (4) Pursuant to the last subparagraph of Article 54(1) of Regulation (EU) No 1151/2012 such cancellations are adopted in accordance with the examination procedure referred to in Article 57(2) of that Regulation.
- (5) The measure provided for in this Regulation is in accordance with the opinion of the Agricultural Product Quality Policy Committee,

HAS ADOPTED THIS REGULATION:

Article 1

The registration of the name ‘Mostviertler Birnmost’ (PGI) is hereby cancelled.

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, 7 December 2018.

For the Commission

The President

Jean-Claude JUNCKER

⁽¹⁾ OJ L 343, 14.12.2012, p. 1.

⁽²⁾ Commission Delegated Regulation (EU) No 664/2014 of 18 December 2013 supplementing Regulation (EU) No 1151/2012 of the European Parliament and of the Council with regard to the establishment of the Union symbols for protected designations of origin, protected geographical indications and traditional specialities guaranteed and with regard to certain rules on sourcing, certain procedural rules and certain additional transitional rules (OJ L 179, 19.6.2014, p. 17).

⁽³⁾ OJ C 62, 17.2.2018, p. 15.

DECISIONS

COUNCIL DECISION (EU) 2018/1925

of 18 September 2018

on the position to be taken on behalf of the European Union position within the Association Council set up by the Euro-Mediterranean Agreement establishing an association between the European Community and its Member States, of the one part, and the Republic of Tunisia, of the other part, with regard to the adoption of the EU-Tunisia strategic priorities for the period 2018-2020

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 217, in conjunction with Article 218(9) thereof,

Having regard to the joint proposal from the High Representative of the Union for Foreign Affairs and Security Policy and the European Commission,

Whereas:

- (1) The Euro-Mediterranean Agreement establishing an association between the European Communities and their Member States, of the one part, and the Republic of Tunisia, of the other part ⁽¹⁾ (hereinafter referred to as the 'Euro-Mediterranean Agreement') was signed on 17 July 1995 and entered into force on 1 March 1998.
- (2) Article 80 of the Euro-Mediterranean Agreement gives the Association Council, established under the Euro-Mediterranean Agreement, the power to take decisions it considers appropriate for the purpose of attaining the objectives of the Agreement.
- (3) In accordance with Article 90 of the Euro-Mediterranean Agreement, the parties are to take any general or specific measures required to fulfil their obligations under the Euro-Mediterranean Agreement and are to see to it that the objectives set out therein are attained.
- (4) The Joint Communication from the High Representative of the Union for Foreign Affairs and Security Policy and from the European Commission of 18 November 2015 on the Review of the European Neighbourhood Policy was welcomed in the Council Conclusions of 14 December 2015. The Council confirmed in particular its intention to start a new phase of engagement with its partners in 2016 which could lead to the setting of new partnership priorities, where appropriate, focused on agreed priorities and interests.
- (5) The Joint Communication from the High Representative of the Union for Foreign Affairs and Security Policy and from the European Commission of 29 September 2016 on Strengthening EU support to Tunisia was welcomed in the Council Conclusions of 17 October 2016. The Council reiterates its commitment to supporting Tunisia's transition and underlines the exceptional nature of the situation in Tunisia and the EU's strategic interest in supporting the emergence of a democratic, strong and stable Tunisia in its neighbourhood, as well as the need to support political progress with economic progress on a similar scale. To that end, it calls for the mobilisation of all the instruments available to the EU and the reinforced commitment of the EU and Member States in close collaboration with the Tunisian authorities.
- (6) The Union and the Republic of Tunisia should work together in order to achieve their common objective as defined under the strategic priorities. The development of a prosperous and stable democratic Tunisia is of mutual strategic interest.
- (7) While addressing the most urgent challenges, the Union and the Republic of Tunisia should continue to pursue the main objectives of their long-term partnership, and to work in particular towards creating future prospects for young people, speeding up socio-economic reforms and continuing and strengthening the process of transition to democracy.
- (8) The position of the Union within the Cooperation Council with regard to the adoption of the EU-Tunisia strategic priorities for the period 2018-2020 should be based on the attached draft Decision,

⁽¹⁾ OJ L 97, 30.3.1998, p. 2.

HAS ADOPTED THIS DECISION:

Article 1

The position to be taken on behalf of the European Union within the Association Council set up by the Euro-Mediterranean Agreement establishing an association between the European Community and its Member States, of the one part, and the Republic of Tunisia, of the other part, with regard to the adoption of the EU-Tunisia strategic priorities for the period 2018-2020 is based on the draft Decision of the Association Council attached to this Decision.

Article 2

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

Done at Brussels, 18 September 2018.

For the Council
The President
G. BLÜMEL

DRAFT

DECISION No 1/2018 OF THE EU-TUNISIA ASSOCIATION COUNCIL
of ...
adopting the EU-Tunisia strategic priorities for the period 2018-2020

THE EU-TUNISIA ASSOCIATION COUNCIL,

Having regard to the Euro-Mediterranean Agreement establishing an association between the European Communities and their Member States, of the one part, and the Republic of Tunisia, of the other part ⁽¹⁾,

Whereas:

- (1) The Euro-Mediterranean Agreement establishing an association between the European Communities and their Member States, of the one part, and the Republic of Tunisia, of the other part (hereinafter referred to as the 'Euro-Mediterranean Agreement') was signed on 17 July 1995 and entered into force on 1 March 1998.
- (2) Article 80 of the Euro-Mediterranean Agreement gives the Association Council the power to take decisions it considers appropriate for the purposes of attaining the objectives of the Agreement.
- (3) In accordance with Article 90 of the Euro-Mediterranean Agreement, the parties are to take any general or specific measures required to fulfil their obligations under the Euro-Mediterranean Agreement and are to see to it that the objectives set out therein are attained.
- (4) The review of the European Neighbourhood Policy in 2016 proposed a new phase of engagement with partners, allowing for a greater sense of ownership by both sides.
- (5) The European Union and the Republic of Tunisia have decided to consolidate their privileged partnership by agreeing on a set of strategic priorities for the period 2018-2020 with the aim of supporting and strengthening resilience and stability in the Republic of Tunisia.
- (6) The parties to the Euro-Mediterranean Agreement should agree on the text of the strategic priorities, which translate the EU-Tunisia privileged partnership into practice for the period 2018-2020. Those priorities should support the implementation of the Euro-Mediterranean Agreement, focusing on cooperation in relation to commonly identified shared interests,

HAS ADOPTED THIS DECISION:

Article 1

The Association Council adopts the EU-Tunisia strategic priorities for the period 2018-2020 as set out in the document: 'Strengthening the EU-Tunisia privileged partnership: strategic priorities for the period 2018-2020' set out in the Annex and recommends that the parties implement them.

Article 2

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

Done at ...,

For the EU-Tunisia Association Council
The President

⁽¹⁾ OJ L 97, 30.3.1998, p. 2.

ANNEX

Strengthening the EU-Tunisia privileged partnership: the strategic priorities for the period 2018-2020

1. Introduction

Tunisia made a strategic choice in anchoring itself to the European area, and the development of a prosperous and stable Tunisian democracy within the neighbourhood of the EU is of mutual strategic interest.

The EU-Tunisia privileged partnership testifies to the special and dynamic bilateral relations that have been established, and the shared ambition to advance towards increasingly close links between Tunisia and the European area. The long-term objective is to develop an ambitious framework for future relations post-2020, building on the progress achieved and making full use of the opportunities for closer links provided by the European Neighbourhood Policy in the period 2018-2020.

In the context of the privileged partnership, Tunisia is fully committed to implementing the reforms necessary for the sustainable socio-economic development of the country and to ensure long-term progress in the democratic transition. Realising the scale of the challenge and the difficulties Tunisia is going through, the European Union reiterates its commitment to supporting implementation of these reforms as soon as possible.

The strategic priorities developed in this document translate the privileged partnership into practical terms for the period 2018 to 2020. The creation of future prospects for young people will be at the core of the actions of both sides. The focus will be placed on speeding up socio-economic reforms including improvement of the business environment, and the conclusion of a deep and comprehensive free trade agreement (DCFTA). Democratic consolidation, in particular effective implementation of the 2014 Constitution and good governance will also remain essential. Both sides will reinforce cooperation in the field of security and counter-terrorism, and in relation to migration and mobility with the completion of negotiations on visa facilitation and on readmission, and the increasingly active participation of Tunisia in EU programmes. Enhancing high-level political dialogue and dialogue with civil society and also the visibility of the partnership will go hand in hand with these efforts.

These priorities are based on the Tunisian 2016-2020 Five-Year Development Plan ⁽¹⁾ and the Joint Communication Strengthening EU support for Tunisia ⁽²⁾.

2. Strategic priorities of the EU-Tunisia privileged partnership for the period 2018-2020

Partnership for youth

The EU and Tunisia consider enhancing young people's prospects for the future to be a major objective, as shown by the EU-Tunisia partnership for youth launched by the Tunisian President and the High Representative/Vice-President on 1 December 2016. In order to respond better to the needs of young Tunisians, the various ongoing and future actions should be more consistent. On the basis of the dialogue launched for implementing this partnership, the EU and Tunisia have undertaken to consolidate measures to promote youth employment and employability, mobility, and increased participation of young people in public life and politics, in particular in local initiatives. Employability will require the reform of education and vocational training, the creation of closer links between the private sector and educational and training systems, and the promotion of and support for innovative initiatives launched by young people, particularly in the areas of new technologies and culture. Support for the development of a Tunisian national strategy for youth will be a key element of the partnership, as will be strengthening institutions and organisations dedicated to youth.

⁽¹⁾ This plan advocates a new development model for sustainable and inclusive growth and is structured around five priorities: (i) good governance, public administration reform and the fight against corruption, (ii) transition from a low-cost economy to an economic hub, (iii) human development and social inclusion, (iv) realisation of regional ambitions, and (v) the green economy, which is a pillar of sustainable development.

⁽²⁾ This Communication from the High Representative of the European Union for Foreign Affairs and Security Policy and the European Commission to the European Parliament and the Council (JOIN (2016)47 final of 29 September 2016) is based on five priorities: (i) promoting good governance and public administration reform; (ii) reinforcing the role played by civil society; (iii) investing in the future: creating jobs and fostering sustainable economic development; (iv) reducing disparities throughout society; (v) support in tackling security challenges; (vi) joint efforts for better management of migration and mobility.

Complementing this commitment to youth, both sides will work on the following strategic priorities:

2.1 Inclusive and sustainable socio-economic development

Tunisia's political progress can only be sustained if it is accompanied by economic progress on a similar scale. In view of Tunisia's fragile socio-economic situation, with high youth unemployment (especially among the educated) and significant regional and social disparities, one of the key objectives will be to contribute to turning round the Tunisian economy, to making it more competitive and diversified and to transforming it in an inclusive and sustainable fashion, with due regard for international commitments on the environment and climate change. The EU will continue to support and encourage structural reforms.

More particularly, measures in the area of socio-economic development will be organised around the following commitments:

- improving the business climate and supporting the development of the private sector and private investment, in particular through: (i) simplification and streamlining of administrative procedures for businesses, (ii) improving access to finance, and (iii) boosting public and private investment – in particular effective implementation of the 2016 law on investment and the 2017 law recasting tax benefits, taking account of harmful arrangements as regards abolition of tax advantages;
- there will also be an emphasis on actively promoting entrepreneurship and the development of SMEs/VSEs;
- defining and implementing missing sectoral strategies, for instance for tourism;
- improving protection of the environment and the management of natural resources (including water), in particular through implementation of the national green economy strategy and implementation of Tunisia's international commitments on climate change (determined national contribution), the blue economy and fishery resources;
- improving the competitiveness of traditional and growth sectors in industry and agriculture, in particular through support for innovation and ensuring sustainable resource management, and diversifying export markets;
- developing the energy sector, including electricity interconnections between the EU and Tunisia, and the promotion of renewable energy sources and energy efficiency;
- developing a safe, secure, sustainable and efficient transport system based on harmonised transport standards and an integrated multimodal network in order to facilitate south-south and north-south connections;
- consolidating the public finance management system through the adoption and implementation of a new organic budget law, reform of the state audit system and improving the governance of public enterprises. Implementing the reform of the tax system (simplification of the tax system, tax fairness, decentralisation, modernisation of the administration, fighting tax avoidance and implementation of relevant international commitments) represents a crucial step towards more inclusive development of the country. Support for the on-going banking reforms and the 2017-2021 national financial inclusion strategy concerning access, use and quality of services are also important;
- implementing the decentralisation process, with a view to developing public services and social infrastructure (in particular in the fields of education, culture, health, water and sanitation) to meet the needs of local communities; and accelerating the process of development of the regions in Tunisia's interior, a commitment shared by both parties to gradually reduce socio-economic disparities.

To foster social progress, both parties undertake to continue to promote:

- employment, in particular through further reforms to ensure fair access to high quality education and vocational training in line with the needs of the labour market; in the framework of an active policy to improve opportunities for entering the labour market;
- an integrated and efficient Tunisian policy on social inclusion and effective social protection, in particular through strengthening the capacities of the relevant public bodies, supporting the reforms undertaken by Tunisia in the field of social cohesion, and implementing Article 67 of the EU-Tunisia Association Agreement on the coordination of social security schemes and guaranteed application of principles of fair treatment in social legislation; and
- inclusive social dialogue to enhance capacity to mitigate socio-economic imbalances, reduce social tensions and promote real social peace – and thus also to improve the attractiveness of the country to foreign investors.

Both sides remain fully committed to the process of negotiations towards a Deep and Comprehensive Free Trade Agreement (DCFTA) and have agreed on a concrete action plan for 2018 to enable progress to be made with a view to accelerating the negotiations with a view to concluding them as soon as possible. The EU and Tunisia will continue to promote the modernisation of the Tunisian economy for the benefit of all, including the most disadvantaged regions and communities, and to boost job creation, particularly for young people. Both sides undertake to increase Tunisia's economic integration in the European market as well as in the Maghreb region.

In order to strengthen the role of innovation and research in economic, social and regional development, the EU and Tunisia will work on integrating Tunisia in the European Research Area, in particular by promoting higher education, strengthening governance, mechanisms for promoting public research and technology transfers between academia and industry.

2.2 Democracy, good governance and human rights

The EU and Tunisia will continue to attach particular importance to the process of democratic reform and the promotion of good governance and the rule of law, to respect for human rights and fundamental freedoms and to the reinforcement of the role and participation of civil society. Both parties will continue to promote the process of political reforms through the effective implementation of the Constitution and of international commitments entered into by Tunisia.

Priority aspects in the areas of good governance and respect for the rule of law will include in particular:

- reinforcement of the institution of parliament and the creation and effective establishment of independent bodies;
- establishment of the Constitutional Court
- consolidation of a democratic, transparent and independent electoral process;
- the fight against corruption and fraud, inter alia through support for the national authority for combating corruption;
- reform of the judicial system, including approximation to international standards including those of the Council of Europe;
- implementation of a strategy to reform and modernise public administration, comprising improvement of services at central and local level, the introduction of evidence-based decision-making, the simplification of administrative procedures and the development of digital administration;
- support for the process of decentralisation, including capacity-building and increasing the budgets of local administrations, in particular in the context of the municipal elections in May 2018; strengthening of civil society organisations, their role and their contribution to the decision-making process, and intensification of the participation of citizens, particularly of young people, in political life and the decision-making process.

Priority commitments relating to respect for and promotion of human rights will include:

- finalisation of the legislative harmonisation process in line with the Constitution and international standards, Tunisia's cooperation in multilateral fora and the implementation of the commitments made under the universal periodic review mechanism;
- support for efforts to combat all forms of discrimination, to combat torture (including the implementation of commitments made in the framework of the UN Committee Against Torture) and to protect people in vulnerable situations and to promote the rights of women, children and migrants;
- support for Tunisia's pioneering action to combat violence against women, to guarantee complete equality between men and women and to promote the role of women in all areas, especially in the economic and political spheres;
- the protection of freedom of expression and freedom of association;
- the right to the protection of personal data; and
- respect for human rights in the area of security.

2.3 Bringing peoples closer together, mobility and migration

Bringing Tunisian and European societies closer together by stepping up exchanges between peoples, societies and cultures is a key pillar of the privileged partnership. This mobility dimension is particularly important in the implementation of the partnership for youth. Effective implementation of Tunisia's association with Horizon 2020 and its participation in Creative Europe and Erasmus+ will be the cornerstones of these efforts.

The coordinated management of migration is a political priority for both Tunisia and the EU. Both sides will seek to improve dialogue and cooperation, in particular with the implementation of the Partnership for Mobility, consolidating the fight against root causes of irregular migration, and European willingness to support the implementation of a Tunisian asylum system. This cooperation, which will also reflect the regional dimension of these issues, will include:

- implementation of the Tunisian national strategy on migration; also covering asylum and international protection, and including implementation of an appropriate legislative framework;
- the completion of negotiations on readmission agreements and on visa facilitation;
- the good governance of legal migration through better coordination with EU Member States, while also respecting their national competences, including implementation of pilot mobility schemes and better integration of migrants in the host countries;
- supporting the mobilisation of Tunisians living abroad to invest in innovative sectors in Tunisia;
- support for the prevention of irregular migration by taking better account of migration issues in development strategies; this also entails enhanced border management and awareness campaigns on the risks of irregular migration;
- support for activities to prevent and combat migrant smuggling and trafficking in human beings, inter alia through the detection and prosecution of criminal networks; and
- strengthening cooperation on returns and readmission, including through support for sustainable reintegration of Tunisian returnees.

2.4 Security and counter-terrorism

The EU and Tunisia face common security challenges that require both sides to take coordinated action, and they must proceed in line with the shared values of democracy and human rights.

Tunisia intends to implement its global and multisectoral strategy for combating terrorism and violent extremism. Priority areas for cooperation will include:

- implementing the national counter-terrorism strategy, in particular by reinforcing and modernising legislation and security and judicial institutions in line with the democratic values enshrined in the Constitution;
- speeding up the implementation of the programme to support the reform and modernisation of the security sector, including the accountability of security forces, and the deepening of this cooperation building on the progress already made;
- combating money laundering and the financing of organised crime and terrorism, including effectively implementing the action plan agreed with the Financial Action Task Force;
- developing a global policy for preventing radicalisation;
- the return of foreign fighters;
- the development of a policy of assistance and protection for victims of terrorism;
- the fight against organised crime, in particular against firearms trafficking and drugs;
- supporting implementation of the national strategy for the security of borders;
- strengthening cooperation with the relevant agencies of the European Union; and
- cooperation in the field of disaster risk management and prevention.

The European Union will also continue to participate fully in the G7 + 6 group that ensures coordination between Tunisia's main partners.

In addition, other areas of the partnership relating to security/defence could be further developed.

3. The way forward for strengthening the privileged partnership between the EU and Tunisia

The importance attached by both sides to their relationship will continue to be reflected in the intensity of political contacts and regular visits, as part of a broader political dialogue on all topics of mutual interest, including regional and global issues. The regional dimension of these discussions should be consolidated. Both sides are aware, in this respect, of the importance of their cooperation in the context of the Union for the Mediterranean. In addition to the existing dialogues, both sides will work together with a view to the organisation of high-level EU-Tunisia meetings and the participation of Tunisian ministers in informal meetings with members of the Council of the European Union on certain subjects. Both sides encourage parliamentary cooperation between the European Parliament and the Assembly of the Representatives of the People [Assemblée des Représentants du Peuple].

The bodies of the Association Agreement (Association Council, Association Committee and the technical sub-committees) will continue to be the preferred fora for effective implementation of the Partnership. The EU and Tunisia will seek to enhance the effectiveness and added value of their work and, as far as possible, to group this work according to the major priority themes in line with the strategic priorities.

To make the priorities listed above more tangible, a roadmap is to be proposed by Tunisia and approved by the EU. This public document will set out the most urgent measures (legislative, strategic and operational) necessary for the socio-economic recovery of the country. This roadmap will be a flexible and operational mechanism for monitoring on a twice-yearly basis.

Under the Joint Communication, the EU undertook to significantly strengthen its financial support to Tunisia through the European Neighbourhood Instrument. The EU and Tunisia will seek to make maximum use of existing financial opportunities, including new instruments such as the EU External Investment Plan, making the most of complementarity and leverage effects between EU subsidies and loans provided by financial institutions. Both sides will seek to improve the synergy between political and sectoral dialogues, and the implementation of financial cooperation. They will also work towards strengthening mechanisms for coordination and dialogue with financial partners and international donors under the responsibility of the Tunisian side both as regards setting of priorities and their implementation.

Lastly, both sides undertake to give more visibility to the strategic relationship between the EU and Tunisia, and to promote the benefits of their cooperation among citizens on both sides of the Mediterranean.

COUNCIL DECISION (EU) 2018/1926**of 19 November 2018****on the position to be taken, on behalf of the European Union, in the Group of Experts on the European Agreement concerning the work of crews of vehicles engaged in international road transport of the United Nations Economic Commission for Europe**

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 91, in conjunction with Article 218(9) thereof,

Having regard to the proposal from the European Commission,

Whereas:

- (1) The European Agreement concerning the work of crews of vehicles engaged in international road transport (AETR) ⁽¹⁾ entered into force on 5 January 1976.
- (2) A Group of Experts on AETR has been established by the United Nations Economic Commission for Europe (UNECE) in the framework of the AETR. That group is a body empowered to develop and submit proposals for amending the AETR to the UNECE Working Party on Road Transport.
- (3) The Group of Experts on AETR is currently discussing amendments to the AETR, based on a Union proposal following, to that effect, a position on behalf of the Union adopted by Council Decision (EU) 2016/1877 ⁽²⁾. A further amendment to the AETR appears necessary in order to ensure that non-EU Contracting Parties to the AETR can participate in data exchange on driver cards based on harmonised security and data protection standards.
- (4) Regulation (EU) No 165/2014 of the European Parliament and of the Council ⁽³⁾ requires Member States to interconnect their national electronic registers on driver cards through the Telematics Network for the Exchange of Information Concerning the Issuing of Tachograph Cards (TACHOnet) messaging system or, when using a compatible system, to ensure that exchange of electronic data with all other Member States is possible through the TACHOnet messaging system. TACHOnet is a platform for the exchange of information on driver cards between Member States, in order to ensure that drivers do not hold more than one driver card.
- (5) In order to achieve a pan-European harmonisation in the field of electronic exchange of information on driver cards, it is necessary that TACHOnet be used as the single platform by all Contracting Parties to the AETR.
- (6) The connection to the TACHOnet messaging system is currently carried out either directly through a Trans-European Services for Telematics between Administrations (TESTA) connection or indirectly through a Member State already connected to TESTA. As TESTA are services restricted to Member States and institutions of the Union, non-EU Contracting Parties to the AETR can only connect to TACHOnet indirectly.
- (7) The Commission has recently assessed the indirect connections to the TACHOnet messaging system and concluded that they do not provide the same level of security as TESTA. In particular, there is not a sufficient guarantee about the authenticity, integrity and confidentiality of the information exchanged through indirect connections. Indirect connections to TACHOnet should therefore be replaced by a secure connection.
- (8) eDelivery is a network of connection nodes for digital communications developed by the Commission, where every participant at national level becomes a node using standard transport protocols and security policies. eDelivery is a flexible tool that may be customised to each specific service.
- (9) eDelivery makes use of widely implemented security technologies, such as public key infrastructure (PKI), in order to ensure the authenticity, integrity and confidentiality of the information exchanged. Access to TACHOnet of non-EU Contracting Parties to the AETR should be granted by means of eDelivery.

⁽¹⁾ OJ L 95, 8.4.1978, p. 1.

⁽²⁾ Council Decision (EU) 2016/1877 of 17 October 2016 on the position to be adopted, on behalf of the European Union, in the Group of Experts on the European Agreement concerning the work of crews of vehicles engaged in international road transport (AETR), and in the Working Party on Road Transport, of the United Nations Economic Commission for Europe (OJ L 288, 22.10.2016, p. 49).

⁽³⁾ Regulation (EU) No 165/2014 of the European Parliament and of the Council of 4 February 2014 on tachographs in road transport, repealing Council Regulation (EEC) No 3821/85 on recording equipment in road transport and amending Regulation (EC) No 561/2006 of the European Parliament and of the Council on the harmonisation of certain social legislation relating to road transport (OJ L 60, 28.2.2014, p. 1).

- (10) The Contracting Parties to the AETR should follow a specific procedure to receive the digital certificates and the respective electronic keys granting access to TACHOnet.
- (11) The connection to TACHOnet by means of eDelivery implies that the Contracting Parties to the AETR are required to ensure that the electronic keys and certificates granting access to the system are protected and cannot be used by non-authorised parties. The Contracting Parties to the AETR should also guarantee that keys covered by certificates having expired are not used anymore.
- (12) It is necessary to guarantee the protection of personal data available to the parties through TACHOnet in accordance with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981.
- (13) National authorities connected to TACHOnet have the obligation to carry out the relevant technical implementations in order to ensure that TACHOnet operates according to high levels of performance. It is the task of the Commission to set up the tests confirming that those levels of performance are achieved and to implement them in coordination with the national competent authorities.
- (14) In its judgment of 31 March 1971 in Case 22/70 ⁽¹⁾, the Court of Justice of the European Union recognised that the work of crews of vehicles engaged in road transport is an area that is an external competence of the Union. That competence has been exercised since then in numerous legal acts adopted by the Union, including Regulations (EC) No 561/2006 ⁽²⁾ and (EU) No 165/2014 of the European Parliament and of the Council. Since the subject matter of the AETR falls within the scope of Regulation (EC) No 561/2006, the power to negotiate and conclude any relevant agreement and modifications thereto lies exclusively with the Union.
- (15) If accepted by the Group of Experts on AETR, the proposals made by the Contracting Parties may lead to an amendment of AETR, after a procedure for the revision of AETR is launched and concluded. Where those proposals are accepted by the Group of Experts on AETR, as a second step, the Union Member States as Contracting Parties to the AETR are under an obligation to cooperate in using the mechanism for the revision of the AETR, in line with the duty of sincere cooperation pursuant to Article 4(3) of the Treaty on European Union and subject to a Council decision in accordance with Article 218(6) of the Treaty on the Functioning of the European Union, as appropriate. The proposed amendments to the AETR will become effective only once the revision of the AETR is completed.
- (16) It is appropriate to establish the position to be taken on the Union's behalf in the Group of Experts on AETR, as the amendment to the AETR will be binding on the Union.
- (17) As the Union is not a Contracting Party to the AETR and its status does not allow it to communicate the proposed amendments, Member States, acting in the interest of the Union, should communicate the proposed amendments to the Group of Experts on AETR in the spirit of loyal cooperation in order to promote the achievement of the Union's objectives.
- (18) The Union's position is to be expressed by its Member States that are members of the Group of Experts on AETR and of the UNECE Working Party on Road Transport, acting jointly,

HAS ADOPTED THIS DECISION:

Article 1

The position to be taken on the Union's behalf in the Group of Experts on the European Agreement concerning the work of crews of vehicles engaged in international road transport (AETR) shall be in favour of the proposed amendments to the AETR as set out in the document attached to this Decision.

Article 2

The position referred to in Article 1 shall be expressed by the Member States of the Union that are Contracting Parties to the AETR, acting jointly.

Formal and minor changes to the position referred to in Article 1 may be agreed without requiring that position to be amended.

⁽¹⁾ ECLI:EU:C:1971:32.

⁽²⁾ Regulation (EC) No 561/2006 of the European Parliament and of the Council of 15 March 2006 on the harmonisation of certain social legislation relating to road transport and amending Council Regulations (EEC) No 3821/85 and (EC) No 2135/98 and repealing Council Regulation (EEC) No 3820/85 (OJ L 102, 11.4.2006, p. 1).

Article 3

This Decision shall enter into force on the day following that of its adoption.

Done at Brussels, 19 November 2018.

For the Council
The President
E. KÖSTINGER

ATTACHMENT

NEW APPENDIX TO THE AETR

Appendix 4

TACHOnet specifications

1. Scope and purpose

- 1.1. This appendix sets out the terms and conditions regarding the connection of AETR Contracting Parties to TACHOnet through eDelivery.
- 1.2. Contracting Parties connecting to TACHOnet through eDelivery shall abide by the provisions laid down in this Appendix.

2. Definitions

- (a) 'Contracting party' or 'party' means any Contracting party to the AETR;
- (b) 'eDelivery' means the service developed by the European Commission making possible to transmit data between third parties by electronic means, providing evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and protecting transmitted data against the risk of any unauthorised alteration;
- (c) 'TACHOnet' means the system for the electronic exchange of information on driver cards between contracting parties referred to in Article 31(2) of Regulation (EU) No 165/2014;
- (d) 'Central hub' means the information system enabling the routing of TACHOnet messages between requesting and responding parties;
- (e) 'Requesting party' means the contracting party emitting a TACHOnet request or a notification, which is then routed to the appropriate responding party by the central hub;
- (f) 'Responding party' means the contracting party to whom the TACHOnet request or notification is addressed;
- (g) 'Card issuing authority' or 'CIA' means the entity empowered by a contracting party for the issuing and management of tachograph cards.

3. General responsibilities

- 3.1. Neither contracting party may conclude agreements for the access to TACHOnet on behalf of another party or in any other way represent the other contracting party on the basis of this Appendix. Neither contracting party acts as the other contracting party's subcontractor in the operations referred to in this Appendix.
- 3.2. The contracting parties shall provide access to their national register on driver cards through TACHOnet, in the way and with the level of service set out in Sub-appendix 4.6.
- 3.3. The contracting parties shall notify each other without delay if they observe disturbances or errors within their domain of responsibility, which may endanger the fulfilling of the normal operation of TACHOnet.
- 3.4. Each party shall designate contact persons for TACHOnet to the AETR Secretariat. Any change in contact points must be provided to the AETR Secretariat in writing.

4. Tests for connection to TACHOnet

- 4.1. The connection of a contracting party to TACHOnet shall be established after the successful completion of the connection, integration and performance tests in accordance with the instructions and under the supervision of the European Commission.
- 4.2. In case of failure of the preliminary tests, the European Commission may temporarily put on hold the testing phase. The tests shall resume once the contracting party has communicated to the European Commission the adoption of the necessary technical improvements at national level, allowing the successful performance of the preliminary tests.
- 4.3. The maximum duration of the preliminary tests shall be six months.

5. Trust architecture

- 5.1. Confidentiality, integrity and non-repudiation of the TACHOnet messages shall be ensured by the TACHOnet trust architecture.
- 5.2. The TACHOnet trust architecture shall be based on a public key infrastructure (PKI) service set up by the European Commission, whose requirements are laid down in Sub-appendices 4.8 and 4.9.
- 5.3. The following entities shall intervene in the TACHOnet trust architecture:
 - (a) Certification Authority, responsible for the generation of the digital certificates to be delivered by the Registration Authority to the national authorities of the contracting parties (via trusted couriers appointed by them), as well as for setting up the technical infrastructure regarding the issuance, revocation and renewal of digital certificates.
 - (b) Domain Owner, responsible for the operation of the central hub referred to in Sub-appendix 4.1 and for the validation and coordination of the TACHOnet trust architecture.
 - (c) Registration Authority, responsible for registering and approving the requests of issuance, revocation and renewal of digital certificates, and for verifying the identity of the trusted couriers.
 - (d) Trusted Courier, is the person appointed by the national authorities, responsible for handing the public key to the Registration Authority and for getting the corresponding certificate being generated by the Certification Authority.
 - (e) National authority from the contracting party, which shall:
 - (i) generate the private keys and the corresponding public keys to be included in the certificates to be generated by the Certification Authority;
 - (ii) request the digital certificates to the Certification Authority;
 - (iii) appoint the Trusted Courier.
- 5.4. The Certification Authority and the Registration Authority shall be appointed by the European Commission.
- 5.5. Any contracting party connecting to TACHOnet must request the issuance of a digital certificate in accordance with Sub-appendix 4.9, in order to sign and encrypt a TACHOnet message.
- 5.6. A certificate may be revoked in accordance with Sub-appendix 4.9.

6. Data protection and confidentiality

- 6.1. The parties, in compliance with data protection laws at international and national level, and in particular with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, shall adopt all necessary technical and organisational measures to guarantee the security of the TACHOnet data and prevent the alteration or loss of, or unauthorised processing of or access to such data (in particular the authenticity, data confidentiality, traceability, integrity, availability and non-repudiation and security of the messages).
- 6.2. Each party shall protect its own national systems against illicit use, malicious code, viruses, computer intrusions, infringements and illegal tampering of data and other comparable actions by third parties. The parties agree to use commercially reasonable efforts to avoid the transmission of any viruses, time bombs, worms or similar items or any computer programming routines that may interfere with other Party's computer systems.

7. Costs

- 7.1. The contracting parties shall bear their own development and operation costs in conjunction to their own data systems and procedures as required to fulfil the obligations according to this Appendix.
- 7.2. The services specified in Sub-appendix 4.1, provided by the central hub, are free of charge.

8. Subcontracting

- 8.1. The parties may subcontract any of the services for which they are responsible under this Appendix.
 - 8.2. Such subcontracting does not relieve the party from the responsibility pursuant to this Appendix, including the responsibility for the appropriate level of service in accordance with Sub-appendix 4.6.
-

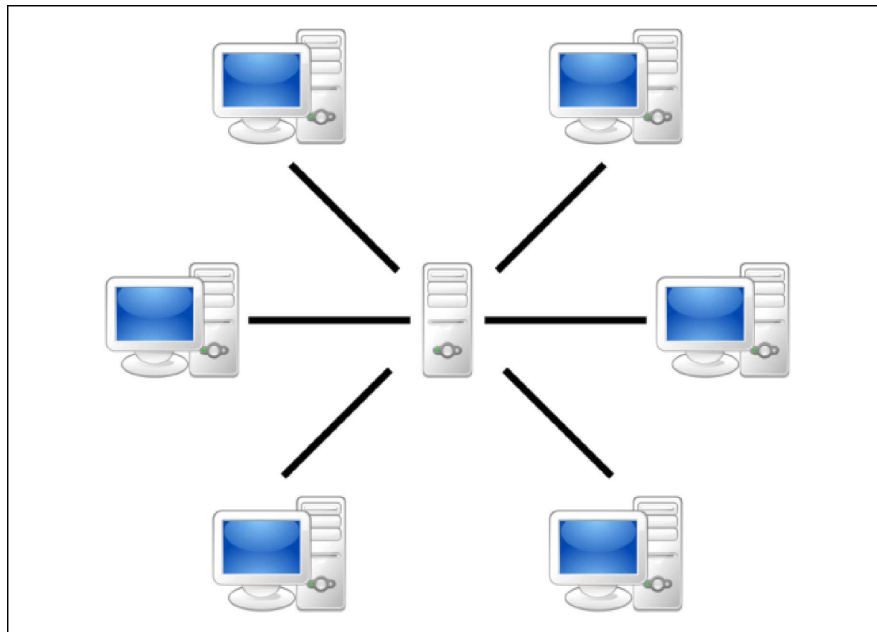
*Sub-appendix 4.1***General aspects of TACHOnet****1. General description**

TACHOnet is an electronic system for the exchange of information on driver cards between AETR contracting parties. TACHOnet routes the requests for information from the requesting parties to the responding parties, as well as the replies from the latter to the former. Contracting parties being part of TACHOnet must connect their national registers on driver cards to the system.

2. Architecture

TACHOnet messaging system shall be composed of the following parts:

- 2.1. A central hub, which shall be able to receive a request from the requesting party, validate it and process it by forwarding it to the responding parties. The central hub shall wait for each responding party to answer, consolidate all the answers and forward the consolidated response to the requesting Party.
- 2.2. National systems of the parties, which shall be fitted with an interface capable of both sending requests to the central hub and receiving the corresponding replies. National systems may use propriety or commercial software to transmit and receive messages from the central hub.

**3. Management**

- 3.1. The central hub shall be managed by the European Commission, which shall be responsible for the technical operation and maintenance of the central hub.
- 3.2. The central hub shall not store data for a period exceeding six months, other than the logging and statistical data set out in Sub-appendix 4.7.
- 3.3. The central hub shall not provide access to personal data, except for authorised European Commission personnel, when necessary for the purpose of monitoring, maintenance and troubleshooting.
- 3.4. Each contracting party shall be responsible for:
 - 3.4.1. The set-up and management of their national systems, including the interface with the central hub.
 - 3.4.2. The installation and maintenance of their national system, both hardware and software, whether proprietary or commercial.
 - 3.4.3. The correct interoperability of their national system with the central hub, including the management of error messages received from the central hub.

- 3.4.4. Taking all the measures to ensure the confidentiality, integrity and availability of the information.
- 3.4.5. The operation of the national systems in accordance with the service levels set out in Sub-appendix 4.6.

Sub-appendix 4.2

Functionalities of TACHOnet

1. The following functionalities shall be provided through TACHOnet messaging system:
 - 1.1. Check Issued Cards (CIC): allows the requesting party to send a Check Issued Cards Request to one or all responding parties, in order to determine if a card applicant already possesses a driver card issued by the responding parties. The responding parties shall reply to the request by sending a Check Issued Cards Response.
 - 1.2. Check Card Status (CCS): allows the requesting party to ask the responding party about the details of a card issued by the latter by sending a Check Card Status Request. The responding party shall reply to the request by sending a Check Card Status Response.
 - 1.3. Modify Card Status (MCS): allows the requesting party to notify the responding party, through a Modify Card Status Request, that the status of a card issued by the latter has changed. The responding party shall reply with a Modify Card Status Acknowledgement.
 - 1.4. Issued Card Driving Licence (ICDL): allows the requesting party to notify the responding party, through an Issued Card Driving Licence Request, that a card has been issued by the former against a driving licence issued by the latter. The responding party shall reply with an Issued Card Driving Licence Response.
2. Other message types deemed suitable for the efficient functioning of TACHOnet shall be included, for instance error notifications.
3. National systems shall recognise the card statuses listed in Table 1, when using any of the functionalities described in point 1. However, parties are not required to implement an administrative procedure that makes use of all of the listed statuses.
4. When a party receives a response or notification giving a status that is not used in its administrative procedures, the national system shall translate the status on the received message to the appropriate value in that procedure. The message shall not be rejected by the responding party, as long as the status in the message is listed in Table 1.
5. The card status listed in Table 1 shall not be used to determine if a driver card is valid for driving. When a party queries the register of the card issuing national authority via the CCS functionality, the response shall contain the dedicated field 'valid for driving'. The national administrative procedures shall be such that CCS responses always contain the appropriate 'valid for driving' value.

Table 1

Card statuses

Card Status	Definition
Application	The CIA has received an application to issue a driver card. This information has been registered and stored in the database with the generated search keys.
Approved	The CIA has approved the application for the tachograph card.
Rejected	The CIA did not approve the application.
Personalised	The tachograph card has been personalised.

Card Status	Definition
Dispatched	The National Authority has dispatched the driver card to the relevant driver or delivering agency.
Handed Over	The National Authority has handed over the driver card to the relevant driver.
Confiscated	The driver card has been taken from the driver by the competent authority.
Suspended	The driver card has been taken temporarily from the driver.
Withdrawn	The CIA has decided to withdraw the driver card. The card has been permanently invalidated.
Surrendered	The tachograph card has been returned to the CIA, and declared no longer needed.
Lost	The tachograph card has been declared lost to the CIA.
Stolen	The tachograph card has been reported stolen to the CIA. A stolen card is considered lost.
Malfunctioning	The tachograph card has been reported as malfunctioning to the CIA.
Expired	The period of validity of the tachograph card has expired.
Replaced	The tachograph card, which has been reported lost, stolen or malfunctioning, has been replaced by a new card. The data on the new card is the same, with the exception of the card number replacement index, which has been increased by one.
Renewed	The tachograph card has been renewed because of a change of administrative data or the validity period coming to an end. The card number of the new card is the same, with the exception of the card number renewal index, which has been increased by one.
In Exchange	The CIA that issued a driver card has received a notification that the procedure to exchange that card for a driver card issued by the CIA of another Party has started.
Exchanged	The CIA that issued a driver card has received a notification that the procedure to exchange that card for a driver card issued by the CIA of another Party has completed.

Sub-appendix 4.3

Message provisions of TACHOnet

1. General technical requirements

- 1.1. The central hub shall provide both synchronous and asynchronous interfaces for the exchange of messages. Parties may choose the most suitable technology to interface with their own applications.
- 1.2. All messages exchanged between the central hub and the national systems must be UTF-8 encoded.
- 1.3. National systems shall be capable of receiving and processing messages containing Greek or Cyrillic characters.

2. XML messages structure and Schema definition (XSD)

- 2.1. The general structure of XML messages shall follow the format defined by the XSD schemas installed in the central hub.
- 2.2. The central hub and the national systems shall transmit and receive messages that conform to the message XSD schema.

2.3. National systems shall be capable of sending, receiving and processing all messages corresponding to any of the functionalities set out in Sub-appendix 4.2.

2.4. The XML messages shall include at least the minimum requirements laid down in Table 2.

Table 2

Minimum requirements for the content of the XML messages

Common Header		Mandatory
Version	The official version of the XML specifications will be specified through the namespace defined in the message XSD and in the <i>version</i> attribute of the Header element of any XML message. The version number ('n.m') will be defined as fixed value in every release of the XML Schema Definition file (xsd).	Yes
Test Identifier	Optional id for testing. The originator of the test will populate the id and all participants in the workflow will forward/return the same id. In production it should be ignored and will not be used if it is supplied.	No
Technical Identifier	A UUID uniquely identifying each individual message. The sender generates a UUID and populates this attribute. This data is not used in any business capacity.	Yes
Workflow Identifier	The workflow id is a UUID and should be generated by the requesting party. This id is then used in all messages to correlate the workflow.	Yes
Sent At	The date and time (UTC) that the message was sent.	Yes
Timeout	This is an optional date and time (in UTC format) attribute. This value will be set only by the central hub for forwarded requests. This will inform the responding party of the time when the request will be timed out. This value is not required in MS2TCN_<x> Req and all response messages. It is optional so that the same header definition can be used for all message types regardless of whether or not the timeoutValue attribute is required.	No
From	The ISO 3166-1 Alpha 2 code of the party sending the message or 'EU'.	Yes
To	The ISO 3166-1 Alpha 2 code of the party to which the message is being sent or 'EU'.	Yes

Sub-appendix 4.4

Transliteration and NYSIIS (New York State Identification and Intelligence System) services

1. The NYSIIS algorithm implemented in the central hub shall be used to encode the names of all the drivers in the national register.
2. When searching for a card via the CIC functionality the NYSIIS keys shall be used as the primary search mechanism.
3. Additionally, parties may employ a custom algorithm to return additional results.
4. The search results shall indicate the search mechanism which was used to find a record, either NYSIIS or custom.
5. If a party chooses to record ICDL notifications then the NYSIIS keys contained in the notification shall be recorded as part of the ICDL data. When searching the ICDL data the party shall use the NYSIIS keys of the applicant's name.

*Sub-appendix 4.5***Security requirements**

1. HTTPS shall be used for the exchange of messages between the central hub and the national systems.
2. National systems shall use the digital certificates referred to in Sub-appendices 4.8 and 4.9 for the purposes of securing the transmission of messages between the national system and the central hub.
3. National systems shall implement, as a minimum, certificates using the SHA-2 (SHA-256) signature hash algorithm and a 2 048 bit public key length.

*Sub-appendix 4.6***Service levels**

1. National systems shall fulfil the following minimum level of service:
 - 1.1. They shall be available 24 hours a day, 7 days a week.
 - 1.2. Their availability shall be monitored by a heartbeat message issued from the central hub.
 - 1.3. Their availability rate shall be 98 %, according to the following table (the figures have been rounded to the nearest convenient unit):

An availability of	means an unavailability of		
	Daily	Monthly	Yearly
98 %	0,5 hours	15 hours	7,5 days

Parties are encouraged to respect the daily availability rate, however it is recognised that certain necessary activities, such as system maintenance, require a downtime of more than 30 minutes. However, the monthly and yearly availability rates remain mandatory.

- 1.4. They shall respond to a minimum of 98 % of the requests forwarded to them in one calendar month.
- 1.5. They shall respond to requests within 10 seconds.
- 1.6. The global request timeout (time within which the requestor may wait for a response) shall not exceed 20 seconds.
- 1.7. They shall be able to service a request rate of 6 messages per second.
- 1.8. National systems may not send requests to the TACHOnet hub at a rate exceeding 2 requests per second.
- 1.9. Every national system shall be able to cope with potential technical problems of the central hub or national systems in other parties. These include, but are not limited to:
 - (a) loss of connection to the central hub;
 - (b) no response to a request;
 - (c) receipt of responses after message timeout;
 - (d) receipt of unsolicited messages;
 - (e) receipt of invalid messages.
2. The central hub shall:
 - 2.1. feature an availability rate of 98 %;
 - 2.2. provide to national systems notification of any errors, either via the response message or via a dedicated error message. The national systems, in turn, shall receive these dedicated error messages and have an escalation workflow in place to take any appropriate action to rectify the notified error.

3. Maintenance

Parties shall notify other parties and the European Commission of any routine maintenance activities via the web application, at least one week before the beginning of those activities if technically possible.

Sub-appendix 4.7

Logging and statistics of the data collected at the central hub

1. In order to ensure privacy, the data for statistical purposes shall be anonymous. Data identifying a specific card, driver or driver licence shall not be available for statistical purposes.
2. Logging information shall keep track of all transactions for monitoring and debugging purposes, and allow the generation of statistics about these transactions.
3. Personal data shall not be retained in the logs for more than 6 months. Statistical information shall be retained indefinitely.
4. The statistical data used for reporting shall include:
 - (a) the requesting party;
 - (b) the responding party;
 - (c) the type of message;
 - (d) the status code of the response;
 - (e) the date and time of the messages;
 - (f) the response time.

Sub-appendix 4.8

General provisions regarding digital keys and certificates for TACHOnet

1. The Directorate-General for Informatics of the European Commission (DIGIT) shall make available a PKI service ⁽¹⁾ (referred to as 'CEF PKI service') to the AETR Contracting Parties connecting to TACHOnet (henceforth the national authorities) through eDelivery.
2. The procedure for request and revocation of digital certificates, as well as the detailed terms and conditions for its usage, are defined in the Appendix
3. Usage of certificates:
 - 3.1. Once the certificate is issued, the national authority ⁽²⁾, shall use the certificate only in the context of TACHOnet. The certificate can be used to:
 - (a) authenticate the origin of data;
 - (b) encrypt data;
 - (c) ensure detection of integrity breaches of data.
 - 3.2. Any usage not explicitly authorised as part of the permitted usages of the certificate is prohibited.
4. Contracting parties shall:
 - (a) protect their private key against unauthorised use;
 - (b) refrain from transferring or revealing their private key to third parties, even as representatives;

⁽¹⁾ A PKI (Public Key Infrastructure) is a set of roles, policies, procedures and systems needed to create, manage, distribute and revoke digital certificates.

⁽²⁾ Identified by the 'O=' attribute value in the Subject Distinguished Name of the issued certificate

- (c) ensure confidentiality, integrity, and availability of the private keys generated, stored and used for TACHOnet;
- (d) refrain from continued use of the private key following expiry of the validity period or revocation of the certificate, other than to view encrypted data (e.g., decrypting emails). Expired keys shall be either destroyed or retained in a manner preventing its use;
- (e) provide the Registration Authority with the identification of those authorised representatives who are authorised to request revocation of certificates issued to the organisation (revocation requests shall include a revocation request password and details about the events that lead to revocation);
- (f) prevent misuse of the private key by requesting the revocation of the associated public key certificate in case of compromise of the private key or of the private key activation data;
- (g) be responsible and hold the obligation of requesting revocation of certificate under circumstances identified in the certification policies (CP) and certification practices statement (CPS) of the Certification Authority;
- (h) notify the Registration Authority without delay of loss, theft, or potential compromise of any AETR keys used in the context of TACHOnet.

5. Liabilities

Without prejudice of the liability of the European Commission in contravention of any requirements laid down in applicable national law or with respect to liability for matters which may not be excluded under that law, the European Commission shall not be responsible or liable with regard to:

- (a) the content of the certificate which lies exclusively with the certificate owner. It shall be the responsibility of the certificate owner to check the accuracy of the certificate content;
- (b) the use of the certificate by its owner.

Sub-appendix 4.9

Description of the PKI service for TACHOnet

1. Introduction

A PKI (Public Key Infrastructure) is a set of roles, policies, procedures and systems needed to create, manage, distribute and revoke digital certificates ⁽¹⁾. The CEF PKI service of eDelivery enables issuance and management of digital certificates used to ensure confidentiality, integrity and non-repudiation of the information exchanged between Access Points (AP).

The PKI service of eDelivery is based on the Trust Centre Services TeleSec Shared Business CA (Certification Authority) for which the Certificate Policy (CP)/Certification Practices Statement (CPS) of TeleSec Shared-Business-CA of T-Systems International GmbH ⁽²⁾ apply.

The PKI service issues certificates that are suitable for securing various business processes within and outside of companies, organisations, public authorities and institutions that require a medium security level to prove the authenticity, integrity and trustworthiness of the end-entity.

2. Certificate Request Process

2.1. Roles and responsibilities

2.1.1. 'Organisation' or 'national authority' requesting the certificate

2.1.1.1. The national authority shall request the certificates in the context of the TACHOnet project.

2.1.1.2. The national authority shall:

- (a) request the certificates from the CEF PKI service;

⁽¹⁾ https://en.wikipedia.org/wiki/Public_key_infrastructure

⁽²⁾ The latest version of the CP and CPS can be downloaded on <https://www.telesec.de/en/sbca-en/support/download-area/>

- (b) generate the private keys and the corresponding public keys to be included in the certificates issued by the Certification Authority;
- (c) download the certificate when approved;
- (d) sign and send back to the Registration Authority:
 - (i) the contact persons and trusted couriers identification form,
 - (ii) the signed individual Power of Attorney ⁽¹⁾.

2.1.2. Trusted Courier

2.1.2.1. The national authority shall appoint a Trusted Courier.

2.1.2.2. The Trusted Courier shall:

- (a) hand over the public key to the Registration Authority during a face-to-face identification and registration process;
- (b) get the corresponding certificate from the Registration Authority.

2.1.3. Domain Owner

2.1.3.1. DG MOVE shall be the Domain Owner.

2.1.3.2. The Domain Owner shall:

- (a) validate and coordinate the TACHOnet network and the TACHOnet trust architecture, including the validation of the procedures for the issuance of the certificates;
- (b) operate the TACHOnet central hub and coordinate the activity of the parties regarding the functioning of TACHOnet;
- (c) perform, along with national authorities, the tests of connection to TACHOnet.

2.1.4. Registration Authority

2.1.4.1. The Joint Research Centre (JRC) shall be the Registration Authority.

2.1.4.2. The Registration Authority shall be responsible for verifying the identity of the trusted courier, for registering and approving the requests of issuance, revocation and renewal of digital certificates.

2.1.4.3. The registration authority shall:

- (a) assign the unique identifier to the national authority;
- (b) authenticate the identity of the national authority, its contact points and trusted couriers;
- (c) communicate with the CEF Support regarding the authenticity of the national authority, its contact points and trusted couriers;
- (d) inform the national authority about the approval or rejection of certificate.

2.1.5. Certification Authority

2.1.5.1. The Certification Authority shall be responsible for the provision of the technical infrastructure for the request, issuing and revocation of digital certificates.

2.1.5.2. The Certification Authority shall:

- (a) provide for the technical infrastructure for certificate requests by national authorities;
- (b) validate or reject certificate request;
- (c) communicate with the Registration Authority for the identity verification of the requesting organisation, when required.

2.2. Certificate issuance

2.2.1. The certificate issuance shall be carried out in accordance with the following sequential steps, represented in Figure 1:

- (a) **Step 1:** Trusted Courier identification;

⁽¹⁾ A power of attorney is a legal document by which the Organisation empowers and authorises the European Commission represented by the identified official responsible for the CEF PKI service the power to request the generation of a certificate on its behalf from the T-Systems International GmbH TeleSec Shared Business CA. See also point 6.

- (b) **Step 2:** Certificate request creation;
- (c) **Step 3:** Registration at RA;
- (d) **Step 4:** Certificate generation;
- (e) **Step 5:** Certificate publication;
- (f) **Step 6:** Certificate acceptance.

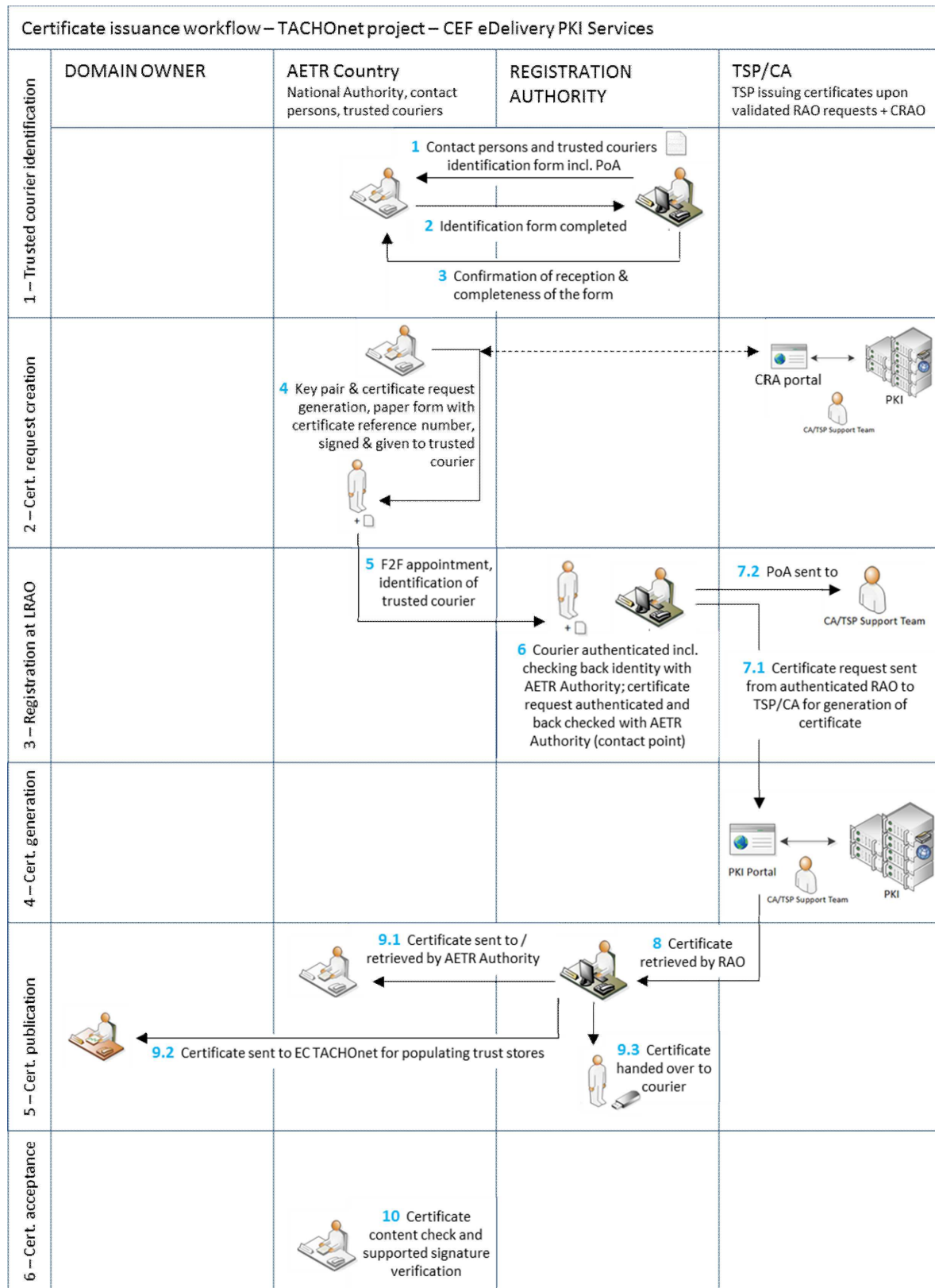


Figure 1 — Certificate issuance workflow

2.2.2. Step 1: Trusted Courier identification

The following process shall be carried out for the Trusted Courier identification:

- (a) The Registration Authority shall send to the national authority the contact persons and trusted couriers' identification form ⁽¹⁾. This form shall also include a power of attorney (PoA) that the organisation (AETR Authority) shall sign.
- (b) The national authority shall send back the completed form and signed PoA to the Registration Authority.
- (c) The Registration Authority shall acknowledge the good reception and completeness of the form.
- (d) The Registration Authority shall provide an updated copy of the list of contact persons and trusted couriers to the domain owner.

2.2.3. Step 2: Certificate request creation

2.2.3.1. The request and the retrieval of the certificate shall be done on the same computer and with the same browser.

2.2.3.2. The following process shall be carried out for the certificate request creation:

- (a) The Organisation shall navigate to the user web interface to request the certificate via the URL <https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en;> and shall enter the username '**sbca/CEF_eDelivery.europa.eu**' and the password '**digit.333**'

Figure 2

- (b) The Organisation shall click on 'request' on the left side of the panel and shall select 'CEF_TACHOnet' in the dropdown list.

Figure 3

- (c) The Organisation shall populate the certificate request form laid down in Figure 4 with the information in Table 3, clicking on 'Next (soft-PSE)' to finish the process.

⁽¹⁾ See point 5.

The screenshot shows a registration form with the following fields and callouts:

- * Country:** BE. Callout: Organisation's Country Code (Case Sensitive, ISO 3166-1)
- Organisation/company (O):** My Company. Callout: Official Organisation Name (case sensitive)
- Master domain (OU1):** CEF_eDelivery.europa.eu
- Area of responsibility (OU2):** CEF_TACHOnet
- Identifiant (OU3):** AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx. Callout: Must be: TYPE=AP_PROD concatenated with '/' separator and 'GTC_OID-1.3.130.0.2018.xxxxxx' where Ares(2018)xxxxxx is the allocated number
- * Last name (CN):** GRP:CEF_TACHOnet_AP_PROD_BE_001. Callout: Must start with: 'GRP:' concatenated with CEF_TACHOnet_<TYPE>_<COUNTRY CODE>_<Unique Identifier of the Accss Point> TYPE=AP_PROD COUNTRY CODE = as defined above. E.g.: 'GRP: CEF_TACHOnet_AP_PROD_BE_001'
- * E-mail:** CEF-EDELIVERY-SUPPORT@ec.europa.eu. Callout: Must be: 'CEF-EDELIVERY-SUPPORT@ec.europa.eu'
- Address:** Leave Empty. Callout: Must be the official address of the Organisation. (Used for the Power of Attorney). Attention: if the ZIP code is NOT a 5-digit ZIP code, leave the ZIP code field empty and put the ZIP code in the City field.
- Street, ZIP code, City, Phone no.:** Fields for address details.
- Identification data:** Includes email (business.register.xx@mail.com) and name (Mr Johan Smith). Callout: Email: the email address must be the same as the one used for registering the Unique Identifier. + Name of the person representing the organisation. (Used for the Power of Attorney)
- * Revocation password:** (max. 50 characters). Callout: The organisation can choose its own password or click on the button 'Adopt revocation password proposal'
- * Revocation password repetition:** (max. 50 characters)
- Revocation password proposal:** juHEVeV36
- Adopt revocation password proposal** button
- Next (soft-PSE)** button. Callout: click here to end
- Next (SmartCard/applet)** and **Cancel** buttons

Figure 4

Requested Fields	Description
Country	C = Country Code , location of certificate owner, verified using a public directory; Constraints: 2 characters, in accordance to ISO 3166-1, alpha-2, Case Sensitive; Examples: DE, BE, NL, Specific cases: UK (for Great-Britain), EL (for Greece)
Organisation/Company (O)	O = Organisation name of the certificate owner
Master domain (OU1)	OU = CEF_eDelivery.europa.eu
Area of responsibility (OU2)	OU = CEF_TACHOnet

Requested Fields	Description
Department (OU3)	Mandatory value per 'AREA OF RESPONSIBILITY' The content must be checked using a positive list (white list) when the certificate is requested. If the information does not correspond to the list, the request is prevented. Format: OU=<TYPE>-<GTC_NUMBER> Where '<TYPE>' is replaced by AP_PROD: Access Point in Production environment. And where <GTC_NUMBER> is GTC_OID-1.3.130.0.2018.xxxxxx, where Ares(2018)xxxxxx is the GTC number for the TACHOnet project. e.g.: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
First name (CN)	Must be Empty
Last name (CN)	Must start with 'GRP:', followed by a common name. Format: CN = GRP:<AREA OF RESPONSIBILITY>-<TYPE>-<COUNTRY CODE>-<UNIQUE IDENTIFIER> e.g.: GRP:CEF_TACHOnet_AP_PROD_BE_001
Email	E = CEF-EDELIVERY-SUPPORT@ec.europa.eu
Email 1 (SAN)	Must be Empty
Email 2 (SAN)	Must be Empty
Email 3 (SAN)	Must be Empty
Address	Must be Empty
Street	Must be the official address of the Organisation of the Certificate Owner. (Used for the Power of Attorney.)
Street no.	Must be the official address of the Organisation of the Certificate Owner. (Used for the Power of Attorney.)
Zip Code	Must be the official address of the Organisation of the Certificate Owner. (Used for the Power of Attorney.) Attention: if the ZIP code is NOT a 5-digit ZIP code, leave the ZIP code field empty and put the ZIP code in the City field.
City	Must be the official address of the Organisation of the Certificate Owner. (Used for the Power of Attorney.) Attention: if the ZIP code is NOT a 5-digit ZIP code, leave the ZIP code field empty and put the ZIP code in the City field.
Phone no	Must be Empty

Requested Fields	Description
Identification data	The email address must be the same as the one used for registering the Unique Identifier. + Must be the name of the person representing the organisation. (Used for the Power of Attorney) + Commercial Register No (only mandatory for private organisations) Entered at the Local Court of (only required for German and Austrian private organisations)
Revocation password	Mandatory field chosen by the requestor
Revocation password repetition	Mandatory field chosen by the requestor repeated

Table 3. Complete details of each requested field

- (d) The selected key length shall be 2 048 (High Grade).

Version: 1.7.14 Home German RSS Newsletter Locations Contact

Login as: CEF_eDelivery.europa.eu

End entity certificate

- request
- fetch
- revoke
- renew
- search
- logout

CRL

CA certificates

Information

User certificate

In the "Information on key length" selection field, please define whether a Soft-PSE (file) consisting of a certificate and private key is to be created or if the certificate is to be issued on the smart card key medium.

Please note that you can only pick up the certificate once the responsible sub-registrar has approved the certificate application. You will be notified of the approval by e-mail.

Certificate data

Country (C) BE

Organization/company (O) European Commission

Master domain (OU1) CEF_eDelivery.europa.eu

Area of responsibility (OU2) CEF_TACHOnet

Department (OU3) AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx

First name (CN)

Last name (CN) GRP:CEF_TACHOnet_AP_PROD_BE_001

E-mail CEF.EDELIVERY-SUPPORT@ec.europa.eu

Selection of key length 2048 (High Grade)

Request Cancel

© 2007-2018 T-Systems International GmbH. All rights reserved. Deutsche Telekom About this Website Privacy Policy Sitemap Glossary

Figure 5

- (e) The Organisation shall record the reference number to retrieve the certificate.

Version: 1.5.5 Home German RSS Newsletter Locations Contact

Login as: CEF_eDelivery.europa.eu

End entity certificate

- request
- fetch
- revoke
- renew
- search
- logout

CRL

CA certificates

Information

User certificate

The certificate was requested. Your request was stored with reference number 776002.

Please note that you can only pick up the certificate once the responsible sub-registrar has approved the certificate application. You will be notified of the approval by e-mail.

© 2007-2018 T-Systems International GmbH. All rights reserved. Deutsche Telekom About this Website Privacy Policy Sitemap Glossary

Certificate Reference Number

Figure 6

- (f) The CEF Support Team shall check for new requests of certificates and verify if the information in the certificate request is valid, i.e. that it conforms to the naming convention specified in Appendix 5.1 Certificate Naming Convention.
- (g) The CEF Support Team shall verify that the information entered in the request is in a valid format.
- (h) When either check from points 5 or 6 above fails, the CEF Support Team shall send an email to the email address provided in the 'Identification data' of the request form, with the Domain Owner in cc, in which the Organisation is requested to start the process again. The failed certificate request shall be cancelled.
- (i) The CEF Support Team shall send an email to the Registration Authority about the validity of the request. The email shall include:
 - (1) the name of the Organisation, available in the field 'Organisation (O)' of the certificate request;
 - (2) the certificate data including the name of the AP for which the certificate is to be issued, available in the field 'Last Name (CN)' of the certificate request;
 - (3) the certificate reference number;
 - (4) the address of the Organisation, its email and the name of the person representing it.

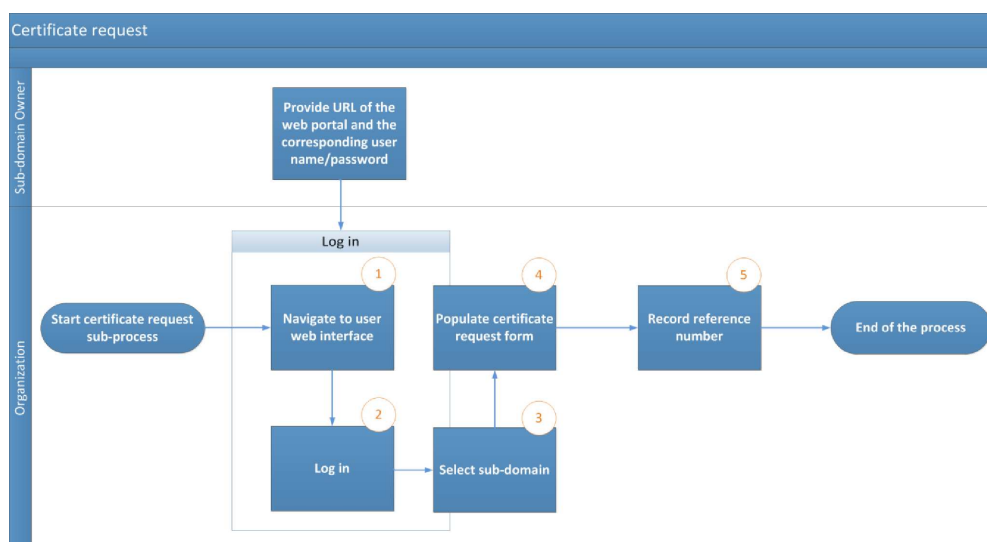


Figure 7 – Certificate request process

2.2.4. Step 3: Registration at Registration Authority (Certificate approval)

2.2.4.1. The Trusted Courier or contact point shall make an appointment with the Registration Authority via email exchange, identifying the Trusted Courier who will proceed to the face-to-face meeting.

2.2.4.2. The Organisation shall prepare the documentary package consisting in:

- (a) the filled-in and signed power of attorney;
- (b) a copy of the valid passport of the trusted courier who will perform the face-to-face. This copy must be signed by one of the step 1 identified Organisation points of contact;
- (c) the certificate request paper form signed by one of the points of contact of the Organisation.

2.2.4.3. The Registration Authority shall receive the Trusted Courier after identity screening at the building reception. The Registration Authority shall conduct the face-to-face registration of the certificate request by:

- (a) identifying and authenticating the Trusted Courier;
- (b) verifying the trusted courier physical appearance against the passport presented by the Trusted Courier;

- (c) verifying the validity of the passport presented by the Trusted Courier;
- (d) verifying the validated passport presented by the trusted courier against the copy of the valid passport of the trusted courier signed by one of the identified points of contact of the Organisation. Signature is authenticated against the original 'trusted courier and contact points identification form';
- (e) verifying the filled-in and signed power of attorney;
- (f) verifying certificate request paper form and its signature against the original 'trusted courier and contact points identification form';
- (g) calling the signatory contact point to double check the identity of the trusted courier and the content of the certificate request.

2.2.4.4. The Registration Authority shall confirm to the CEF Support Team that the national authority is indeed authorised to operate the components for which it is asking the certificates and that the corresponding face-to-face registration process was successful. The confirmation shall be sent using a 'CommiSign' certificate secure email, attaching a scanned copy of the authenticated face-to-face documentary package and of the signed process check list carried out by the Registration Authority.

2.2.4.5. If the Registration Authority confirms the validity of the request, the process shall carry on as set out in 2.2.4.6 and 2.2.4.7. Otherwise the certificate issuance shall be rejected and the Organisation shall be informed.

2.2.4.6. The CEF Support Team shall approve the certificate request and shall notify the Registration Authority the approval of the certificate.

2.2.4.7. The Registration Authority shall notify the Organisation that the certificate can be retrieved via the user portal.

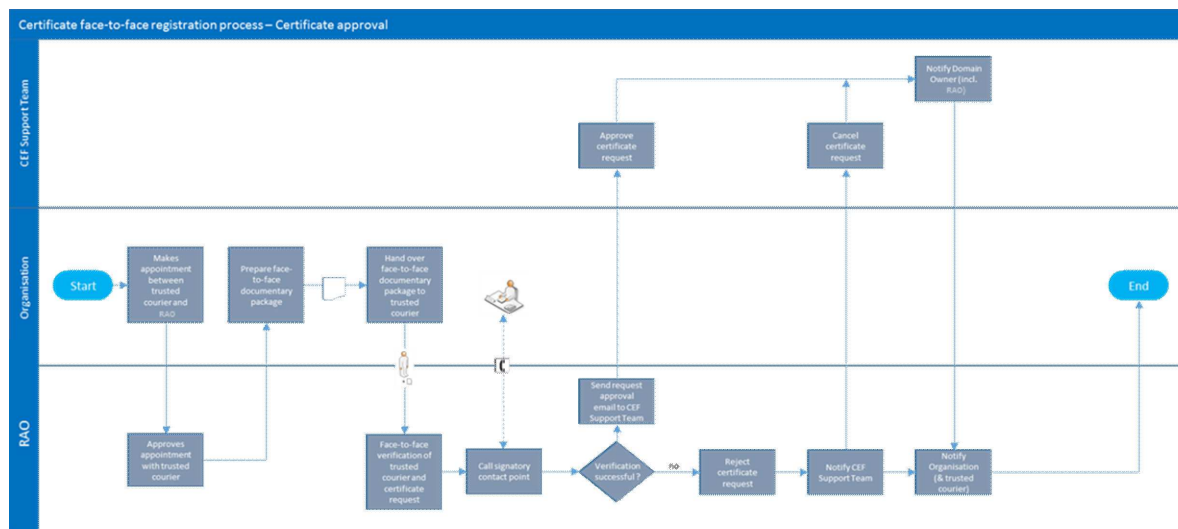


Figure 8 — Certificate approval

2.2.5. Step 4: Certificate generation

Upon approval of the certificate request, the certificate shall be generated.

2.2.6. Step 5: Certificate publication and retrieval

2.2.6.1. Following approval of the certificate request, the Registration Authority shall retrieve the certificate and hand over a copy to the Trusted Courier.

2.2.6.2. The Organisation shall receive the notification from the Registration Authority that the certificates can be retrieved.

- 2.2.6.3. The Organisation shall navigate to the user portal at <https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en> and shall log in with the username '**sbca/CEF_eDelivery.europa.eu**' and the password '**digit.333**'.

Figure 9

- 2.2.6.4. The Organisation shall click on the 'fetch' button on the left-hand side and shall provide the reference number recorded during the certificate request process;

Figure 10

- 2.2.6.5. The Organisation shall install the certificates by clicking on the install button;

Certificate details	
Serial number	128ff8fc035ade0b
Reference number	776002
Subject DN	C=BE; O=MyCompany; OU=CEF_eDelivery.Europa.eu; OU=CEF_TACHOnet; OU=AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx; CN=GRP:CEF_TACHOnet_AP_PROD_BE_001; E=CEF-EDELIVERY-SUPPORT@ec.europa.eu; SERIALNUMBER=1
Issuer DN	C=DE, O=T-Systems International GmbH, OU=T-Systems Trust Center, ST=Nordrhein Westfalen, PostalCode=57250, L=Netphen, STREET=Untere Industriestr. 20, CN=Shared Business CA 4
Valid from	05/12/2016 17:56:56 CEST
Valid to	05/13/2019 01:59:59 CEST
Status	Active

Figure 11

- 2.2.6.6. The certificate shall be installed on the Access Point. As this is implementation-specific, the Organisation shall refer to its Access Point provider to obtain the description of this process.

- 2.2.6.7. The following steps are needed for the certificate installation on the Access Point:

- export the private key and the certificate,
- create the keystore and the truststore,

(c) install the keystore and the truststore on the access point.

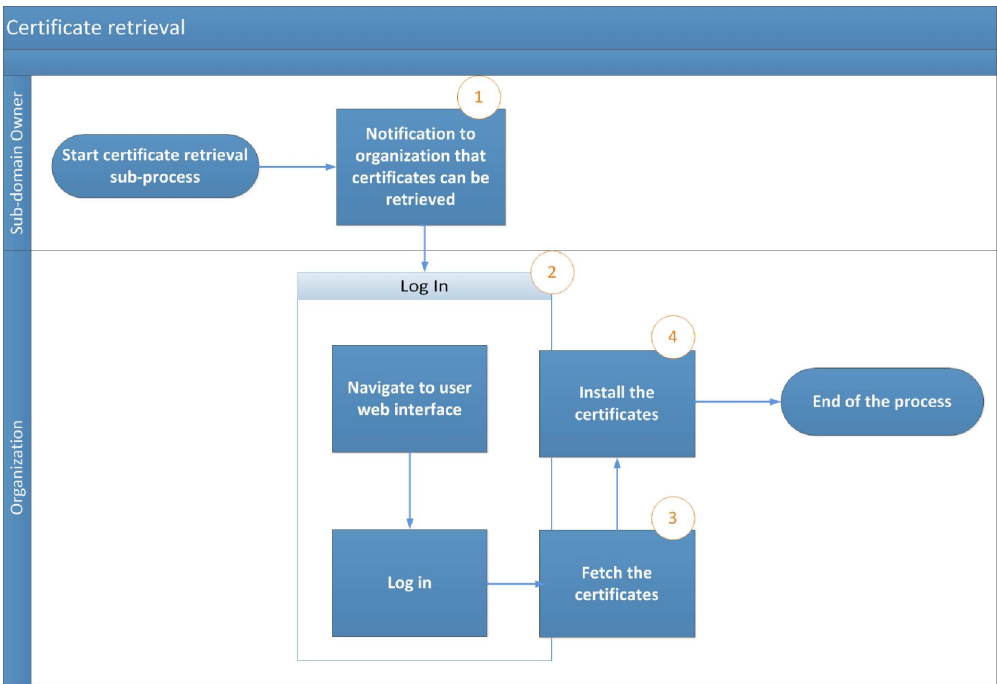


Figure 12 — Certificate retrieval

3. Certificate revocation process

- 3.1. The Organisation shall submit a revocation request through the user web portal;
- 3.2. The CEF Support Team shall execute the certificate revocation.

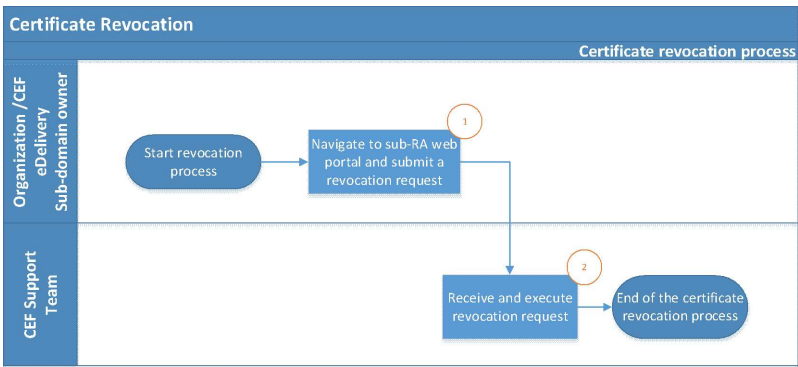


Figure 13 — Certificate revocation

4. General Terms and conditions of the CEF PKI service

4.1. Context

In its capacity as Solution Provider of the eDelivery Building Block of the Connecting Europe Facility, DIGIT shall make available a PKI service ⁽¹⁾ ('CEF PKI service') to the AETR Contracting Parties. The CEF PKI service shall be used by national authorities ('end-users') participating in TACHOnet.

DIGIT is a PKI tenant within the TeleSec Shared-Business-CA solution ('SBCA') operated in the Trust Centre of the Group unit T-Systems International GmbH ('T-Systems' ⁽²⁾). DIGIT plays the role of Master Registrar of the 'CEF_eDelivery.europa.eu' domain of the SBCA. In this role, DIGIT creates sub-domains within the 'CEF_eDelivery.europa.eu' domain for each project using the CEF PKI service.

⁽¹⁾ A PKI (Public Key Infrastructure) is a set of roles, policies, procedures and systems needed to create, manage, distribute and revoke digital certificates.
⁽²⁾ The trusted role of the Trust Centre operator, located in the T-Systems Trust Centre, also performs the task of internal registration authority.

This document provides details on the terms and conditions of the TACHOnet sub-domain. DIGIT plays the role of sub-Registrar of this sub-domain. In this capacity, it issues, revokes and renews the certificates of this project.

4.2. Disclaimer on liability

The European Commission accepts no responsibility or liability whatsoever with regard to the content of the certificate which lies exclusively with the certificate owner. It is the responsibility of the certificate owner to check the accuracy of the certificate content.

The European Commission accepts no responsibility or liability whatsoever with regard to the use of the certificate by its owner being a third legal entity outside the European Commission.

This disclaimer is not intended to limit the liability of the European Commission in contravention of any requirements laid down in applicable national law or to exclude its liability for matters which may not be excluded under that law.

4.3. Authorised/prohibited uses of certificates

4.3.1. Permitted usage of certificates

Once the certificate is issued, the certificate owner ⁽¹⁾ shall use the certificate only in the context of TACHOnet. Within this context, the certificate can be used to:

- authenticate the origin of data,
- encrypt data,
- ensure detection of integrity breaches of data.

4.3.2. Prohibited usage of certificates

Any usage not explicitly authorised as part of the permitted usages of the certificate is prohibited.

4.4. Additional obligations of the certificate owner

The detailed terms and conditions of the SBICA are defined by T-Systems in the Certificate Policy (CP)/Certification Practice Statement (CPS) of the SBICA service ⁽²⁾. This document includes security specifications and guidelines regarding technical and organisational aspects and describes the activities of the Trust Centre operator in the roles of Certification Authority (CA) and Registration Authority (RA) as well as the Registration Authority's (RA) delegated third party.

Only entities authorised to participate TACHOnet can request a certificate.

Regarding certificate acceptance, clause 4.4.1 of the SBICA Certificate Policy and Certification Practice Statement ('CP/CPS') applies, furthermore the terms of use and provisions described in the present document are deemed accepted by the organisation to which the certificate is issued ('O=') when first used.

Regarding publication of the certificate, clause 2.2 of the SBICA CP/CPS applies.

All certificate owners shall comply with the following requirements:

- (1) protect their private key against unauthorised use;
- (2) refrain from transferring or revealing their private key to third parties, even as representatives;
- (3) refrain from continued use of the private key following expiry of the validity period or revocation of the certificate, other than to view encrypted data (e.g., decrypting emails);
- (4) the certificate owner is responsible for copying or forwarding the key to the end-entity or entities;

⁽¹⁾ Identified by the 'O=' attribute value in the Subject Distinguished Name of the issued certificate.

⁽²⁾ The latest version of the T-Systems SBICA CP/CPS is available from <https://www.telesec.de/en/sbica-en/support/download-area/>

- (5) the certificate owner must obligate the end-entity/all end-entities to comply with the present terms and conditions, including the SBCA CP/CPS, when dealing with the private key;
- (6) the certificate owner must provide the identification of those authorised representatives who are authorised to request revocation of certificates issued to the organisation with the details of events that lead to revocation and the revocation password;
- (7) for certificates associated to groups of persons and functions and/or legal persons, after a person leaves the group of end-entities (e.g. termination of the employment relationship), the certificate owner must prevent misuse of the private key by revoking the certificate;
- (8) the certificate owner is responsible and shall request revocation of the certificate under the circumstances referred to in clause 4.9.1 of the SBCA CP/CPS.

Regarding renewal or rekey of certificates, clause 4.6 or 4.7 of the SBCA CP/CPS applies.

Regarding amendment of certificate, clause 4.8 of the SBCA CP/CPS applies.

Regarding certificate revocation, clause 4.9 of the SBCA CP/CPS applies.

5. Contact persons and trusted couriers identification form (sample)

I, [name and address of the organisation representative], certifies that the following information are to be used in the context of the request, generation and retrieval of public key digital certificates for TACHOnet access points supporting the confidentiality, integrity and non-repudiation of the TACHOnet messages:

Contact person information:

— Contact person #1	— Contact person #2
— Name:	— Name:
— First names:	— First names:
— Mobile phone:	— Mobile phone:
— Telephone:	— Telephone:
— Email:	— Email:
— Specimen handwritten signature: —	— Specimen handwritten signature: — — —

Trusted courier information:

— Trusted courier #1	— Trusted courier #2
— Name:	— Name:
— First names:	— First names:
— Mobile phone:	— Mobile phone:
— Email:	— Email:
— Passport issuing country:	— Passport issuing country:
— Passport number:	— Passport number:
— Passport validity end date:	— Passport validity end date:

Place, date, company stamp or seal of the Organisation:

Signature of the authorised representative:

6. Documents

6.1. Individual Power of Attorney (sample)

A sample of the individual Power of Attorney that must be signed and presented by the trusted courier during face-to-face registration at RAO can be found here:

Please print the text of this document on your letterhead, add your company stamp and have it signed by the administrative contact or admin-c of the domain.

The power of attorney must be signed by an authorized representative of the organization (principal).

The Shared-Business-CA customer will then submit this document together with the order document to the T-Systems International GmbH Trust Center.

Individual power of attorney / Power of attorney granted to one person

I, *[name and address of the end-user]*, empower as an authorized person of this organization *

[name of the company receiving the certificate]

(e. g. sample company, sample authority, to be registered in the O-field of the certificate *)

following company and/or person:

Company: **European Commission**

Address: **DG DIGIT, 28 rue Belliard, 1000 Brussels**

Represented by Mr/Mrs/Ms: **Adrien FERIAL**

On my behalf, by complying with all and any regulations and formalities (particularly Certificate Policy (CP) / Certification Practice Statement (CPS)), for authorisation to manage (i.e. issue, revoke, renew) X.509v3-certificates, including the complete key-material, issued by the certification authority „TeleSec Shared-Business-CA“, in respect of the domain as above mentioned.

This power of attorney relates to issuing and management of the following certificate types (the applicable type has to be marked):

☒ user¹: e.g. mail security (signature, encryption), virtual private network (VPN), TLS/SSL client

☐ server²: e.g. identity of web server, TLS/SSL client server authentication

Please enter additionally the country, organization, locality, state or province name of the server:

☐ eMail-Gateway³: e.g. identity of eMail gateways / eMail-Appliance, virtual mail-administrating centre.

Validity

☒ The power of attorney is valid until further notice, but up to a **maximum of 27 months**² or **maximum of 36 months**^{1,3} from date of issuance.

☐ The power of attorney is valid until _____ (mm.dd.yyyy), but up to a **maximum of 27 month**² months or **maximum of 36 months**^{1,3} from date of issuance.

Please note that a time limit on the power of attorney can cause that a request for certificate order, renewal or revocation may not be possible because the validity period of the authorization has been exceeded!

Place, date, company stamp or seal of the organisation (principal)

Signature of the authorized representative

6.2. Certificate request paper form (sample)

A sample of the certificate request paper form that must be signed and presented by the trusted courier during face-to-face registration at RAO can be found here:

TACHOnet certificate request paper form

I, *[name and address of the organisation representative]*, certifies that the following information are to be used in the context of the request, generation and retrieval of public key digital certificates for TACHOnet access points supporting the confidentiality, integrity and non-repudiation of the TACHOnet messages:

Please reproduce the certificate data information provided by CEF Support Team acknowledging the completeness of the electronic certificate request, e.g.:

Certificate data	
Country (C)	BE
Organization/company (O)	European Commission
Master domain (OU1)	CEF_eDelivery.europa.eu
Area of responsibility (OU2)	CEF_TACHOnet
Department (OU3)	AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxxx
First name (CN)	
Last name (CN)	GRP:CEF_TACHOnet_AP_PROD_BE_001
E-mail	CEF-EDELIVERY-SUPPORT@ec.europa.eu

Certificate request reference number: *insert reference number (e.g. 776002)*

Identification of the trusted courier proceeding to the face-to-face registration of the request: *please fill in*

Trusted courier #1
Name:
First names:
Mobile phone:
Email:
Passport issuing country:
Passport number:
Passport validity end date:

Place, date, company stamp or seal of the Organisation:

Signature of the authorised representative:

7. Glossary

The key terms used in this Sub-appendix are defined in the CEF Definitions section on the CEF Digital Single Web Portal:

<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Definitions>

The key acronyms used in this Component Offering Description are defined in the CEF Glossary on the CEF Digital Single Web Portal:

<https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?spaceKey=CEFDIGITAL&title=CEF+Glossary>

COMMISSION DECISION (EU) 2018/1927**of 5 December 2018****laying down internal rules concerning the processing of personal data by the European Commission in the field of competition in relation to the provision of information to data subjects and the restriction of certain rights**

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 249(1) thereof,

Whereas:

- (1) The Commission conducts administrative investigations for the purpose of enforcing the competition rules in accordance with the Treaty and secondary legislation as well as international agreements adopted for that purpose. ⁽¹⁾ To that end, it exercises powers of investigation and enforcement (including related operational activities) in the fields of antitrust, merger control and State aid control conferred on the Commission by the relevant Union acts.
- (2) Commission investigations and enforcement activities in the field of competition target undertakings or Member States which are subject to the competition rules of the Treaty, and not natural persons as such. Nevertheless, during competition investigations, personal data within the meaning of Article 3(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council ⁽²⁾ are inevitably processed within the meaning of Article 3(3) of Regulation (EU) 2018/1725. The Commission needs to process such personal data in order to fulfil the tasks assigned to it as the public authority enforcing Union competition rules. Investigation in the field of antitrust, merger control and State aid control, and enforcement of competition rules constitute monitoring, inspection or regulatory functions connected to the exercise of official authority in the cases referred to in Article 25(1)(c) and (g) of Regulation (EU) 2018/1725. Those activities serve the promotion and protection of a competitive internal market, thereby safeguarding an important economic and financial interest of the Union and of the Member States.
- (3) For the purpose of its investigation and enforcement activities in the fields of antitrust, merger control and State aid control, the Commission processes personal data acquired or received from legal persons, natural persons, Member States and other entities (such as National Competition Authorities, regulatory bodies and other public bodies and authorities), competition authorities of third countries and international bodies and organisations. During competition investigations and enforcement activities, whether acting on its own initiative or on the basis of received input, the Commission may also process personal data acquired or received from publicly available sources (for example, in the context of market monitoring or screening activities), from anonymous sources (for example, whistle-blowers/informants) or identified sources (for example, complainants) that require protection of their identity.
- (4) The Commission may, in turn, transmit personal data to legal or natural persons (for example, in the context of the access to file procedure), to National Competition Authorities and other authorities and bodies in the context of bilateral or multilateral cooperation with Member States or third country authorities and organisations, as necessary and appropriate to exercise its powers, to safeguard the rights of defence of parties subject to Commission proceedings and to ensure the efficient and effective application of Union competition rules.
- (5) Personal data processing activities, within the meaning of Article 3(3) of Regulation (EU) 2018/1725, carried out in the course of investigation and enforcement activities in the field of competition, may take place even before the Commission formally initiates proceedings, continue throughout the handling of the investigation and may continue even after the formal closure of the investigation (for example, for the purposes of market or compliance monitoring or screening activities, assessing the need for initiating new investigative activities, legal proceedings, etc.).

⁽¹⁾ See in particular for antitrust Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty (OJ L 1, 4.1.2003, p. 1), for merger control Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation) (OJ L 24, 29.1.2004, p. 1) and for State aid Council Regulation (EU) 2015/1589 of 13 July 2015 laying down detailed rules for the application of Article 108 of the Treaty on the Functioning of the European Union (OJ L 248, 24.9.2015, p. 9).

⁽²⁾ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39). Processing within the meaning of Article 3(3) of Regulation (EU) 2018/1725 also includes a situation where the Commission receives personal data voluntarily submitted to it.

- (6) The personal data processed by the Commission are, for example, identification data, contact data, professional data and data related to or brought in connection with the subject matter of the investigation or procedure. The personal data are stored in a secured electronic environment to prevent unlawful access or transfer of data to persons who do not have a need to know. The personal data are retained in the services of the Commission in charge of the investigation for the time necessary for the investigation, for assessing the need to initiate new investigative activities, during the administrative procedure, and throughout any subsequent judicial review proceedings, and the administrative retention period that follows the definitive closure of the file. At the end of the retention period, the case related information including personal data is transferred to the historical archives of the Commission ⁽¹⁾.
- (7) While carrying out its tasks, the Commission is bound to respect the rights of natural persons in relation to the processing of personal data recognised by Article 8(1) of the Charter of Fundamental Rights of the European Union and by Article 16(1) of the Treaty. At the same time, the Commission is responsible for enforcing competition rules, which requires the Commission to conduct investigations in a timely manner, while respecting rules of confidentiality and professional secrecy ⁽²⁾ as well as the rights of defence of parties subject to its investigations, ⁽³⁾ and the rights of individuals that require protection of their identity.
- (8) In certain circumstances, it is necessary to reconcile the rights of data subjects pursuant to Regulation (EU) 2018/1725 with the needs of investigations and enforcement activities, as well as with full respect for fundamental rights and freedoms of other data subjects. To that effect, Article 25 of Regulation (EU) 2018/1725 provides the Commission with the possibility to restrict the application of Articles 14 to 22 and 35, as well as Article 4 thereof, insofar as its provisions correspond to the rights and obligations provided for in Articles 14 to 22 of that Regulation.
- (9) These internal rules should cover all processing operations carried out by the Commission in the performance of its powers of investigation, whether acting on its own initiative or on the basis of received input, and enforcement and related operational activities in the fields of antitrust, merger control and State aid control whenever the exercise of data subjects' rights may jeopardise the conduct of investigations or enforcement activities. These rules should apply to processing operations carried out prior to the formal initiation of proceedings, during the handling of investigations as well as after the formal closure of investigations, including processing in the context of bilateral or multilateral cooperation with National Competition Authorities, Member States or third country authorities and organisations.
- (10) In order to comply with Articles 14, 15 and 16 of Regulation (EU) 2018/1725, the Commission should inform all individuals of its activities involving processing of their personal data and of their rights in a transparent and coherent manner in the form of the data protection notices published on the Commission's website.
- (11) Without prejudice to Articles 14(5) and 16(5) of Regulation (EU) 2018/1725, the Commission is also able on the basis of Article 25 of that Regulation to restrict the provision of information to data subjects and the application of other rights of data subjects in order to protect its own competition investigations and enforcement of competition rules, investigations and proceedings of competition authorities of the Member States, the investigation tools and methods, as well as the rights of other persons related to its investigations.
- (12) In addition, in order to maintain effective cooperation it may be necessary for the Commission to restrict the application of data subjects' rights in order to protect processing operations of other Union institutions, bodies, offices and agencies or of Member States' authorities. To that effect, the Commission should consult those services, institutions, bodies, offices, agencies, and authorities on the relevant grounds for imposing restrictions and the necessity and proportionality of the restrictions.

⁽¹⁾ Retention of files in the Commission is regulated by the Common retention list, a regulatory document (the last version is SEC(2012)713) in the form of a retention schedule that establishes the retention periods for the different types of Commission files.

⁽²⁾ See, in particular, Article 339 of the Treaty, as well as Article 28 of Regulation (EC) No 1/2003; Article 15(4) of Commission Regulation (EC) No 773/2004 of 7 April 2004 relating to the conduct of proceedings by the Commission pursuant to Articles 81 and 82 of the EC Treaty (OJ L 123, 27.4.2004, p. 18); Article 17 of Regulation (EC) No 139/2004 and Article 18 of Commission Regulation (EC) No 802/2004 of 21 April 2004 implementing Council Regulation (EC) No 139/2004 on the control of concentrations between undertakings (OJ L 133, 30.4.2004, p. 1); Articles 30 and 31 of Regulation (EU) 2015/1589; required declarations on confidential information in State aid notification forms as annexes to Regulation (EC) No 794/2004 in its amended form.

⁽³⁾ Implementation of the rights of data subjects under the Regulation (EU) 2018/1725 and compliance with the obligations of data controllers under that Regulation does not affect the Commission's handling of the rights of defence of parties subject to the competition proceedings. The integrity and authenticity of evidence on file collected in the course of competition investigations can therefore not be compromised by modifying documents received or collected in conformity with the applicable procedural rules in the competition field.

- (13) The Commission may also have to restrict the provision of information to data subjects and the application of other rights of data subjects in relation to personal data received from third countries or international organisations, in order to cooperate with those countries or organisation and thus safeguard an important objective of general public interest of the Union. However, in some circumstances the interest or fundamental rights of the data subject may override the interest of international cooperation.
- (14) The Commission has therefore identified the grounds listed in Article 25(1)(c), (g) and (h) of Regulation (EU) 2018/1725 as grounds for restrictions under Article 25 of the Regulation that may be necessary to apply to data processing operations carried out in the framework of the Commission's investigative and enforcement activities in the area of competition, encompassing antitrust, merger control and State aid control.
- (15) The Commission should handle all restrictions in a transparent manner and register each application of restrictions in the corresponding record system.
- (16) Pursuant to Article 25(8) of Regulation (EU) 2018/1725, controllers may defer or refrain from providing information on the reasons for the application of a restriction to the data subject if providing that information would in any way compromise the purpose of the restriction. This is, in particular, the case of restrictions to the rights provided for in Articles 16 and 35 of Regulation (EU) 2018/1725. In order to ensure that the data subject's rights under Articles 16 and 35 of Regulation (EU) 2018/1725 are restricted only as long as the reasons for the restriction last, the Commission should review its position regularly and at the closure of the relevant investigation.
- (17) Where a restriction of other rights of data subjects is applied, the controller should assess on a case-by-case basis whether the communication of the restriction would compromise its purpose. The controller is the service in charge of the competition policy within the Commission.
- (18) The Data Protection Officer of the Commission should carry out an independent review of the application of restrictions, with a view to ensuring compliance with this Decision.
- (19) This Decision is adopted for the purposes of Article 25 of Regulation (EU) 2018/1725 and should enter into force at the same time as that Regulation in order to ensure legal certainty.
- (20) The European Data Protection Supervisor has been consulted.

HAS ADOPTED THIS DECISION:

Article 1

Subject-matter and scope

1. This Decision lays down the rules to be followed by the Commission to inform data subjects of the processing of their data in accordance with Articles 14, 15 and 16 of Regulation (EU) 2018/1725, in the framework of its activities in the field of competition.

It also lays down the conditions under which the Commission may restrict the application of Articles 4, 14 to 17, 19, 20 and 35 of Regulation (EU) 2018/1725, in accordance with Article 25 thereof.

2. This Decision applies to the processing of personal data by the Commission for the purpose of or in relation to the activities carried out in order to fulfil its tasks pursuant to Articles 101 to 109 of the Treaty.

Article 2

Applicable exceptions and restrictions

1. Where the Commission exercises its duties with respect to the data subjects' rights pursuant to Regulation (EU) 2018/1725, it shall consider whether any of the exceptions laid down in that Regulation apply.

2. Subject to Articles 3 to 7 of this Decision, the Commission may restrict the application of Articles 14 to 17, 19, 20 and 35 of Regulation (EU) 2018/1725, as well as the principle of transparency laid down in Article 4(1)(a) in so far as its provisions correspond to the right and obligations provided for in Articles 14 to 17, 19, 20 and 35 of the Regulation (EU) 2018/1725 where the exercise of those rights and obligations would jeopardise the purpose of the Commission's investigative and enforcement activities, including by revealing its investigative tools and methods, or would adversely affect the rights and freedoms of other data subjects.

3. Subject to Articles 3 to 7, the Commission may restrict the rights and obligations referred to in paragraph 2 of this Article in relation to personal data obtained from other Union institutions, bodies, agencies and offices, competent authorities of Member States or third countries or from international organisations, in the following circumstances:

- (a) where the exercise of those rights and obligations could be restricted by other Union institutions, bodies, agencies and offices on the basis of other acts provided for in Article 25 of Regulation (EU) 2018/1725 or in accordance with Chapter IX of that Regulation or in accordance with Regulation (EU) 2016/794 of the European Parliament and of the Council ⁽¹⁾ or Council Regulation (EU) 2017/1939 ⁽²⁾;
- (b) where the exercise of those rights and obligations could be restricted by competent authorities of Member States on the basis of acts referred to in Article 23 of Regulation (EU) 2016/679 of the European Parliament and of the Council ⁽³⁾, or under national measures transposing Articles 13(3), 15(3) or 16(3) of Directive (EU) 2016/680 of the European Parliament and of the Council ⁽⁴⁾;
- (c) where the exercise of those rights and obligations could jeopardise the Commission's cooperation with third countries or international organisations in the conduct of competition investigations or enforcement of competition decisions.

Before applying restrictions in the circumstances referred to in points (a) and (b) of the first subparagraph, the Commission shall consult the relevant Union institutions, bodies, agencies, offices or competent authorities of the Member States unless it is clear to the Commission that the application of a restriction is provided for by one of the acts referred to in those points.

Point (c) of the first subparagraph shall not apply where the interest of the Commission to cooperate with third countries or international organisation is overridden by the interests or fundamental rights and freedom of the data subjects.

4. Paragraphs 1, 2 and 3 are without prejudice to the application of other Commission decisions laying down internal rules concerning the provision of information to data subjects and the restriction of certain rights under Article 25 of Regulation (EU) 2018/1725 and to Article 23 of the Rules of Procedure of the Commission.

Article 3

Provision of information to data subjects

1. The Commission shall publish on its website data protection notices that inform all data subjects of its activities involving processing of their personal data.

2. Without prejudice to Articles 14(5) and 16(5) of Regulation (EU) 2018/1725, where the Commission restricts, wholly or partly, the provision of information to data subjects, whose data are processed for purposes of competition investigation or enforcement (including related operational activities) it shall record and register the reasons for the restriction in accordance with Article 6.

Article 4

Right of access by data subject, right of erasure and to restriction of processing

1. Where the Commission restricts, wholly or partly, the right of access to data by data subjects, the right of erasure, or the right to restriction of processing as referred to in Articles 17, 19 and 20 respectively of Regulation (EU) 2018/1725 it shall inform the data subject concerned, in its reply to the request for access, erasure or restriction of processing, of the restriction applied and of the principal reasons thereof, and of the possibility of lodging a complaint with the European Data Protection Supervisor or of seeking a judicial remedy in the Court of Justice of the European Union.

⁽¹⁾ Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

⁽²⁾ Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO') (OJ L 283, 31.10.2017, p. 1).

⁽³⁾ 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) (OJ L 119, 4.5.2016, p. 1).

⁽⁴⁾ Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

2. The provision of information concerning the reasons for the restriction referred to in paragraph 1 may be omitted for as long as it would undermine the purpose of the restriction.
3. The Commission shall record and register the reasons for the restriction in accordance with Article 6.
4. Where the right of access is wholly or partly restricted, the data subject shall exercise his or her right of access through the intermediary of the European Data Protection Supervisor, in accordance with paragraphs 6, 7 and 8 of Article 25 of the Regulation (EU) 2018/1725.

Article 5

Communication of personal data breaches to data subjects

Where the Commission restricts the communication of a personal data breach to the data subject, as referred to in Article 35 of Regulation (EU) 2018/1725, it shall record and register the reasons for the restriction in accordance with Article 6 of this Decision.

Article 6

Recording and registering of restrictions

1. The Commission shall record the reasons for any restriction applied pursuant to this Decision, including an assessment of the necessity and proportionality of the restriction.
2. To that end, the record shall state how the exercise of the right would jeopardise the purpose of the Commission's investigation and enforcement activities, or of restrictions applied pursuant to Article 2(2) or (3), or would adversely affect the rights and freedoms of other data subjects.
3. The record and, where applicable, the documents containing underlying factual and legal elements shall be registered. They shall be made available to the European Data Protection Supervisor on request.

Article 7

Duration of restrictions

1. Restrictions referred to in Articles 3, 4 and 5 shall continue to apply as long as the reasons justifying them remain applicable.
2. Where the reasons for a restriction referred to in Article 3 or 5 no longer apply, the Commission shall lift the restriction and provide the reasons for the restriction to the data subject. At the same time, the Commission shall inform the data subject of the possibility of lodging a complaint with the European Data Protection Supervisor at any time or of seeking a judicial remedy in the Court of Justice of the European Union.
3. The Commission shall review the application of the restrictions referred to in Articles 3 and 5 every year and at the closure of the relevant investigation.

Article 8

Review by the Data Protection Officer

1. The Data Protection Officer shall be informed, without undue delay, whenever data subjects' rights are restricted in accordance with this Decision. Upon request, the Data Protection Officer shall be provided with access to the record and any documents containing underlying factual and legal elements.
2. The Data Protection Officer may request a review of the restriction. The Data Protection Officer shall be informed about the outcome of the requested review.

*Article 9***Entry into force**

This Decision shall enter into force on the date of entry into force of Regulation (EU) 2018/1725.

Done at Brussels, 5 December 2018.

For the Commission

The President

Jean-Claude JUNCKER

COMMISSION IMPLEMENTING DECISION (EU) 2018/1928**of 6 December 2018****granting a derogation requested by Denmark pursuant to Council Directive 91/676/EEC concerning the protection of waters against pollution caused by nitrates from agricultural sources***(notified under document C(2018) 8081)***(Only the Danish text is authentic)**

THE EUROPEAN COMMISSION,

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

Having regard to Council Directive 91/676/EEC of 12 December 1991 concerning the protection of waters against pollution caused by nitrates from agricultural sources ⁽¹⁾, and in particular the third subparagraph of paragraph 2 of Annex III thereof,

Whereas:

- (1) On 18 November 2002, the Commission adopted Decision 2002/915/EC ⁽²⁾ granting a derogation requested by Denmark pursuant to Directive 91/676/EEC concerning the protection of waters against pollution caused by nitrates from agricultural sources, allowing the application of livestock manure containing up to 230 kg nitrogen per hectare per year on certain cattle holdings within the framework of the Danish action programme 1999 to 2003. The derogation was extended by Commission Decision 2005/294/EC ⁽³⁾ in connection with the Danish action programme 2004 to 2007, by Commission Decision 2008/664/EC ⁽⁴⁾ in connection with the Danish action programme 2008-2012, by Commission Implementing Decision 2012/659/EU ⁽⁵⁾ in connection with the Danish action programme 2008 to 2015 and by Commission Implementing Decision (EU) 2017/847 ⁽⁶⁾ in connection with the Danish regulation of nutrients in agriculture and the Danish nitrates action programme of June 2017.
- (2) The derogation granted by Implementing Decision (EU) 2017/847 concerned for the period 2015/2016 approximately 1 466 cattle holdings, 443 134 livestock units and 210 061 hectares of arable land, corresponding respectively to 4,2 % of the total number of holdings, 19,6 % of the total livestock units and 8,6 % of the total arable area in Denmark.
- (3) On 6 February 2018, Denmark submitted a request to the Commission for renewal of the derogation under the third subparagraph of paragraph 2 of Annex III to Directive 91/676/EEC.
- (4) Denmark has an action programme covering the period 2017 to 2020, in conformity with Article 5 of Directive 91/676/EEC, by means of parts of Order on commercial livestock, livestock manure, silage, etc. No 865 of 23 June 2017 as amended, Consolidated Act on agricultural use of fertiliser and on plant cover No 433 of 3 May 2017 as amended and Order No 963 of 12 July 2017 on agricultural use of fertiliser in the planning period 2017/2018. As supplement to those measures, Denmark performs a targeted catch crop scheme in 2017 and 2018 and targeted regulation from 2019 pursuant to Act on agricultural use of fertiliser and on plant cover. In addition, Danish legislation includes a general phosphorus regulation, according to Act on livestock husbandry and use of fertiliser and Order on commercial livestock, livestock manure, silage, etc.

⁽¹⁾ OJ L 375, 31.12.1991, p. 1.⁽²⁾ Commission Decision 2002/915/EC of 18 November 2002 concerning a request for derogation under paragraph 2(b) of Annex III to and Article 9 of Council Directive 91/676/EEC concerning protection of waters against pollution caused by nitrates from agricultural sources (OJ L 319, 23.11.2002, p. 24).⁽³⁾ Commission Decision 2005/294/EC of 5 April 2005 concerning a request for derogation under point 2(b) of Annex III to and Article 9 of Council Directive 91/676/EEC concerning the protection of waters against pollution caused by nitrates from agricultural sources (OJ L 94, 13.4.2005, p. 34).⁽⁴⁾ Commission Decision 2008/664/EC of 8 August 2008 amending Decision 2005/294/EC concerning a request for derogation under point 2(b) of Annex III to and Article 9 of Council Directive 91/676/EEC concerning the protection of waters against pollution caused by nitrates from agricultural sources (OJ L 217, 13.8.2008, p. 16).⁽⁵⁾ Commission Implementing Decision 2012/659/EU of 23 October 2012 on granting a derogation requested by the Kingdom of Denmark pursuant to Council Directive 91/676/EEC concerning the protection of waters against pollution caused by nitrates from agricultural sources (OJ L 295, 25.10.2012, p. 20).⁽⁶⁾ Commission Implementing Decision (EU) 2017/847 of 16 May 2017 granting a derogation requested by Denmark pursuant to Council Directive 91/676/EEC concerning the protection of waters against pollution caused by nitrates from agricultural sources (OJ L 125, 18.5.2017, p. 35).

- (5) The Danish legislation implementing Directive 91/676/EEC includes limits for the application of nitrogen. Legislation limiting the application of phosphorus has entered into force in August 2017.
- (6) The Danish legislation includes a combined targeted scheme for voluntary and mandatory catch crops for the period covered by this Decision. Under that scheme, the obligatory provisions for catch crops are to enter into force automatically if the voluntary agreements for catch crops fail to fulfil the environmental objectives. The areas under catch crops are in addition to the national requirement for mandatory catch crops pursuant to the Danish Act No 433 of 3 May 2017 on agricultural use of fertiliser and on plant cover. The abovementioned scheme is necessary to ensure that the application of the current derogation would not lead to deterioration of water quality.
- (7) The information provided by Denmark in the context of the derogation granted by Implementing Decision (EU) 2017/847 shows that the derogation is not leading to a deterioration of water quality as compared to areas not encompassed by the derogation. Data on the implementation of Directive 91/676/EEC for the period 2012 to 2015 ⁽¹⁾ show that for groundwater 83,4 % of the monitoring sites have mean nitrate concentrations below 50 mg/l, and 27,5 % below 25 mg/l. For fresh surface water, 99,4 % of the monitoring sites have mean nitrate concentrations below 50 mg/l and 85,8 % of monitoring sites below 25 mg/l. Monitoring data show an overall stable trend in nitrate concentration in groundwater and fresh surface water as compared to the previous reporting period (2008 to 2011). Data on eutrophication show that that 25 % of monitored lakes were classified as high/good status and 75 % as less than good status and that 2 out of 119 monitored estuarine/coastal water bodies were classified in a good status.
- (8) The Commission, after examination of Denmark's request on the basis of the elements described in the third subparagraph of paragraph 2 of Annex III of Directive 91/676/EEC and in the light of the experience gained from the derogation as provided for in Decisions 2002/915/EC, 2005/294/EC, 2008/664/EC and Implementing Decision 2012/659/EU, considers that the amount of manure envisaged by Denmark, 230 kg nitrogen per hectare per year, will not prejudice the achievement of the objectives of Directive 91/676/EEC, subject to certain strict conditions as regards catch crops, phosphorus ceilings, crop rotation, application of manure and other fertilisers, soil sampling and analyses being met.
- (9) In farms authorised to apply livestock manure containing up to 230 kg nitrogen per hectare per year, fertilisation plans should be updated in a timely manner to ensure consistency with actual agricultural practices and permanent vegetal cover of arable area and catch crops should be used to ensure recovering subsoil autumn losses of nitrates and limit nitrogen winter losses.
- (10) Directive 2000/60/EC of the European Parliament and the Council ⁽²⁾ provides for a comprehensive, cross-border approach to water protection organised around river basin districts, with the objective of achieving a good status for European bodies of water by 2015. Reducing nutrients is an integral part of that objective. The granting of a derogation under this Decision is without prejudice to the provisions pursuant to Directive 2000/60/EC and does not exclude that additional measures may be needed to fulfil obligations derived from it.
- (11) Directive 2007/2/EC of the European Parliament and of the Council ⁽³⁾ lays down general rules aimed at the establishment of the Infrastructure for Spatial Information in the Union for the purposes of environmental policies of the Union and policies or activities which may have an impact on the environment. Where applicable, the spatial information collected in the context of this Decision should be in line with the provisions set out in that Directive. In order to reduce the administrative burden and enhance data coherence, Denmark, when collecting the necessary data under this Decision should make use of the information generated under the Integrated Administration and Control System established pursuant to Chapter II of Title V of Regulation (EU) No 1306/2013 of the European Parliament and of the Council ⁽⁴⁾.

⁽¹⁾ SWD(2018) 246 final — Commission Staff Working Document accompanying the document Report from the Commission to the Council and the European Parliament on the implementation of Council Directive 91/676/EEC concerning the protection of waters against pollution caused by nitrates from agricultural sources based on Member State reports for the period 2012-2015.

⁽²⁾ Directive 2000/60/EC of the European Parliament and of the Council of 23 October 2000 establishing a framework for Community action in the field of water policy (OJ L 327, 22.12.2000, p. 1).

⁽³⁾ Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE) (OJ L 108, 25.4.2007, p. 1).

⁽⁴⁾ Regulation (EU) No 1306/2013 of the European Parliament and of the Council of 17 December 2013 on the financing, management and monitoring of the common agricultural policy and repealing Council Regulations (EEC) No 352/78, (EC) No 165/94, (EC) No 2799/98, (EC) No 814/2000, (EC) No 1290/2005 and (EC) No 485/2008 (OJ L 347, 20.12.2013, p. 549).

- (12) The measures provided for in this Decision are in accordance with the opinion of the Nitrates Committee set up pursuant to Article 9 of Directive 91/676/EEC,

HAS ADOPTED THIS DECISION:

Article 1

Derogation

The derogation requested by Denmark by letter of 6 February 2018, for the purpose of allowing application to the land of a higher amount of nitrogen from livestock manure than that provided for in the first sentence of the second subparagraph of paragraph 2 of Annex III to Directive 91/676/EEC, is granted subject to the conditions laid down in this Decision.

Article 2

Scope

This derogation applies to cattle farms on which the crop rotation includes more than 80 % of crops with high nitrogen uptake and long growing season and for which an authorisation has been granted in accordance with Article 6.

Article 3

Definitions

For the purposes of this Decision, the following definitions shall apply:

- (a) 'cattle farm' means a holding with a yearly production of nitrogen in livestock manure above 300 kg of which at least two thirds are from cattle;
- (b) 'crops being undersown by grass' means silage cereals, silage maize, spring cereals, winter cereals or spring barley and pea, to be undersown by grass before or after harvest;
- (c) 'crops with high nitrogen uptake and long growing season' means any of the following:
 - (i) grass;
 - (ii) grass catch crops;
 - (iii) forage beets;
 - (iv) crops being undersown by grass;
 - (v) chicory;
- (d) 'grass' means permanent or temporary grassland;
- (e) 'soil profile' means the soil layer below ground level to a depth of 0,90 m or to the average highest groundwater level where that level is less than 0,90 m below ground level;

Article 4

Conditions for the derogation

The derogation is granted on the following conditions:

- (1) As of 1 August 2017, Order No 865 of 23 June 2017 on commercial livestock, livestock manure, silage, etc. has entered into force establishing direct phosphorus ceilings at different levels throughout the country depending on fertiliser type. Ceilings cover application of phosphorus from all types of fertilisers: organic fertilisers, including manure, biogas digestate, degassed plant biomass, sludge from sewage water treatment as well as industrial fertilisers. Stricter phosphorus application ceilings shall be applied in certain catchments having a phosphorus vulnerable aquatic environment.
- (2) An indicator and monitoring system shall be in place for the amount of phosphorus applied on agricultural fields in Denmark. Where either the indicator system or the monitoring system shows that the actual annual average phosphorus fertilisation rate on agricultural soils in Denmark might exceed or has actually exceeded the levels of average national phosphorus fertilisation allowed to be reached over the period 2018 to 2025, the ceilings for maximum phosphorus application shall be reduced accordingly.

- (3) As of 5 April 2017, Danish Act No 310 of 4 April 2017 amending the Act on agricultural use of fertiliser and plant cover (Requirement to establish targeted catch crops) has entered into force establishing a combined targeted scheme for voluntary and mandatory catch crops based on the need to reduce nitrates contents in groundwater bodies and in coastal waters. Under the scheme, the obligatory provisions for catch crops shall enter into force automatically if the voluntary agreements for catch crops fail to deliver the sufficient environmental objectives. According to Act No 497 of 22 May 2018 amending Act on agricultural use of fertiliser and on plant cover (Targeted nitrates regulation etc.), catch crops may be substituted by specified alternative measures under the scheme.
- (4) The catch crops established under that scheme shall be additional to the catch crops planted in order to fulfil the national mandatory requirement of 10 or 14 % catch crops on the farm's crop ground area, and may not be established in the same area as that used to meet the Ecological Focus Area requirement for catch crops.

Article 5

Applications for authorisation

1. Cattle farmers may submit an application for an annual authorisation to apply livestock manure containing up to 230 kg nitrogen per hectare per planning period to the competent authorities.

The time limit for submitting the application shall be the same as the national time limit for applying for Basic Payment of the CAP and for submitting the fertiliser quota and catch crops plan.

2. The submission of an application as referred to in paragraph 1 shall be considered to imply a declaration by the applicant that the conditions in Articles 7 and 8 and 9 are fulfilled.

Article 6

The granting of authorisations

Authorisations to apply an amount of manure from the cattle farm, including manure excreted by the animals themselves and treated manure, containing up to 230 kg nitrogen per hectare land each planning period shall be granted subject to the conditions laid down in Articles 7, 8 and 9.

Article 7

Conditions regarding application of manure and other fertilisers

1. The total nitrogen input shall not exceed the foreseeable nutrient demand of the crop, taking into account the nutrient supply from the soil. It shall not exceed maximum application standards, as laid down in Order on agricultural use of fertiliser in the planning period 2017/2018 No 963 (12 July 2017), and in corresponding orders in the following planning periods.
2. A fertilisation plan shall be prepared for the whole acreage of the cattle farm. The plan shall be kept on the farm. It shall cover the period from 1 August to 31 July the following year. The fertilisation plan shall include the following:
 - (a) a crop rotation plan specifying the following:
 - (i) the acreage of parcels with crops with high nitrogen uptake and long growing season;
 - (ii) the acreage of parcels with other crops than those mentioned in point (i);
 - (iii) a sketch map indicating the location of the parcels referred to in points (i) and (ii) respectively;
 - (b) the number of livestock on the farm, a description of the housing and manure storage system, including the volume of manure storage available;
 - (c) a calculation of the manure nitrogen and phosphorus produced on the farm;
 - (d) a description of manure treatment, where applicable, and expected characteristics of the treated manure;
 - (e) the amount, type and characteristics of manure delivered outside the farm or to the farm;
 - (f) the foreseeable amount of nitrogen and phosphorus required for the crop in each parcel;
 - (g) a calculation of nitrogen and phosphorus application from manure for each parcel;

- (h) a calculation of nitrogen and phosphorus application from chemical and other fertilisers for each parcel;
- (i) an indication of the time of application of manure and chemical fertilisers.

The fertilisation plan shall be revised no later than seven days following any change in agricultural practices at the cattle farm. The fertilisation account shall be submitted to the competent authorities by the end of March each year at the latest.

- 3. Manure shall not be spread in the period from 31 August to 1 March on grassland which will be ploughed the following spring.

Article 8

Conditions regarding soil sampling and analyses

- 1. Samples shall be taken from the upper 30 cm of the farmland soil and analysed for their content of nitrogen and phosphorus.
- 2. The sampling and analyses shall be carried out at least once every four years for each area of the cattle farm presenting homogeneous features with regard to crop rotation and soil characteristics.
- 3. At least one sampling and analysis shall be carried out for each five hectares of farmland.
- 4. The results of the analyses shall be available for inspection at the cattle farm.

Article 9

Conditions regarding land management

- 1. 80 % or more of the acreage available for manure application shall be cultivated with crops with high nitrogen uptake and long growing season.
- 2. Grass catch crops shall not be ploughed before 1 March the year after they have been established.
- 3. Temporary grasslands shall be ploughed in spring. A crop with high nitrogen uptake and long growing season shall be seeded as soon as possible, and no later than 3 weeks, after grass has been ploughed.
- 4. Crops used in crop rotation shall not include leguminous plants or other plants fixing atmospheric nitrogen, except for the following:
 - (a) clover in grassland with less than 50 % clover and alfalfa;
 - (b) alfalfa in grassland with less than 50 % clover and alfalfa;
 - (c) barley and pea undersown with grass;
- 5. Nitrogen fertilisations standards for crops following temporary grassland shall be reduced by the previous crop nitrogen value according to Order on agricultural use of fertiliser in the planning period 2017/2018 No 963 (12 July 2017), and in corresponding orders in the subsequent planning periods regarding fertilisation standards, table on fertilisation norms for agricultural crops and vegetables, and subsequent changes.

Article 10

Monitoring

- 1. The competent authorities shall ensure that maps are drawn up showing the following:
 - (a) the percentage of the cattle farms in each municipality which are covered by authorisations;
 - (b) the percentage of the livestock in each municipality which is covered by authorisations;
 - (c) the percentage of the agricultural land in each municipality which is covered by authorisations;

Those maps shall be updated every year.

Data on crop rotations and agricultural practices on cattle farms covered by authorisations under this Decision shall be collected by the competent authorities. Those data shall be updated every year.

- 2. The competent authorities shall monitor root zone water, surface waters and groundwater and shall provide the Commission with data on nitrogen and phosphorus in the soil profile and nitrates concentrations in surface and groundwater, both under derogation and non-derogation conditions.

The monitoring shall be carried out at farm field scale in the agricultural catchment national monitoring programme. The monitoring sites shall be representative of the main soil types, the prevalent fertilisation practices and the main crops.

Reinforced monitoring of water quality shall be carried out in areas with sandy soils. In addition, nitrates concentrations in surface and groundwater shall be monitored in at least 3 % of all holdings covered by an authorisation.

3. The competent authorities shall carry out surveys and continuous nutrient analyses in the agricultural catchment national monitoring programme and shall provide data on local land use, crop rotations and agricultural practices on cattle farms benefiting from an authorisation.

Information and data collected from nutrient analysis as referred to in Article 7 and from monitoring as referred to in paragraph 2 of this Article shall be used for model-based calculations of nitrogen and phosphorus losses from cattle farms benefitting from an authorisation based on scientific principles.

4. The competent authorities shall quantify and record the percentages of the land under derogation which is covered by:

- (a) clover or alfalfa in grassland;
- (b) barley and pea undersown with grass.

Article 11

Verification

1. The competent authorities shall ensure that applications for authorisation are submitted to administrative control. Where the control demonstrates that the conditions laid down in Articles 7, 8 and 9 are not fulfilled by the applicant, the application shall be refused, and the applicant shall be informed of the reasons for refusal.

2. The competent authorities shall establish a programme for inspections of farms benefiting from authorisations.

The programme shall be based on risk analysis having regard to the results of controls of the previous years concerning the conditions laid down in Articles 7, 8 and 9 and the results of controls of compliance with national legislation transposing Directive 91/676/EEC.

3. The inspections shall consist of field inspections and on the spot control for compliance with the conditions set out in Articles 7, 8 and 9 and shall cover annually at least 7 % of the cattle farms benefiting from an authorisation. Where a cattle farm is found not to comply with those conditions, the holder of the authorisation shall be fined in accordance with national law and shall not be eligible for an authorisation the subsequent planning period.

4. The competent authorities shall be granted the necessary powers and means to verify compliance with the conditions of the derogation granted under this Decision.

Article 12

Reporting

The competent authorities shall, every year by 31 December at the latest, submit a report to the Commission containing the following information:

- (a) maps showing the percentage of cattle farms, percentage of livestock, percentage of agricultural land covered by individual derogations for each municipality, as well as maps on local land use, referred to in Article 10(1);
- (b) the results of ground and surface water monitoring, as regards nitrates and phosphorus concentrations, including information on water quality trends, both under derogation and non-derogation conditions, as well as the impact of derogation on water quality, as referred to in Article 10(2);
- (c) the results of soil monitoring as regards nitrogen and phosphorus concentrations in the root zone water, both under derogation and non-derogation conditions, as referred to in Article 10(2);
- (d) results of the surveys on local land use, crop rotations and agricultural practices, referred to in Article 10(3);
- (e) results of model-based calculations of the magnitude of nitrogen and phosphorus losses from cattle farms benefiting from an authorisation, referred to in Article 10(3);

- (f) tables showing the percentage of agricultural land under derogation covered by clover or alfalfa in grassland and by barley/pea undersown with grass, referred to in Article 10(4);
- (g) evaluation of the implementation of the derogation conditions, on the basis of controls at farm level and information on non-compliant cattle farms, on the basis of the results of the administrative control and inspections, referred to in Article 11;
- (h) trends in livestock numbers and manure production for each livestock category in Denmark and in cattle farms benefitting from the derogation.
- (i) the implementation of the conditions for the derogation set in Article 4.

The spatial data contained in the report shall, where applicable, comply with Directive 2007/2/EC. In collecting the necessary data, Denmark shall make use, where appropriate, of the information generated under the Integrated Administration and Control System set up in accordance with Article 67(1) of Regulation (EU) No 1306/2013.

Article 13

Period of application

This Decision shall apply until 31 July 2020.

Article 14

Addressee

This Decision is addressed to the Kingdom of Denmark.

Done at Brussels, 6 December 2018.

For the Commission
Karmenu VELLA
Member of the Commission

