

Official Journal of the European Union

L 58



English edition

Legislation

Volume 64

19 February 2021

Contents

I *Legislative acts*

REGULATIONS

- ★ **Regulation (EU) 2021/250 of the European Parliament and of the Council of 16 February 2021 amending Council Regulation (EEC) No 95/93 as regards temporary relief from the slot utilisation rules at Union airports due to the COVID-19 crisis ⁽¹⁾ 1**

II *Non-legislative acts*

REGULATIONS

- ★ **Council Regulation (CFSP) 2021/251 of 18 February 2021 amending Regulation (EC) No 314/2004 concerning restrictive measures in view of the situation in Zimbabwe 9**
- ★ **Commission Implementing Regulation (EU) 2021/252 of 29 January 2021 operating a deduction from the Portuguese fishing quota available for anchovy, on account of overfishing in the previous year 12**
- ★ **Commission Implementing Regulation (EU) 2021/253 of 17 February 2021 amending Council Regulation (EC) No 314/2004 concerning restrictive measures in view of the situation in Zimbabwe 15**
- ★ **Commission Implementing Regulation (EU) 2021/254 of 18 February 2021 amending Implementing Regulations (EU) 2020/761 and (EU) 2020/1988 and Regulations (EC) No 218/2007 and (EC) No 1518/2007 as regards imports of products originating in the United Kingdom and excluding those products from the tariff quotas with ongoing quota periods 17**
- ★ **Commission Implementing Regulation (EU) 2021/255 of 18 February 2021 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security ⁽¹⁾ 23**

⁽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 Implementing Regulation (EU) 2021/256 of 18 February 2021 amending Annex I to Regulation (EC) No 798/2008 as regards the entry for the United Kingdom in the list of third countries, territories, zones or compartments from which certain poultry commodities may be imported into and transit through the Union in relation to highly pathogenic avian influenza ⁽¹⁾ ...** 36

DECISIONS

- ★ **Council Decision (CFSP) 2021/257 of 18 February 2021 in support of the Oslo Action Plan for the implementation of the 1997 Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction** 41
- ★ **Council Decision (CFSP) 2021/258 of 18 February 2021 amending Decision 2011/101/CFSP concerning restrictive measures in view of the situation in Zimbabwe** 51
- ★ **Commission Decision (EU, Euratom) 2021/259 of 10 February 2021 laying down implementing rules on industrial security with regard to classified grants** 55

⁽¹⁾ Text with EEA relevance.

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2021/250 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**of 16 February 2021****amending Council Regulation (EEC) No 95/93 as regards temporary relief from the slot utilisation rules at Union airports due to the COVID-19 crisis****(Text with EEA relevance)**

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 100(2) thereof,

Having regard to the proposal from the European Commission,

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

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

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure ⁽²⁾,

Whereas:

- (1) The COVID-19 crisis has led to a sharp drop in air traffic because of a significant fall in demand and direct measures taken by the Member States and third countries to contain the spread of COVID-19. The impact on air carriers has been detrimental since 1 March 2020, and this is likely to continue in the years to come.
- (2) Those circumstances are beyond the control of air carriers and have led to the voluntary or obligatory cancellation of their air services. In particular, voluntary cancellations protect the financial health of air carriers and avoid the negative environmental impact caused by operating empty or largely-empty flights only to retain their slots.
- (3) Figures published by Eurocontrol, which is the network manager for the air traffic network functions of the single European sky, indicate a continued year-on-year fall in air traffic of around 74 % as of mid-June 2020.
- (4) It is not possible, on the basis of known forward bookings, Eurocontrol forecasts and epidemiological forecasts, to predict when the period of severely depressed demand caused by the COVID-19 crisis is likely to end. According to the latest Eurocontrol forecasts, air traffic in February 2021 will be around half of the level of February 2020. Forecasts extending beyond that date depend on a number of unknown factors, such as the availability of COVID-19 vaccines. Under these circumstances, air carriers that fail to use their slots in accordance with the slot

⁽¹⁾ Opinion of 27 January 2021 (not yet published in the Official Journal).

⁽²⁾ Position of the European Parliament of 11 February 2021 (not yet published in the Official Journal) and decision of the Council of 15 February 2021.

utilisation rate set out in Council Regulation (EEC) No 95/93 ⁽³⁾ should not automatically lose the precedence, in respect of the series of slots, laid down in Articles 8(2) and 10(2) of that Regulation that they might otherwise enjoy. This Regulation should establish specific rules to this effect.

- (5) Those rules should at the same time address potentially negative impacts on air carrier competition. In particular, it is necessary to ensure that air carriers prepared to provide services are allowed to take up unused capacity and that they have the prospect of maintaining such slots in the long term. This should maintain air carriers' incentives to make use of airport capacity, which in turn would benefit consumers.
- (6) It is therefore necessary to lay down, in accordance with these principles and for a limited period, the conditions under which air carriers continue to be entitled to series of slots under Articles 8(2) and 10(2) of Regulation (EEC) No 95/93, and to establish requirements for air carriers concerned to release unused capacity.
- (7) For the period during which air transport is negatively affected by the COVID-19 crisis, the definition of the term 'new entrant' should be broadened in order to increase the number of air carriers covered, thereby giving more air carriers the opportunity to establish and expand their operations if they so wish. However, it is necessary to restrict the privileges corresponding to air carriers covered by that definition to genuine new entrants by excluding any air carrier which, together with its parent company, or with its own subsidiaries or subsidiaries of its parent company, holds more than 10 % of the total number of slots allocated on the day in question in any given airport.
- (8) During the period for which the relief from the slot utilisation rules is applied, the system of slot allocation should recognise the efforts of the air carriers that have operated flights using slots which are part of a series that another air carrier is entitled to under Articles 8(2) and 10(2) of Regulation (EEC) No 95/93, but which have been made available to the slot coordinator for temporary reallocation. Therefore, air carriers that have operated at least five slots of a series should receive priority for the allocation of those series in the next equivalent scheduling period, provided the air carrier entitled to them under those Articles does not request them.
- (9) The imposition of specific COVID-19 sanitary measures at airports may reduce available capacity, which may make it necessary to provide for specific COVID-19 coordination parameters. In such situations, and in order to enable the proper application of such parameters, coordinators should be allowed to adapt the timing of slots allocated to air carriers under Article 8 of Regulation (EEC) No 95/93 or to cancel such slots for the scheduling period during which the specific COVID-19 sanitary measures apply.
- (10) To facilitate the use of airport capacity during the summer 2021 scheduling period, air carriers should be allowed to return historical slots to the coordinator before the beginning of the scheduling period so that they can be reallocated on an ad hoc basis. Air carriers returning a complete series of slots before the deadline set by this Regulation should retain their entitlement for the same series of slots at that airport for the summer 2022 scheduling period. In view of the other slot relief measures contained in this Regulation, air carriers with a significant number of slots at an airport should be allowed to return a maximum of half of their slots in this way.
- (11) Without prejudice to the obligation of Member States to comply with Union law, in particular with the rules laid down in the Treaties and in Regulation (EC) No 1008/2008 of the European Parliament and of the Council ⁽⁴⁾, the negative consequences of possible measures, adopted by public authorities of Member States or third countries addressing the spread of COVID-19 and restricting the ability to travel at very short notice, cannot be imputed to air carriers and should be mitigated where those measures significantly impact the viability or the possibility of travel or the demand on the routes concerned. This should include measures which lead to a partial or total closure of the border or airspace or to a partial or total closure or reduction of capacity of the airports concerned, to restrictions on airline crew movements significantly hampering the operation of air services or to a severe impediment to passengers' ability to travel with any carrier on the route concerned, including travel restrictions, restrictions of movement or quarantine measures in the country or the region of destination or restrictions on the availability of

⁽³⁾ Council Regulation (EEC) No 95/93 of 18 January 1993 on common rules for the allocation of slots at Community airports (OJ L 14, 22.1.1993, p. 1).

⁽⁴⁾ Regulation (EC) No 1008/2008 of the European Parliament and of the Council of 24 September 2008 on common rules for the operation of air services in the Community (OJ L 293, 31.10.2008, p. 3).

services essential to support directly the operation of an air service. Mitigations should ensure that air carriers should not be penalised for failure to use slots where that failure is the result of such restrictive measures which had not yet been published when the slots were allocated. Specific relief from the effects of the imposition of such measures should be of limited duration and, in any event, should not exceed two consecutive scheduling periods.

- (12) During periods where demand is significantly impacted as a result of the COVID-19 crisis, air carriers should be released, to the necessary extent, from the requirements to use slots in order to retain entitlement to those slots in the subsequent equivalent scheduling period. This should enable air carriers to increase services when circumstances allow. The lower minimum usage rate fixed for this purpose should take into account the air traffic outlook for 2021, as of the beginning of 2021, which was 50 % of 2019 traffic levels, the uncertainty surrounding the COVID-19 crisis and the return of consumer confidence and traffic levels.
- (13) In order to address the evolving impact of the COVID-19 crisis and the resulting lack of clarity concerning the evolution of the traffic levels in the mid-term, and to respond flexibly, where strictly necessary and justified, to the challenges the air transport sector is facing as a consequence, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of amending the period of application of the relief from the slot utilisation rule and the percentage values of the minimum usage rate within a certain range. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making ⁽⁵⁾. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.
- (14) In order to be able to make the necessary preparations in time, air carriers and coordinators need to be aware of the conditions to be applied to the operation of slots in a given scheduling period. The Commission should therefore endeavour to adopt the delegated acts as early as possible and should adopt such acts in any event before the deadline for the return of slots laid down in Article 10(3) of Regulation (EEC) No 95/93.
- (15) Airports, airport services providers and air carriers need to have information on available capacity for the purpose of adequate planning. Air carriers should make available to the coordinator for possible reallocation to other air carriers any slot that they do not intend to use at the earliest possible opportunity and no later than three weeks before the planned date of their operation. Where air carriers repeatedly and intentionally fail to comply with that requirement, or with any other requirement of Regulation (EEC) No 95/93, they should be subject to appropriate penalties or equivalent measures.
- (16) Where a coordinator is satisfied that an air carrier has ceased operations at an airport, the coordinator should immediately withdraw the slots from the air carrier in question and place them in the pool for reallocation to other carriers.
- (17) Since the objective of this Regulation, namely the establishment of specific rules and the relief from the general slot utilisation rules for a limited period of time in order to mitigate the effects of the Covid-19 crisis on air traffic, cannot be sufficiently achieved by the Member States but can rather, by reason of the scale and effects of the proposed action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary to achieve that objective.

⁽⁵⁾ OJ L 123, 12.5.2016, p. 1.

- (18) In view of the urgency entailed by the exceptional circumstances related to the COVID-19 crisis, it is considered to be appropriate to provide for an exception to the eight-week period referred to in Article 4 of Protocol No 1 on the role of national Parliaments in the Union, annexed to the Treaty on European Union, to the Treaty on the Functioning of the European Union and to the Treaty establishing the European Atomic Energy Community.
- (19) In order to allow for the prompt application of the measures provided for in this Regulation, it should enter into force as a matter of urgency on the day following that of its publication in the *Official Journal of the European Union*,

HAVE ADOPTED THIS REGULATION:

Article 1

Regulation (EEC) No 95/93 is amended as follows:

(1) Article 2 is amended as follows:

(a) the following point is inserted:

‘(ba) during the period referred to in Article 10a(3) ‘new entrant’ shall mean:

- (i) an air carrier requesting, as part of a series of slots, a slot at an airport on any day, where, if the carrier’s request were accepted, it would in total hold fewer than seven slots at that airport on that day; or
- (ii) an air carrier requesting a series of slots for a non-stop scheduled passenger service between two Union airports, where at most two other air carriers operate the same non-stop scheduled service between those airports on that day, and where, if the air carrier’s request were accepted, the air carrier would nonetheless hold fewer than nine slots at that airport on that day for that non-stop service.

An air carrier which, together with its parent company, its own subsidiaries or the subsidiaries of its parent company, holds more than 10 % of the total slots allocated on the day in question at a particular airport, shall not be considered as a new entrant at that airport;’

(b) the following point is added:

‘(n) ‘COVID-19 coordination parameters’ shall mean revised coordination parameters resulting in a reduction of available airport capacity at a coordinated airport as a result of specific sanitary measures imposed by Member States in response to the COVID-19 crisis.’;

(2) in Article 7(1), the first subparagraph is replaced by the following:

‘1. Air carriers operating or intending to operate at a schedules facilitated or coordinated airport shall submit to the schedules facilitator or coordinator respectively all relevant information requested by them. All relevant information shall be provided in the format and within the time-limit specified by the schedules facilitator or coordinator. In particular, an air carrier shall inform the coordinator, at the time of the request for allocation, whether it would benefit from the status of new entrant, in accordance with Article 2(b) or (ba), in respect of requested slots.’;

(3) Article 8 is amended as follows:

(a) the introductory wording of the first subparagraph of paragraph 2 is replaced by the following:

‘2. Without prejudice to Articles 7, 8a and 9, Article 10(1) and (2a) and Article 14, paragraph 1 of this Article shall not apply when the following conditions are satisfied:’;

- (b) the following paragraph is inserted:

‘2a. During the period referred to in Article 10a(3), a series of slots which was returned to the slot pool in accordance with paragraph 1 of this Article at the end of the scheduling period (the “reference scheduling period”) shall, upon request, be allocated for the next equivalent scheduling period to an air carrier which has operated at least five slots of the series in question following the application of Article 10a(7) during the reference scheduling period, provided that the series of slots has not already been allocated to the carrier originally holding that series for the next equivalent scheduling period in accordance with paragraph 2 of this Article.

In the event that more than one applicant fulfils the requirements of the first subparagraph, priority shall be given to the air carrier that has operated the greater number of slots of that series.’;

- (c) the following paragraph is inserted:

‘6a. Within the period during which COVID-19 coordination parameters apply and in order to enable the proper application of such coordination parameters, the coordinator may amend the timing of requested or allocated slots falling within the period specified in Article 10a(3) or cancel them after having heard the air carrier concerned. In this context, the coordinator shall take into account additional rules and guidelines referred to in paragraph 5 of this Article, under the conditions set out therein.’;

- (4) in Article 8a, paragraph 3 is replaced by the following:

‘3.

- (a) Slots allocated to a new entrant as defined in Article 2(b) or (ba) may not be transferred as provided for in paragraph 1(b) of this Article for a period of two equivalent scheduling periods, except in the case of a legally authorised takeover of the activities of a bankrupt undertaking.
- (b) Slots allocated to a new entrant as defined in Article 2(b)(ii) and (iii) or in Article 2(ba)(ii) may not be transferred to another route as provided for in paragraph 1(a) of this Article for a period of two equivalent scheduling periods unless the new entrant would have been treated with the same priority on the new route as on the initial route.
- (c) Slots allocated to a new entrant as defined in Article 2(b) or (ba) may not be exchanged as provided for in paragraph 1(c) of this Article for a period of two equivalent scheduling periods, except in order to improve the slot timings for these services in relation to the timings initially requested.’;

- (5) Article 10 is amended as follows:

- (a) the following paragraph is inserted:

‘2a. Notwithstanding paragraph 2, a series of slots allocated for the scheduling period from 28 March 2021 until 30 October 2021 shall entitle the air carrier to the same series of slots for the scheduling period from 27 March 2022 until 29 October 2022 if the air carrier has made the complete series of slots available to the coordinator for reallocation before 28 February 2021. This paragraph shall only apply to series of slots which had been allocated to the same carrier for the scheduling period from 29 March 2020 until 24 October 2020. The number of slots in respect of which the air carrier in question may benefit under this paragraph shall be limited to a number equivalent to 50 % of the slots which were allocated to the same carrier for the scheduling period from 29 March 2020 until 24 October 2020 except for an air carrier allocated fewer than 29 slots per week on average during the previous equivalent scheduling period at the airport in question.’;

- (b) paragraph 4 is amended as follows:

- (i) the following point is added:

‘(e) during the period referred to in Article 10a(3), the introduction by public authorities of measures intended to address the spread of COVID-19 at one end of a route for which the slots in question were used or planned to be used, on condition that the measures had not been published at the time the series of slots had been allocated, that those measures significantly impact the viability or possibility of travel or the demand on the routes concerned and that they lead to any of the following:

- (i) a partial or total closure of the border or airspace, or a partial or total closure or reduction of capacity of the airport, during a substantial part of the relevant scheduling period,

- (ii) a severe impediment to passengers' ability to travel with any carrier on that direct route during a substantial part of the relevant scheduling period including,
 - travel restrictions based on nationality or place of residence, prohibition of all except essential travel, or bans on flights from or to certain countries or geographical areas,
 - restrictions of movement or quarantine or isolation measures within the country or region where the airport of destination is located (including intermediate points),
 - restrictions on the availability of services essential to support directly the operation of an air service,
- (iii) restrictions on airline crew movements significantly hampering the operation of air services from or to the airports served, including sudden bans on entry or the stranding of crew in unexpected locations due to quarantine measures.;

(ii) the following subparagraphs are added:

'Point (e) shall apply within the period during which the measures referred to in that point apply and, within the limits referred to in the third, fourth and fifth subparagraphs, for an additional period of up to six weeks. However, where the measures referred to in point (e) cease to apply less than six weeks before the end of a scheduling period, point (e) shall apply to the remainder of the six week period only where the slots in the subsequent scheduling period are used for the same route.

Point (e) shall only apply to slots used for routes for which they were already used by the air carrier prior to the publication of the measures referred to in that point.

Point (e) shall cease to apply where the air carrier uses the slots in question to change to a route not affected by the measures of the public authorities.

Air carriers may justify the non-utilisation of a slot in accordance with point (e) for a maximum of two consecutive scheduling periods.;

(c) the second subparagraph of paragraph 6 is replaced by the following:

'Among requests from new entrants, preference shall be given to air carriers qualifying for new entrant status under Article 2(b)(i) and (ii), Article 2(b)(i) and (iii) or Article 2(ba)(i) and (ii).';

(6) Article 10a is replaced by the following:

'Article 10a

Allocation of slots in response to the COVID-19 crisis

1. For the purposes of Articles 8(2) and 10(2), coordinators shall consider slots allocated for the period from 1 March 2020 until 27 March 2021 as having been operated by the air carrier to which they were initially allocated.

2. For the purposes of Articles 8(2) and 10(2), coordinators shall consider slots allocated for the period from 23 January 2020 until 29 February 2020 as having been operated by the air carrier to which they were initially allocated, as regards air services between airports in the Union and airports either in the People's Republic of China or in the Hong Kong Special Administrative Region of the People's Republic of China.

3. In respect of slots which have not been made available to the coordinator for reallocation in accordance with Article 10(2a), during the period from 28 March 2021 until 30 October 2021 and for the purposes of Articles 8(2) and 10(2), if an air carrier demonstrates to the satisfaction of the coordinator that the series of slots in question has been operated, as cleared by the coordinator, by that air carrier for at least 50 % of the time during the scheduling period for which it has been allocated, the air carrier shall be entitled to the same series of slots for the next equivalent scheduling period.

In respect of the period referred to in the first subparagraph of this paragraph, the percentage values referred to in Article 10(4) and in point (a) of Article 14(6) shall be 50 %.

4. In respect of slots with a date from 9 April 2020 until 27 March 2021, paragraph 1 shall only apply where the air carrier returned the relevant unused slots to the coordinator for reallocation to other air carriers.

5. Where the Commission finds, on the basis of data published by Eurocontrol, which is the network manager for the air traffic network functions of the single European sky, that the reduction in the level of air traffic as compared to the level in the corresponding period in 2019 is persisting and, on the basis of Eurocontrol traffic forecasts, is likely to persist, and also finds, on the basis of the best available scientific data, that this situation is the result of the impact of the COVID-19 crisis, the Commission shall adopt delegated acts in accordance with Article 12a to amend the period specified in paragraph 3 of this Article accordingly.

The Commission is empowered to adopt, where strictly necessary in order to address the evolving impact of the COVID-19 crisis on air traffic levels, delegated acts in accordance with Article 12a to amend the percentage values referred to in paragraph 3 of this Article within a range between 30 % and 70 %. For this purpose, the Commission shall take into account changes that have occurred since 20 February 2021, on the basis of the following elements:

- (a) data published by Eurocontrol on traffic levels and traffic forecasts;
- (b) the evolution of air traffic trends during the scheduling periods, taking into account the evolution observed since the start of the COVID-19 crisis; and
- (c) indicators relating to demand for passenger and cargo air transport, including trends regarding fleet size, fleet utilisation, and load factors.

Delegated acts pursuant to this paragraph shall be adopted no later than 31 December for the following summer scheduling period and no later than 31 July for the following winter scheduling period.

6. Where, in the case of a prolonged impact of the COVID-19 crisis on the air transport sector in the Union, imperative grounds of urgency so require, the procedure provided for in Article 12b shall apply to delegated acts adopted pursuant to this Article.

7. During the period referred to in paragraph 3, air carriers shall make available to the coordinator for reallocation to other air carriers any slot they do not intend to use, no less than three weeks before the date of operation.;

(7) in Article 12a, paragraph 2 is replaced by the following:

‘2. The power to adopt delegated acts referred to in Article 10a shall be conferred on the Commission until 21 February 2022.’;

(8) Article 14 is amended as follows:

(a) Paragraph 5 is replaced by the following:

‘5. Member States shall establish and apply effective, proportionate and dissuasive penalties or equivalent measures to air carriers who repeatedly and intentionally fail to comply with this Regulation.’;

(b) in paragraph 6, the following point is added:

‘(c) During the period referred to Article 10a(3), when a coordinator determines, on the basis of information at its disposal, that an air carrier has ceased its operations at an airport and is no longer able to operate the slots which it has been allocated, the coordinator shall withdraw from that air carrier the series of slots in question for the remainder of the scheduling period and place them in the pool, after having heard the air carrier concerned.’.

Article 2

This Regulation shall enter into force on the 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, 16 February 2021.

For the European Parliament
The President
D. M. SASSOLI

For the Council
The President
A. P. ZACARIAS

II

(Non-legislative acts)

REGULATIONS

COUNCIL REGULATION (CFSP) 2021/251**of 18 February 2021****amending Regulation (EC) No 314/2004 concerning restrictive measures in view of the situation in Zimbabwe**

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 215 thereof,

Having regard to Council Decision (CFSP) 2021/258 of 18 February 2021 amending Decision 2011/101/CFSP concerning restrictive measures in view of the situation in Zimbabwe ⁽¹⁾,

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

Whereas:

- (1) Council Regulation (EC) No 314/2004 ⁽²⁾ gives effect to several measures provided for by Council Decision 2011/101/CFSP ⁽³⁾, including the freezing of funds and economic resources of designated persons and entities in view of the situation in Zimbabwe.
- (2) On 18 February 2021, the Council adopted Decision (CSFP) 2021/258, removing one person from, and amending the entries for two persons on the list of persons and entities subject to restrictive measures as set out in, respectively, Annexes I and II to Decision 2011/101/CFSP.
- (3) On 17 February 2021, Commission Implementing Regulation (EU) 2021/253 ⁽⁴⁾ amended Annex III to Regulation (EC) No 314/2004 accordingly. The removal of a person from the list of persons and entities subject to restrictive measures also requires the removal of the person from Annex IV to Regulation (EC) No 314/2004, listing persons and entities suspended from restrictive measures pursuant to Article 6(4) of that Regulation.
- (4) Annex IV to Regulation (EC) No 314/2004 should be amended accordingly,

HAS ADOPTED THIS REGULATION:

Article 1

Annex IV to Regulation (EC) No 314/2004 is amended as set out in the Annex to this Regulation.

⁽¹⁾ See page 51 of this Official Journal.⁽²⁾ Council Regulation (EC) No 314/2004 of 19 February 2004 concerning certain restrictive measures in respect of Zimbabwe (OJ L 55, 24.2.2004, p. 1).⁽³⁾ Council Decision 2011/101/CFSP of 15 February 2011 concerning restrictive measures against Zimbabwe (OJ L 42, 16.2.2011, p. 6).⁽⁴⁾ See page 15 of this Official Journal.

Article 2

This Regulation shall enter into force on the 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, 18 February 2021.

For the Council
The President
A. P. ZACARIAS

ANNEX

In Annex IV to Regulation (EC) No 314/2004, the following entry is deleted:

‘4. Shiri, Perence (a.k.a Bigboy) Samson Chikerema’.

COMMISSION IMPLEMENTING REGULATION (EU) 2021/252**of 29 January 2021****operating a deduction from the Portuguese fishing quota available for anchovy, on account of overfishing in the previous year**

THE EUROPEAN COMMISSION,

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

Having regard to Council Regulation (EC) No 1224/2009 of 20 November 2009 establishing a Union control system for ensuring compliance with the rules of the common fisheries policy, amending Regulations (EC) No 847/96, (EC) No 2371/2002, (EC) No 811/2004, (EC) No 768/2005, (EC) No 2115/2005, (EC) No 2166/2005, (EC) No 388/2006, (EC) No 509/2007, (EC) No 676/2007, (EC) No 1098/2007, (EC) No 1300/2008, (EC) No 1342/2008 and repealing Regulations (EEC) No 2847/93, (EC) No 1627/94 and (EC) No 1966/2006 ⁽¹⁾, and in particular Article 105(1), (2) and (3) thereof,

Whereas:

- (1) Fishing quotas for anchovy (*Engraulis encrasicolus*) in International Council for the Exploration of the Sea (ICES) zones 9 and 10 and Union waters of Committee for Eastern Central Atlantic Fisheries (CECAF) area 34.1.1 (ANE/9/3411) have been established by Council Regulation (EU) 2019/124 ⁽²⁾, for the period from 1 July 2019 to 30 June 2020.
- (2) Fishing quotas for anchovy (*Engraulis encrasicolus*) in ICES zones 9 and 10 and Union waters of CECAF area 34.1.1 (ANE/9/3411) have been established by Council Regulation (EU) 2020/123 ⁽³⁾, for the period from 1 July 2020 to 30 June 2021.
- (3) Pursuant to Article 105(1) of Regulation (EC) No 1224/2009, when the Commission has established that a Member State has exceeded the fishing quotas which have been allocated to it, the Commission is to operate deductions from future fishing quotas of that Member State.
- (4) Article 105(2) and (3) of Regulation (EC) No 1224/2009 provides that such deductions have to be operated in the following year or years by applying the respective multiplying factors as set out therein.
- (5) Portugal has exceeded its fishing quota for anchovy (*Engraulis encrasicolus*) in ICES zones 9 and 10 and Union waters of CECAF area 34.1.1 (ANE/9/3411) for the period from 1 July 2019 to 30 June 2020.
- (6) It is therefore appropriate to operate a deduction on the fishing quota allocated to Portugal for the period from 1 July 2020 to 30 June 2021 and, where relevant, in subsequent years, for the overfished stock,

HAS ADOPTED THIS REGULATION:

Article 1

The fishing quota allocated to Portugal for anchovy (*Engraulis encrasicolus*) in International Council for the Exploration of the Sea (ICES) zones 9 and 10 and Union waters of Committee for Eastern Central Atlantic Fisheries (CECAF) area 34.1.1 (ANE/9/3411), for the period from 1 July 2020 to 30 June 2021, fixed in Regulation (EU) 2020/123, shall be reduced as set out in the Annex to this Regulation.

⁽¹⁾ OJ L 343, 22.12.2009, p. 1.

⁽²⁾ Council Regulation (EU) 2019/124 of 30 January 2019 fixing for 2019 the fishing opportunities for certain fish stocks and groups of fish stocks, applicable in Union waters and, for Union fishing vessels, in certain non-Union waters (OJ L 29, 31.1.2019, p. 1).

⁽³⁾ Council Regulation (EU) 2020/123 of 27 January 2020 fixing for 2020 the fishing opportunities for certain fish stocks and groups of fish stocks, applicable in Union waters and, for Union fishing vessels, in certain non-Union waters (OJ L 25, 30.1.2020, p. 1).

Article 2

This Regulation shall enter into force on the seventh 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, 29 January 2021.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX

Member State	Species code	Area code	Species name	Area name	Initial quota for the period 1 July 2019 – 30 June 2020 (in kilograms)	Permitted landings for the period 1 July 2019 – 30 June 2020 (Total adapted quantity in kilograms) ⁽¹⁾	Total catches for the period 1 July 2019 – 30 June 2020 (quantity in kilograms)	Quota consumption related to permitted landings (%)	Overfishing related to permitted landings (quantity in kilograms)	Multi-plying factor ⁽²⁾	Additional Multi-plying factor ⁽³⁾ ⁽⁴⁾	Out-standing deductions from previous year(s) ⁽⁵⁾ (quantity in kilograms)	Deductions to apply to the period 1 July 2020 – 30 June 2021 (quantity in kilograms)
PT	ANE	9/3411	Anchovy	ICES zones 9 and 10; Union waters of CECAF area 34.1.1	5 343 000	3 779 330	3 858 005	102,08	78 675	/	/	/	78 675

⁽¹⁾ Quotas available to a Member State pursuant to Regulation (EU) 2019/124 after taking into account exchanges of fishing opportunities in accordance with Article 16(8) of Regulation (EU) No 1380/2013 of the European Parliament and of the Council on the Common Fisheries Policy, amending Council Regulations (EC) No 1954/2003 and (EC) No 1224/2009 and repealing Council Regulations (EC) No 2371/2002 and (EC) No 639/2004 and Council Decision 2004/585/EC (OJ L 354, 28.12.2013, p. 22), quota transfers from 2018 to 2019 in accordance with Article 4(2) of Council Regulation (EC) No 847/96 introducing additional conditions for year-to-year management of TACs and quotas (OJ L 115, 9.5.1996, p. 3) and with Article 15(9) of Regulation (EU) No 1380/2013, or reallocation and deduction of fishing opportunities in accordance with Articles 37 and 105 of Regulation (EC) No 1224/2009 of 20 November 2009 establishing a Union control system for ensuring compliance with the rules of the common fisheries policy, amending Regulations (EC) No 847/96, (EC) No 2371/2002, (EC) No 811/2004, (EC) No 768/2005, (EC) No 2115/2005, (EC) No 2166/2005, (EC) No 388/2006, (EC) No 509/2007, (EC) No 676/2007, (EC) No 1098/2007, (EC) No 1300/2008, (EC) No 1342/2008 and repealing Regulations (EEC) No 2847/93, (EC) No 1627/94 and (EC) No 1966/2006 (OJ L 343, 22.12.2009, p. 1).

⁽²⁾ As set out in Article 105(2) of Regulation (EC) No 1224/2009. Deduction equal to the overfishing * 1,00 shall apply in all cases of overfishing equal to, or less than, 100 tonnes.

⁽³⁾ As set out in Article 105(3) of Regulation (EC) No 1224/2009 and provided that the extent of overfishing exceeds 10 %.

⁽⁴⁾ Letter 'A' indicates that an additional multiplying factor of 1,5 has been applied because the Member State has repeatedly overfished its quota over the previous 2 years. Letter 'C' indicates that an additional multiplying factor of 1,5 has been applied as the stock is subject to a multiannual plan.

⁽⁵⁾ Remaining quantities from previous year(s).

COMMISSION IMPLEMENTING REGULATION (EU) 2021/253**of 17 February 2021****amending Council Regulation (EC) No 314/2004 concerning restrictive measures in view of the situation in Zimbabwe**

THE EUROPEAN COMMISSION,

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

Having regard to Council Regulation (EC) No 314/2004 of 19 February 2004 concerning restrictive measures in view of the situation in Zimbabwe ⁽¹⁾, and in particular Article 11(b) thereof,

Whereas:

- (1) Council Decision 2011/101/CFSP ⁽²⁾ identifies the persons and entities to whom restrictive measures apply as provided for in Articles 4 and 5 of that Decision.
- (2) Regulation (EC) No 314/2004 gives effect to that Decision to the extent that action at Union level is required. In particular, Annex III to Regulation (EC) No 314/2004 lists the persons and entities covered by the freezing of funds and economic resources under that Regulation.
- (3) On 18 February 2021, the Council adopted Decision (CFSP) 2021/258 ⁽³⁾ amending the entries for two persons in and removing one person from the list of persons and entities subject to restrictive measures.
- (4) Annex III to Regulation (EC) No 314/2004 should therefore be amended accordingly,

HAS ADOPTED THIS REGULATION:

Article 1

Annex III to Regulation (EC) No 314/2004 is amended as set out in the Annex to this Regulation.

Article 2

This Regulation shall enter into force on the 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 the Member States in accordance with the Treaties.

Done at Brussels, 17 February 2021.

*For the Commission,
On behalf of the President,
Director-General*

*Directorate-General for Financial Stability, Financial
Services and Capital Markets Union*

⁽¹⁾ OJ L 55, 24.2.2004, p. 1.

⁽²⁾ Council Decision 2011/101/CFSP of 15 February 2011 concerning restrictive measures against Zimbabwe (OJ L 42, 16.2.2011, p. 6).

⁽³⁾ Council Decision (CFSP) 2021/258 of 18 February 2021 amending Decision 2011/101/CFSP concerning restrictive measures in view of the situation in Zimbabwe (see page 51 of this Official Journal).

ANNEX

Annex III, Section I, to Council Regulation (EC) No 314/2004 is amended as follows:

(1) the entries for the persons listed below are replaced as follows:

'(5) CHIWENGA, Constantine	Vice-President Former Commander of the Zimbabwe Defence Forces, retired General, born 25.8.1956 Passport AD000263 ID 63-327568M80	Vice-President and former Commander of the Zimbabwe Defence Forces. Member of Joint Operations Command and complicit in forming or directing repressive state policy. Used army for farm takeovers. During the 2008 elections, he was a prime architect of the violence associated with the process of the Presidential run-off.'
'(7) SIBANDA, Phillip Valerio (a.k.a. Valentine)	Commander of the Zimbabwe Defence Forces Former Commander of the Zimbabwe National Army, General, born 25.8.1956 or 24.12.1954 ID 63-357671H26	Commander of the Zimbabwe Defence Forces and former Commander of the Zimbabwe National Army. Senior army figure with ties to the Government and complicit in forming or directing oppressive state policy.'

(2) the following entry is deleted:

'(6) Shiri, Perence (a.k.a. Bigboy) Samson Chikerema	Air Marshal (Air Force) Born 1.11.1955 ID 29-098876M18	Senior military officer and member of ZANU-PF Joint Operational Command and complicit in forming or directing oppressive state policy. Involved in political violence, including during the 2008 election in Mashonaland West in Chiadzwa.'
--	--	---

COMMISSION IMPLEMENTING REGULATION (EU) 2021/254**of 18 February 2021****amending Implementing Regulations (EU) 2020/761 and (EU) 2020/1988 and Regulations (EC) No 218/2007 and (EC) No 1518/2007 as regards imports of products originating in the United Kingdom and excluding those products from the tariff quotas with ongoing quota periods**

THE EUROPEAN COMMISSION,

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

Having regard to Regulation (EU) No 1308/2013 of the European Parliament and of the Council of 17 December 2013 establishing a common organisation of the markets in agricultural products and repealing Council Regulations (EEC) No 922/72, (EEC) No 234/79, (EC) No 1037/2001 and (EC) No 1234/2007 ⁽¹⁾, and in particular Article 187 thereof,

Having regard to 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 ⁽²⁾, and in particular Article 66(4) thereof,

Having regard to Regulation (EU) No 510/2014 of the European Parliament and of the Council of 16 April 2014 laying down the trade arrangements applicable to certain goods resulting from the processing of agricultural products and repealing Council Regulations (EC) No 1216/2009 and (EC) No 614/2009 ⁽³⁾, and in particular points (a) to (d) of the first paragraph of Article 9 and point (a) of the first subparagraph of Article 16(1) thereof,

Whereas:

- (1) Commission Implementing Regulation (EU) 2020/761 ⁽⁴⁾ lays down the rules for the management of import and export tariff quotas for agricultural products managed by a system of import and export licences and replaces and repeals a certain number of acts that have opened these quotas and provides for specific rules.
- (2) Commission Implementing Regulation (EU) 2020/1988 ⁽⁵⁾ lays down the rules for the application of Regulation (EU) No 1308/2013 as regards the rules for the administration of import tariff quotas designed to be used following the chronological order of dates of acceptance of customs declarations ('first come, first served' principle).
- (3) Commission Regulation (EC) No 218/2007 ⁽⁶⁾ opens and provides for the administration of some tariff quotas for wine.
- (4) Commission Regulation (EC) No 1518/2007 ⁽⁷⁾ opens and provides for the administration of a tariff quota for vermouth.

⁽¹⁾ OJ L 347, 20.12.2013, p. 671.

⁽²⁾ OJ L 347, 20.12.2013, p. 549.

⁽³⁾ OJ L 150, 20.5.2014, p. 1.

⁽⁴⁾ Commission Implementing Regulation (EU) 2020/761 of 17 December 2019 laying down rules for the application of Regulations (EU) No 1306/2013, (EU) No 1308/2013 and (EU) No 510/2014 of the European Parliament and of the Council as regards the management system of tariff quotas with licences (OJ L 185, 12.6.2020, p. 24).

⁽⁵⁾ Commission Implementing Regulation (EU) 2020/1988 of 11 November 2020 laying down rules for the application of Regulations (EU) No 1308/2013 and (EU) No 510/2014 of the European Parliament and of the Council as regards the administration of import tariff quotas in accordance with the 'first come, first served' principle (OJ L 422, 14.12.2020, p. 4).

⁽⁶⁾ Commission Regulation (EC) No 218/2007 of 28 February 2007 opening and providing for the administration of Community tariff quotas for wines (OJ L 62, 1.3.2007, p. 22).

⁽⁷⁾ Commission Regulation (EC) No 1518/2007 of 19 December 2007 opening and providing for the administration of a tariff quota for vermouth (OJ L 335, 20.12.2007, p. 14).

- (5) The Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part (hereafter 'the Agreement') ⁽⁸⁾ provides that products originating in the United Kingdom are not eligible to be imported into the Union under existing WTO tariff quotas as defined in Article GOODS.18 of the Agreement. That Article refers to tariff quotas apportioned between the Parties pursuant to Article XXVIII GATT negotiations initiated by the Union in WTO document G/SECRET/42/Add.2 ⁽⁹⁾ and by the United Kingdom in WTO document G/SECRET/44 ⁽¹⁰⁾ and as set out in each Party's respective internal legislation. That Article provides that the originating status of the products is to be determined on the basis of non-preferential rules of origin applicable in the importing Party.
- (6) The existing WTO tariff quotas as defined in Article GOODS.18 of the Agreement refer to WTO concessions of the Union included in the draft EU28 schedule of concessions and commitments under GATT 1994 submitted to the WTO in document G/MA/TAR/RS/506 ⁽¹¹⁾ as amended by documents G/MA/TAR/RS/506/Add.1 and G/MA/TAR/RS/506/Add.2 ⁽¹²⁾.
- (7) Implementing Regulations (EU) 2020/761 and (EU) 2020/1988 and Regulations (EC) No 218/2007 and (EC) No 1518/2007 should therefore be amended to comply with Article GOOD.18 of the Agreement in order to exclude products originating in the United Kingdom from existing WTO tariff quotas.
- (8) As Implementing Regulations (EU) 2020/761 and (EU) 2020/1988 apply only to tariff quotas with quota periods starting from 1 January 2021, the United Kingdom should also be excluded for purposes of the same tariff quotas whose quota periods have started before 1 January 2021 (ongoing quota periods on 1 January 2021) and for which imports occur as of 1 January 2021. Licences already issued are not needed for the import of products originating in the United Kingdom due to the possibility to import duty-free and quota-free under the Agreement. In case such licences have been issued before 1 January 2021, the relevant securities lodged should be released at the request of the operators concerned. As of 1 January 2021, licences for those tariff quotas should not be issued for products originating in the United Kingdom.
- (9) In order to ensure the conformity with Article GOODS.18 of the Agreement, this Regulation should enter into force as a matter of urgency on the day of its publication in the *Official Journal of the European Union* and apply as of 1 January 2021.
- (10) The measures provided for in this Regulation are in accordance with the opinion of the Committee for the Common Organisation of the Agricultural Markets,

HAS ADOPTED THIS REGULATION:

Article 1

Amendments to Implementing Regulation (EU) 2020/761

Implementing Regulation (EU) 2020/761 is amended as follows:

- (1) Annex II is amended as follows:
- (a) the box 'Origin' of the tables referring to TRQs with order numbers 09.4131, 09.4133, 09.4120, 09.4121 and 09.4122 is replaced by the following:

'Origin'	All third countries except the United Kingdom'
-----------------	--

- (b) the box 'Origin' of the table referring to TRQ with order number 09.4125 is replaced by the following:

'Origin'	All third countries except the United States of America, Canada and the United Kingdom'
-----------------	---

⁽⁸⁾ OJ L 444, 31.12.2020, p. 14.

⁽⁹⁾ <https://docs.wto.org>

⁽¹⁰⁾ <https://docs.wto.org>

⁽¹¹⁾ <https://docs.wto.org>

⁽¹²⁾ <https://docs.wto.org>

(2) Annex III is amended as follows:

- (a) the box 'Origin' of the tables referring to TRQs with order numbers 09.4138, 09.4148, 09.4166 and 09.4168 is replaced by the following:

'Origin'	All third countries except the United Kingdom'
-----------------	--

- (b) the box 'Origin' of the table referring to TRQ with order number 09.4119 is replaced by the following:

'Origin'	All third countries except India, Pakistan, Thailand, United States of America, and the United Kingdom'
-----------------	---

- (c) the box 'Origin' of the table referring to TRQ with order number 09.4130 is replaced by the following:

'Origin'	All third countries except Australia, Thailand, United States of America, and the United Kingdom'
-----------------	---

- (d) the box 'Origin' of the table referring to TRQ with order number 09.4154 is replaced by the following:

'Origin'	All third countries except Australia, Guyana, Thailand, United States of America, and the United Kingdom'
-----------------	---

- (3) in Annex IV, the box 'Origin' of the table referring to TRQ with order number 09.4320 is replaced by the following:

'Origin'	All third countries except the United Kingdom'
-----------------	--

- (4) in Annex VI, the box 'Origin' of the table referring to TRQ with order number 09.4287 is replaced by the following:

'Origin'	All third countries except China, Argentina and the United Kingdom'
-----------------	---

- (5) in Annex VII, the box 'Origin' of the table referring to TRQ with order number 09.4286 is replaced by the following:

'Origin'	All third countries except China and the United Kingdom'
-----------------	--

- (6) in Annex VIII, the box 'Origin' of the table referring to TRQ with order number 09.4003 is replaced by the following:

'Origin'	All third countries except the United Kingdom'
-----------------	--

- (7) in Annex IX, the box 'Origin' of the table referring to TRQ with order number 09.4595 is replaced by the following:

'Origin'	All third countries except the United Kingdom'
-----------------	--

- (8) in Annex X, the box 'Origin' of the table referring to TRQ with order number 09.4038 is replaced by the following:

'Origin'	All third countries except the United Kingdom'
-----------------	--

- (9) in Annex XI, the box 'Origin' of the tables referring to TRQs with order numbers 09.4401 and 09.4402 is replaced by the following:

'Origin'	All third countries except the United Kingdom'
-----------------	--

- (10) Annex XII is amended as follows:

- (a) the box 'Origin' of the tables referring to TRQs with order numbers 09.4067, 09.4068, 09.4069, 09.4070 and 09.4422 is replaced by the following:

'Origin'	All third countries except the United Kingdom'
-----------------	--

- (b) the tables referring to TRQs with order numbers 09.4213, 09.4216, 09.4260 and 09.4412 are amended as follows:

- (i) the box 'Origin' is replaced by the following:

'Origin'	All third countries except Brazil, Thailand and the United Kingdom'
-----------------	---

- (ii) the box 'Specific entries to be made on the licence application and on the licence' is replaced by the following:

'Specific entries to be made on the licence application and on the licence'	Licences shall contain in Section 24 the statement "Not to be used for products originating in Brazil, Thailand and the United Kingdom"
--	---

- (c) the table referring to TRQ with order number 09.4218 is amended as follows:

- (i) the box 'Origin' is replaced by the following:

'Origin'	All third countries except Brazil and the United Kingdom'
-----------------	---

- (ii) the box 'Specific entries to be made on the licence application and on the licence' is replaced by the following:

'Specific entries to be made on the licence application and on the licence'	Licences shall contain in Section 24 the statement "Not to be used for products originating in Brazil and the United Kingdom"
--	---

- (d) the tables referring to TRQs with order numbers 09.4263, 09.4264 and 09.4265 are amended as follows:

- (i) the box 'Origin' is replaced by the following:

'Origin'	All third countries except Thailand and the United Kingdom'
-----------------	---

- (ii) the box 'Specific entries to be made on the licence application and on the licence' is replaced by the following:

'Specific entries to be made on the licence application and on the licence'	Licences shall contain in Section 24 the statement "Not to be used for products originating in Thailand and the United Kingdom"
--	---

Article 2

Amendments to Implementing Regulation (EU) 2020/1988

Annex I to Implementing Regulation (EU) 2020/1988 is amended as follows:

- (1) the box 'Origin' of the tables referring to TRQs with order numbers 09.0138, 09.0132, 09.0135, 09.2903, 09.2905, 09.0071, 09.0072, 09.0073, 09.0074, 09.0075, 09.0076, 09.0089, 09.0070, 09.0043, 09.0083, 09.0139,, 09.0056, 09.0057, 09.0041, 09.0039, 09.0058, 09.0094, 09.0059, 09.0060, 09.0061, 09.0062, 09.0063, 09.0040, 09.0025, 09.0027, 09.0033, 09.0092, 09.0093, 09.0035, 09.0144, 09.0161 (sub-tariff quota of 09.0144), 09.0162 (sub-tariff quota of 09.0144), 09.0145, 09.0163 (sub-tariff quota of 09.0145), 09.0164 (sub-tariff quota of 09.0145), 09.0113, 09.0114, 09.0115, 09.0147, 09.0148, 09.0149, 09.0150, 09.0151, 09.0152, 09.0153, 09.0159 (sub-tariff quota of 09.0153), 09.0160 (sub-tariff quota of 09.0153), 09.0118, 09.0119, 09.0120, 09.0121, 09.0122, 09.0123, 09.2178, 09.2179, 09.2016, 09.2181, 09.2019, 09.0154 and 09.0055 is replaced by the following:

'Origin'	All third countries except the United Kingdom'
-----------------	--

- (2) the box 'Origin' of the table referring to TRQ with order number 09.0128 is replaced by the following:

'Origin'	Third countries which are members of the WTO except China, Thailand, Indonesia and the United Kingdom'
-----------------	--

- (3) the box 'Origin' of the table referring to TRQs with order number 09.0131 is replaced by the following:

'Origin'	All third countries except China and the United Kingdom'
-----------------	--

- (4) the box 'Origin' of the table referring to TRQs with order number 09.0142 is replaced by the following:

'Origin'	All third countries except Argentina and the United Kingdom'
-----------------	--

- (5) the box 'Origin' of the tables referring to TRQs with order numbers 09.2171, 09.2175 and 09.2015 is replaced by the following:

'Origin'	All WTO members except Argentina, Australia, New Zealand, Uruguay, Chile, Greenland, Iceland and the United Kingdom'
-----------------	--

- (6) the box 'Origin' of the tables referring to TRQs with order numbers 09.0156 and 09.0158 is replaced by the following:

'Origin'	All third countries except Brazil and the United Kingdom'
-----------------	---

(7) the box 'Origin' of the table referring to TRQs with order number 09.0157 is replaced by the following:

'Origin'	All third countries except Brazil, Thailand and the United Kingdom'
-----------------	---

Article 3

Amendments to Regulation (EC) No 218/2007

Article 1 of Regulation (EC) No 218/2007 is amended as follows:

- (1) in point (a), the words '*erga omnes*' are replaced by the words '(all third countries except the United Kingdom)';
- (2) in point (b), the words '*erga omnes*' are replaced by the words '(all third countries except the United Kingdom)'.

Article 4

Amendment to Regulation (EC) No 1518/2007

In Article 1 of Regulation (EC) No 1518/2007, the words '*erga omnes*' are replaced by the words '(all third countries except the United Kingdom)'.

Article 5

Tariff quotas with ongoing quota periods

1. As of 1 January 2021, licences shall not be issued for products originating in the United Kingdom under the tariff quotas referred to in Article 1 whose quota period is ongoing on 1 January 2021. As of the same date, products originating in the United Kingdom shall not enter under the tariff quotas referred to in Article 2.
2. As regards imports into the Union from the United Kingdom on the basis of licenses under the tariff quotas referred to in Article 1 issued before 1 January 2021 that include the United Kingdom as a country of origin and whose quota period is ongoing on 1 January 2021 and which Member States do not place under release for free circulation in accordance with the Agreement, the respective securities lodged shall be released at the request of the operators concerned.

Article 6

Entry into force and application

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

It shall apply from 1 January 2021.

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

Done at Brussels, 18 February 2021.

For the Commission
The President
Ursula VON DER LEYEN

COMMISSION IMPLEMENTING REGULATION (EU) 2021/255**of 18 February 2021****amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security****(Text with EEA relevance)**

THE EUROPEAN COMMISSION,

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

Having regard to Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 ⁽¹⁾, and in particular Article 4(3) thereof,

Whereas:

- (1) The COVID-19 pandemic continues to impact international and European civil aviation to the extent that the performance of on-site visits for the designation and re-designations of air carriers and cargo operators in third countries pursuant to point 6.8 of the Annex to Commission Implementing Regulation (EU) 2015/1998 ⁽²⁾ remains severely impeded for objective reasons, which are beyond the control of those carriers or cargo operators.
- (2) It is therefore necessary to extend the applicability of the alternative and expedite process for the EU aviation security validations of the Union-bound supply chain operators affected by the COVID-19 pandemic, beyond the date established in point 6.8.1.7 of the Annex to Implementing Regulation (EU) 2015/1998.
- (3) The Union has promoted, in the context of the International Civil Aviation Organisation (ICAO) and the World Customs Organisation (WCO), the development of an international policy concept of Pre-Loading Advance Cargo Information (PLACI), used to describe a specific 7 + 1 data set ⁽³⁾ as defined in the WCO SAFE Framework of Standards (SAFE FoS). Consignments' data, provided to regulators by freight forwarders, air carriers, postal operators, integrators, regulated agents, or other entities as soon as possible prior to loading of cargo on an aircraft at the last point of departure, allow the implementation of an additional security layer, consisting in the performance by the entry customs of a threat and risk analysis before departure.
- (4) Therefore, before loading goods onto an aircraft departing from a third country, for the purposes of civil aviation security a first risk analysis on goods to be brought into the customs territory of the Union by air should be carried out as soon as possible upon receipt of the minimum dataset of the entry summary declaration referred to in Article 106(2) and (2a) of Commission Delegated Regulation (EU) 2015/2446 ⁽⁴⁾. The requirement of carrying out a first risk analysis should apply from 15 March 2021.
- (5) Article 186 of Commission Implementing Regulation (EU) 2015/2447 ⁽⁵⁾ establishes the risk analysis and control process implemented by the customs office of first entry, and Article 182 of that Regulation establishes the Import Control System (ICS2), designed by the Commission and the Member States in mutual agreement, as the EU

⁽¹⁾ OJ L 97, 9.4.2008, p. 72.

⁽²⁾ Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security (OJ L 299, 14.11.2015, p. 1).

⁽³⁾ Name of the consignor, address of the consignor, name of the consignee, address of the consignee, number of packages, total gross weight, description of cargo, and House or Master Air Waybill.

⁽⁴⁾ Commission Delegated Regulation (EU) 2015/2446 of 28 July 2015 supplementing Regulation (EU) No 952/2013 of the European Parliament and of the Council as regards detailed rules concerning certain provisions of the Union Customs Code (OJ L 343, 29.12.2015, p. 1).

⁽⁵⁾ Commission Implementing Regulation (EU) 2015/2447 of 24 November 2015 laying down detailed rules for implementing certain provisions of Regulation (EU) No 952/2013 of the European Parliament and of the Council laying down the Union Customs Code (OJ L 343, 29.12.2015, p. 558).

harmonised trader interface for submissions, requests for amendments, requests for invalidations, processing and storage of the particulars of entry summary declarations and for the exchange of related information with the customs authorities.

- (6) Since the results of the Pre-Loading Advance Cargo Information risk analysis can require, from 15 March 2021, specific mitigating aviation security measures to be applied by operators engaged in the Union-bound supply chain during their operations in a third country, it is necessary to urgently integrate the implementing rules for civil aviation security accordingly.
- (7) The ability of airports in the Union to complete the process of installation of standard 3 explosive detection systems (EDS) equipment is severely impacted by the current COVID-19 pandemic. The Commission and the Member States remain highly committed to complete the implementation of newest technology for the screening of hold baggage. A new road map has been elaborated to allow additional flexibility to adapt to the current situation, in accordance with a prioritisation mechanism based on categories of airports, as well as to provide visibility for the introduction of higher standards for detection performance.
- (8) Experience gained with the implementation of Commission Implementing Regulation (EU) 2015/1998 has shown the need for some amendments to the implementing modalities of certain common basic standards. The implementing modalities of certain of those standards need to be adjusted in order to clarify, harmonise, simplify and strengthen certain specific aviation security measures, to improve legal clarity, standardize the common interpretation of the legislation and further ensure the best implementation of the common basic standards in aviation security.
- (9) Implementing Regulation (EU) 2015/1998 should therefore be amended accordingly.
- (10) The measures provided for in this Regulation are in accordance with the opinion of the Committee referred to in Article 19 of Regulation (EC) No 300/2008,

HAS ADOPTED THIS REGULATION:

Article 1

The Annex to Implementing Regulation (EU) 2015/1998 is amended in accordance with the Annex to this Regulation.

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*.

However, points (1) and (22) of the Annex shall apply from 15 March 2021, point (2) of the Annex shall apply from 1 March 2022, and point (14) shall apply from 1 July 2021.

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

Done at Brussels, 18 February 2021.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX

The Annex is amended as follows:

- (1) the following point 6.0.4 is added:

‘6.0.4 For the purposes of this Annex, “Pre-Loading Advance Cargo Information” or “PLACI” means the process of first risk analysis for aviation security purposes of goods to be brought into the customs territory of the Union * by air.

* As Iceland is not part of the customs territory of the Union, for the purposes of point 6.8.7 of this Annex, Iceland is considered a third country.’;

- (2) the following points 6.1.4, 6.1.5 and 6.1.6 are added:

‘6.1.4 Access into the security restricted areas of cargo and mail may only be granted after having established to which of the following categories the entity transporting the consignment from landside belongs:

- (a) a regulated agent;
- (b) a known consignor;
- (c) a haulier appointed in accordance with point 6.6.1.1(c), transporting consignments to which security controls have been previously applied;
- (d) neither of the entities referred to in points (a), (b) and (c).

6.1.5 Where point 6.1.4(c) applies, a copy of the signed declaration as contained in Attachment 6-E shall be made available to the regulated agent, air carrier or airport operator granting access into the security restricted areas, unless either of the following applies:

- (a) the haulier is itself a regulated agent;
- (b) the transport is performed on behalf of the receiving regulated agent or air carrier in the security restricted areas.

The presentation by the haulier of a copy of the signed declaration in Attachment 6-E may be replaced by an equivalent mechanism of prior notification to the access point, ensured either by the off-airport known consignor or regulated agent on whose behalf the transport is performed, or by the receiving regulated agent or air carrier in the security restricted areas.

6.1.6 Cargo or mail consignments to which security controls have not been previously applied may be allowed into the security restricted areas, provided they are subject to the implementation of one of the following options:

- (a) screened before entry, in accordance with point 6.2, and under the responsibility of the receiving regulated agent or air carrier;
- (b) escorted to the premises of the regulated agent or of the air carrier located in the security restricted areas, under their responsibility.

Upon delivery, such consignments shall be kept protected from unauthorised interference, until they are subjected to screening.

The personnel escorting such consignments or protecting them from unauthorised interference, shall have been recruited in accordance with point 11.1.1, and trained in accordance with at least point 11.2.3.9.’;

- (3) in point 6.3.1.2, point (b) is replaced by the following:

‘(b) the appropriate authority or an EU aviation security validator acting on its behalf shall examine the security programme before carrying out an on-site verification of the sites specified in order to assess compliance of the applicant with the requirements of Regulation (EC) No 300/2008 and the implementing acts adopted on its basis.

Except for the screening requirements laid down in point 6.2, an examination of the site of the applicant by the relevant customs authority in accordance with Article 29 of Commission Implementing Regulation (EU) 2015/2447 * shall be considered as an on-site verification where it is carried out not earlier than 3 years before the date on which the applicant seeks approval as a regulated agent. The AEO authorisation and the relevant assessment of the customs authorities shall be made available by the applicant for further inspection.

* Commission Implementing Regulation (EU) 2015/2447 of 24 November 2015 laying down detailed rules for implementing certain provisions of Regulation (EU) No 952/2013 of the European Parliament and of the Council laying down the Union Customs Code (OJ L 343, 29.12.2015, p. 558).;

- (4) in point 6.3.1.4, the third paragraph is replaced by the following:

‘Except for the screening requirements laid down in point 6.2, an examination of the site of the regulated agent by the relevant customs authority carried out in accordance with Article 29 of Implementing Regulation (EU) 2015/2447 shall be considered as an on-site verification.’;

- (5) point 6.3.1.5 is replaced by the following:

‘6.3.1.5 Where the appropriate authority is no longer satisfied that the regulated agent complies with the requirements of Regulation (EC) No 300/2008, it shall withdraw the status of regulated agent for the specified site or sites.

Immediately after withdrawal, and in all cases within 24 hours of withdrawal, the appropriate authority shall ensure that the former regulated agent’s change of status is indicated in the “Union database on supply chain security”. Where the regulated agent is no longer a holder of an AEO authorisation referred to in (b) of Article 38(2) of Regulation (EU) No 952/2013 of the European Parliament and of the Council * and in Article 33 of Implementing Regulation (EU) 2015/2447 or where its AEO authorisation is suspended due to non-compliance with point (e) of Article 39 of Regulation (EU) No 952/2013 and Article 28 of Implementing Regulation (EU) 2015/2447, the appropriate authority shall take appropriate action to ensure compliance of the regulated agent with the requirements of Regulation (EC) No 300/2008.

The regulated agent shall inform the appropriate authority of any changes related to its AEO authorisation referred to in point (b) of Article 38(2) of Regulation (EU) No 952/2013 and in Article 33 of Regulation (EU) 2015/2447.

* Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code (OJ L 269, 10.10.2013, p. 1).;

- (6) point 6.3.1.8 is replaced by the following:

‘6.3.1.8 The appropriate authority shall make available to the customs authority any information related to the status of a regulated agent which could be relevant to the holding an AEO authorisation referred to in point (b) of Article 38(2) of Regulation (EU) No 952/2013 and in Article 33 of Implementing Regulation (EU) 2015/2447. That information shall include the information related to new approvals of regulated agents, withdrawal of the regulated agent status, revalidation and inspections, verification schedules and outcomes of those assessments.

The modalities for that exchange of information shall be established between the appropriate authority and the national customs authorities.’;

- (7) in point 6.3.2.6, point (g) is replaced by the following:

‘(g) the unique identifier received from the appropriate authority, of any regulated agent who has accepted the security status given to a consignment by another regulated agent, including during transfer operations.’;

- (8) the following paragraph is added in point 6.3.2.6:

‘Transfer cargo or mail for which the air carrier, or the regulated agent operating on its behalf, is unable to confirm in the accompanying documentation the information required by this point, or by point 6.3.2.7 as applicable, shall be subject to screening before being loaded on board an aircraft for the subsequent flight.’;

- (9) in point 6.4.1.2, point (c) is replaced by the following:

‘(c) an examination of the site of the applicant by the relevant customs authority in accordance with Article 29 of Implementing Regulation (EU) 2015/2447 shall be considered as an on-site verification where it is carried out not earlier than 3 years before the date on which the applicant seeks approval as a known consignor. In those cases, the applicant shall complete the information required in Part One of the “Validation checklist for known consignors” as contained in Attachment 6-C and send it to the appropriate authority jointly with the declaration of commitments which shall be signed by the applicant’s legal representative or by the person responsible for security at the site.

The AEO authorisation and the relevant assessment of the customs authorities shall be made available by the applicant for further inspection.

The signed declaration shall be retained by the appropriate authority concerned or retained by the EU aviation security validator and made available on request to the appropriate authority concerned;’

- (10) in point 6.4.1.4, the third paragraph is replaced by the following:

‘An examination of the site of the known consignor by the relevant customs authority in accordance with Article 29 of Implementing Regulation (EU) 2015/2447 shall be considered as an on-site verification.’;

- (11) point 6.4.1.5 is replaced by the following:

‘6.4.1.5 Where the appropriate authority is no longer satisfied that the known consignor complies with the requirements of Regulation (EC) No 300/2008, it shall withdraw the status of known consignor for the specified site(s).

Immediately after withdrawal, and in all cases within 24 hours of withdrawal, the appropriate authority shall ensure that the known consignor’s change of status is indicated in the “Union database on supply chain security”.

Where the known consignor is no longer a holder of an AEO authorisation referred to in point (b) of Article 38(2) of Regulation (EU) No 952/2013 and in Article 33 of Implementing Regulation (EU) 2015/2447 or where its AEO authorisation is suspended due to non-compliance with point (e) of Article 39 of Regulation (EU) No 952/2013 and Article 28 of Implementing Regulation (EU) 2015/2447, the appropriate authority shall take appropriate action to ensure compliance of the known consignor with the requirements of Regulation (EC) No 300/2008.

The known consignor shall inform the appropriate authority of any changes related to its AEO authorisation referred to in point (b) of Article 38(2) of Regulation (EU) No 952/2013 and in Article 33 of Implementing Regulation (EU) 2015/2447.’;

- (12) point 6.4.1.7 is replaced by the following:

‘6.4.1.7 The appropriate authority shall make available to the customs authority any information related to the status of a known consignor which could be relevant to the holding an AEO authorisation referred to in point (b) of Article 38(2) of Regulation (EU) No 952/2013 and in Article 33 of Implementing Regulation (EU) 2015/2447. That information shall include the information related to new approvals of known consignors, withdrawal of the known consignor status, revalidation and inspections, verification schedules and outcomes of those assessments.

The modalities for that exchange of information shall be established between the appropriate authority and the national customs authorities.’;

(13) point 6.5.1 is replaced by the following:

‘6.5.1 The regulated agent shall keep a database containing all the following information of any account consignor it has designated before 1 June 2017:

- (a) the company details, including the bona fide business address;
- (b) the nature of the business;
- (c) contact details, including those of the person or persons responsible for security;
- (d) VAT reference number or company registration number;
- (e) signed “Declaration of commitments – account consignor” as contained in Attachment 6-D.

Where the account consignor is a holder of an AEO authorisation referred to in point (b) of Article 38(2) of Regulation (EU) No 952/2013 and in Article 33 of Implementing Regulation (EU) 2015/2447, the AEO authorisation number shall be kept in the database referred to in the first paragraph.

The database shall be available for inspection by the appropriate authority.’;

(14) the following points 6.6.1.3, 6.6.1.4 and 6.6.1.5 are added:

‘6.6.1.3 The haulier shall ensure that staff collecting, carrying, storing and delivering air cargo and mail to which security controls have been applied undergoes at least the following:

- (a) a check of the personal integrity, consisting of the verification of the identity and of the curriculum vitae and/or provided references;
- (b) general security awareness training, in accordance with point 11.2.7.

6.6.1.4 Any of the haulier’s staff granted unsupervised access to cargo and mail while performing any of the functions referred to in point 6.6.1.3, or while implementing any of the security controls set out in this Chapter shall:

- (a) have successfully completed a background check;
- (b) undergo security training, in accordance with point 11.2.3.9.

6.6.1.5 Where a haulier uses the services of another company to perform one or more of the functions referred to in point 6.6.1.3, such other company shall fulfil the following conditions:

- (a) sign a haulier agreement with the haulier;
- (b) refrain from subcontracting further;
- (c) implement the provisions of points 6.6.1.3 and 6.6.1.4, as applicable.

The subcontracting haulier retains full responsibility for the entire transport on behalf of the agent or consignor.’;

(15) in point 6.8.1.7, the introductory wording is replaced by the following:

‘During the period from 1 April 2020 to 30 June 2021, the appropriate authority may derogate from the process established in point 6.8.2 and temporarily designate an air carrier as ACC3, in the case where an EU aviation security validation could not take place for objective reasons which are related to the pandemic crisis caused by the COVID-19 and are beyond the responsibility of the air carrier. The designation shall be subject to the following conditions’;

(16) points 6.8.3.6 and 6.8.3.7 are replaced by the following:

‘6.8.3.6 After the security controls referred to in points 6.8.3.1 to 6.8.3.5 have been implemented, the ACC3 or the EU aviation security validated regulated agent (RA3) responsible for the application of the security controls,

shall ensure that the accompanying documentation, in the form of an air waybill, an equivalent postal documentation or in a separate declaration, provided in an electronic format or in writing, includes at least the following information:

- (a) the unique alphanumeric identifier of the ACC3;
- (b) the security status of the consignment referred to in point (d) of point 6.3.2.6 and issued by the ACC3 or by the EU aviation security validated regulated agent (RA3), as appropriate;
- (c) the unique identifier of the consignment, such as the number of the house or master air waybill, where applicable;
- (d) the content of the consignment, or indication of consolidation where applicable;
- (e) the reasons for issuing the security status, including the means or method of screening used or the grounds for exempting the consignment from screening, using the standards adopted in the ICAO Consignment Security Declaration scheme.

In the case of consolidations, the ACC3 or the EU aviation security validated regulated agent (RA3) who has performed the consolidation shall retain the information set out in points (a) to (e) of the first paragraph for each individual consignment at least until the estimated time of arrival of the consignments at the first airport in the Union or for 24 hours, whichever period is longer.

6.8.3.7 Any air carrier arriving from a third country listed in Attachment 6-F shall ensure compliance with the applicable points laid down in point 6.8.3.6 in respect of cargo and mail transported on board. The accompanying documentation regarding such consignments shall at least comply with the ICAO Consignment Security Declaration scheme or with an alternative scheme providing the required information in an equivalent manner.’;

(17) point 6.8.3.9 is replaced by the following:

‘6.8.3.9 Transit or transfer consignments arriving from a third country not referred to in point 6.8.3.8 the accompanying documentation of which does not comply with point 6.8.3.6, shall be treated in accordance with point 6.2 before the subsequent flight.’;

(18) in point 6.8.4.11, the introductory wording is replaced by the following:

‘During the period from 1 April 2020 to 30 June 2021, the appropriate authority may derogate from the process established in point 6.8.5 and temporarily designate a third country entity as RA3 or KC3, in the case where an EU aviation security validation could not take place for objective reasons which are related to the pandemic crisis caused by the COVID-19 and are beyond the responsibility of the entity. The designation shall be subject to the following conditions:’;

(19) in point 6.8.4.12, point (d) is replaced by the following:

‘(d) the designation is granted for a period not exceeding six months and may be subject to extension within the derogation period as set out in point 6.8.4.11.’;

(20) points 6.8.5.5, 6.8.5.6 and 6.8.5.7 are deleted;

(21) in point 6.8.6.1, point 1 is replaced by the following:

‘1. Where the Commission or an appropriate authority identifies or receives written information about a serious deficiency relating to the operations of an ACC3, an RA3 or a KC3, which is deemed to have a significant impact on the overall level of aviation security in the Union, it shall:

- (a) inform the air carrier or entity concerned promptly, request comments and appropriate measures in respect to the serious deficiency;
- (b) promptly inform the other Member States and the Commission.

The serious deficiency referred to in the first paragraph may be identified during either of the following activities:

- (1) during compliance monitoring activities;
- (2) during the examination of documentation including the EU aviation security validation report of other operators which are part of the supply chain of the ACC3, RA3 or KC3;
- (3) upon receipt of factual written information from other authorities and/or operators in respect of the activities of the concerned ACC3, RA3 or KC3, in form of documented evidence clearly indicating security breaches.;

(22) the following point 6.8.7 is added:

‘6.8.7 Pre-Loading Advance Cargo Information (PLACI)

- 6.8.7.1 Pursuant to Article 186 of Implementing Regulation (EU) 2015/2447, the PLACI shall be carried out before departure from a third country, upon receipt by the customs authority of the first point of entry, of the minimum dataset of the entry summary declaration referred to in Article 106(2) and (2a) of Commission Delegated Regulation (EU) 2015/2446 *.
- 6.8.7.2 In the course of the PLACI and where there are reasonable grounds for the customs office of first entry to suspect that a consignment entering the customs territory of the Union by air could pose a serious threat to civil aviation, that consignment shall be treated as high risk cargo or mail (HRCM) in accordance with point 6.7.
- 6.8.7.3 The air carrier, operator, entity or person in a third country other than those listed in Attachment 6-F and Iceland, shall, upon receipt of a notification from the customs office of first entry requiring a consignment to be treated as high risk cargo or mail (HRCM) in accordance with point 6.8.7.2:
- (a) implement in respect of the specific consignment, the security controls listed in points 6.7.3 and 6.7.4 of the Annex to Implementing Decision C(2015) 8005, in case of an ACC3 or an RA3 approved for the performance of such security controls;
 - (b) ensure that an ACC3 or an RA3 approved for the performance of such security controls complies with the provisions laid down in point (a). Information to the customs office of first entry shall be provided in case the consignment is to be tendered or it has been tendered to another operator, entity or authority for the application of the security controls. Such other operator, entity or authority shall ensure the implementation of the security controls referred to in point (a) and confirm to the air carrier, operator, entity or person from which the consignment was received, both the implementation of such security controls and the results thereof;
 - (c) confirm to the customs office of first entry both the implementation of the security controls referred to in point (a) and the results thereof.

Points (a) and (b) of the first paragraph shall not apply in case the requested security controls have been previously implemented. However, should there be specific threat information that has only become available after the implementation of the previous security controls, the air carrier, operator, entity or person may be requested to repeat the security controls by using specific means and methods, and provide confirmation as set out in point (c) of the first paragraph. The air carrier, operator, entity or person may be made aware of any element and information necessary in order to effectively meet the security objective.

- 6.8.7.4 Air carriers, operators, entities or persons in a third country listed in Attachment 6-F or in Iceland, that receive a notification from the customs office of first entry requiring a consignment to be treated as high risk cargo or mail (HRCM) in accordance with point 6.8.7.2, shall:

- (a) implement, in respect of the specific consignment, at least the security controls established by ICAO Annex 17 for High Risk Cargo or Mail **;
- (b) ensure that the requirements of point (a) are fulfilled by an operator, entity or authority approved by the relevant appropriate authority in the third country for the performance of such security controls. Information to the customs office of first entry shall be provided in case the consignment is to be tendered or it has been tendered to another operator, entity or authority for the application of the security controls. Such other operator, entity or authority shall ensure the implementation of the security controls referred to in point (a) and confirm to the air carrier, operator, entity or person from which the consignment was received, both the implementation of such security controls and the results thereof;
- (c) confirm to the customs office of first entry both the implementation of the security controls referred to in point (a) and the results thereof.

Points (a) and (b) of the first paragraph shall not apply in case the requested security controls have been previously implemented. However, should there be specific threat information that has only become available after the implementation of the previous security controls, the air carrier, operator, entity or person may be requested to repeat the security controls by using specific means and methods, and provide confirmation as set out in point (c) of the first paragraph. The air carrier, operator, entity or person may be made aware of any element and information necessary in order to effectively meet the security objective.

- 6.8.7.5 In the course of the PLACI and where there are reasonable grounds for the customs office of first entry to suspect that a consignment entering the customs territory of the Union by air poses a serious threat to security, leading it to issue a do not load notification, that consignment shall not be loaded on board of an aircraft, or off-loaded, as applicable.
- 6.8.7.6 The air carrier, operator, entity or person in a third country that receives a notification from the customs office of first entry requiring a consignment not to be loaded on board of an aircraft in accordance with point 6.8.7.5, shall:
- (a) ensure that the consignment in its possession is not loaded on board an aircraft, or it is immediately off-loaded in case the consignment is already on board the aircraft;
 - (b) provide confirmation that it has fulfilled the request to the customs office of first entry in the customs territory of the Union;
 - (c) cooperate with the relevant authorities of the Member State of the customs office of first entry;
 - (d) inform the appropriate authority for civil aviation security of the State where the air carrier, operator, entity or person receiving the notification is located and of the third country where the consignment is currently located, if different.
- 6.8.7.7 Should the consignment be already with another air carrier, operator or entity along the supply chain, the air carrier, operator, entity or person receiving the do not load notification laid down in point 6.8.7.5 shall immediately inform such other air carrier, operator, entity or person that it shall:
- (a) ensure compliance with the provisions of points (a), (c) and (d) of point 6.8.7.6;
 - (b) confirm the application of point (b) of point 6.8.7.6 to the air carrier, operator, entity or person that received the notification laid down in point 6.8.7.5.
- 6.8.7.8 Should the aircraft be already airborne with a consignment on board for which the customs office of first entry had notified, pursuant to point 6.8.7.5, that a consignment must not be loaded, the air carrier, operator, entity or person receiving the notification shall immediately inform:

- (a) the relevant authorities of the Member State referred to in point (c) of point 6.8.7.6 for the purpose of informing and liaising with the relevant authorities of the Member State of first overflight in the Union;
- (b) the appropriate authority for civil aviation security of the third country where the air carrier, operator, entity or person receiving the notification is located and of the third country from which the flight has departed, if different.

6.8.7.9 Following the notification received from the customs office of first entry that has issued a notification as laid down in point 6.8.7.5, the appropriate authority of the same Member State shall, as applicable, implement or ensure the implementation thereof, or cooperate in any subsequent actions, including the coordination with the authorities of the third country of departure and where applicable in the country or countries of transit and/or transfer, the relevant security contingency protocols in accordance with the Member State's national civil aviation security programme and the international standards and recommended practices regulating crisis management and response to acts of unlawful interference.

6.8.7.10 The air carrier, operator, entity or person in a third country that receives a notification issued by the customs authority of a third country implementing a Pre-Loading Advance Cargo Information scheme in adherence to the principles set out by the World Customs Organisation's SAFE Framework of Standards, shall ensure the implementation of the requirements laid down in points 6.8.7.3 and 6.8.7.4 and in points 6.8.7.6, 6.8.7.7, 6.8.7.8.

This point applies only in respect of consignments of cargo or mail fulfilling any of the criteria below:

- (a) they are carried for transit or transfer at a Union airport before reaching the final destination at an airport based in the third country of the notifying customs authority;
- (b) they are carried for transit or transfer at a Union airport before having another transit or transfer at an airport based in the third country of the notifying customs authority.

For the purposes of the requirements set out in points 6.8.7.6(c) and 6.8.7.8(a), the air carrier, operator, entity or person receiving the notification in a third country, shall immediately inform the relevant authorities of the Member State of first landing in the Union.

Should the aircraft be already airborne, the information shall be provided to the relevant authorities of the Member State of first overflight in the Union that shall ensure the implementation of the actions referred to in point 6.8.7.9, in coordination with the relevant authorities of the Member State of first landing in the Union.

The relevant authorities of both the Member State of first overflight in the Union and of the Member State of first landing in the Union shall inform the respective customs authority.

* Commission Delegated Regulation (EU) 2015/2446 of 28 July 2015 supplementing Regulation (EU) No 952/2013 of the European Parliament and of the Council as regards detailed rules concerning certain provisions of the Union Customs Code (OJ L 343, 29.12.2015, p. 1).

** Air carriers, operators and entities in Iceland shall apply points 6.7.3 and 6.7.4 of the Annex to Implementing Decision C(2015) 8005.;

(23) the following sentence is added in point 11.6.3.6:

'The appropriate authority shall provide the validators it approves with the relevant parts of the non-public legislation and national programmes referring to the operations and areas to validate.';

(24) point 11.6.3.8 is replaced by the following:

‘11.6.3.8 The appropriate authority acting as validator may only perform validations in respect of air carriers, operators and entities that are placed under its responsibility or under the responsibility of the appropriate authority of another Member State, where it has been explicitly requested or appointed to do so by that authority.’;

(25) the following point 11.6.3.11 is added:

‘11.6.3.11 The approval of an EU aviation security validator shall be valid for a maximum period of five years.’;

(26) point 11.6.4.1 is replaced by the following:

‘11.6.4.1 An EU aviation security validator:

- (a) shall not be considered to be approved until its details are listed in the “Union database on supply chain security”;
- (b) shall be provided with proof of its status by or on behalf of the appropriate authority;
- (c) may not perform EU aviation security validations if it holds the status of aviation security validator under an equivalent scheme in place in a third country or an international organisation, unless point 11.6.4.5 applies.

EU aviation security validators listed in the “Union database on supply chain security” on account of the appropriate authority, may only perform validations of airlines, operators or entities under the responsibility of that appropriate authority.’;

(27) point 11.6.5.6 is replaced by the following:

‘11.6.5.6 By default the report shall be in English and delivered to the appropriate authority along with the validated entity, within not more than one month after the on-site verification.

The appropriate authority shall assess the validation report within not more than six weeks after its reception.

Where the report concerns an airline, operator or entity undergoing validation for the purposes of an existing designation that expires after the periods referred to in the paragraphs above, the appropriate authority may set a longer period to complete the assessment.

In such case, and unless further information and additional documentary evidence is necessary to successfully conclude the assessment, the appropriate authority shall ensure that the process is completed before the expiry of the validity of status.

Within three months from the date of reception of the report, the validator shall be provided with a written feedback regarding the quality of the report, and where applicable, any recommendations and remarks that the appropriate authority may deem necessary. Where applicable, a copy of such feedback shall be transmitted to the appropriate authority that has approved the validator.

For the purposes of the designation of other airlines, operators or entities as provided for in this Regulation, an appropriate authority may request and shall obtain, within 15 days, from the appropriate authority that has drafted a validation report in its national language or has required the validator performing the validation to do so, a copy of the full validation report in the English language.’;

(28) point 12.0.2.1 is replaced by the following:

‘12.0.2.1 Subject to the provisions of 12.0.5, the following security equipment may be installed after 1 October 2020 only if it has been granted an “EU Stamp” marking or an “EU Stamp pending” marking status as referred to in point 12.0.2.5:

- (a) walk-through metal detection (WTMD) equipment;
- (b) explosive detection systems (EDS) equipment;

- (c) explosive trace detection (ETD) equipment;
- (d) liquid explosive detection systems (LEDS) equipment;
- (e) metal detection equipment (MDE);
- (f) security scanners;
- (g) shoe scanner equipment;
- (h) explosive vapour detection (EVD) equipment.’;

(29) point 12.0.2.3 is replaced by the following:

‘12.0.2.3 The “EU Stamp” marking shall be granted to security equipment tested by test centres which implement quality control measures in accordance with the Common Evaluation Process of the European Civil Aviation Conference under the responsibility of the appropriate authority.’;

(30) point 12.0.5.3 is replaced by the following:

‘12.0.5.3 Security equipment approved at national level on the basis of point 12.0.5.1 or 12.0.5.2 shall not automatically receive the “EU Stamp” marking.’;

(31) the following point 12.3.1 is added:

‘12.3.1 All equipment installed from 1 January 2023 at the latest, to be used for the screening of cargo and mail, as well as air carrier mail and air carrier materials subject to security controls in accordance with Chapter 6, shall be multi-view.

The appropriate authority, for objective reasons, may allow the use of single-view X-ray equipment installed before 1 January 2023 until the following dates:

- (a) single-view X-ray equipment installed before 1 January 2016, until 31 December 2025 at the latest;
- (b) single-view X-ray equipment installed from 1 January 2016, for a maximum period of 10 years from the date of its installation or at the latest until 31 December 2027, whichever is the earlier.

The appropriate authority shall inform the Commission where it applies the provisions of the second paragraph.’;

(32) point 12.4.2 is replaced by the following:

‘12.4.2 Standards for EDS

12.4.2.1 All EDS equipment shall fulfil the following requirements:

- (a) equipment installed before 1 September 2014 must at least meet standard 2;
- (b) equipment installed from 1 September 2014 to 31 August 2022 must at least meet standard 3;
- (c) equipment installed from 1 September 2022 to 31 August 2026 must at least meet standard 3.1;
- (d) equipment installed from 1 September 2026 must at least meet standard 3.2.

12.4.2.2 Standard 2 shall expire on 1 September 2021.

12.4.2.3 For the purposes of allowing an extension of the use of standard 2 EDS, there shall be four categories of airports:

- (a) category I – airport with more than 25 million passengers in 2019;
- (b) category II – airport with scheduled services to at least one of the third countries listed in Attachment 5-A of this Regulation, with the exception of the United Kingdom of Great Britain and Northern Ireland;
- (c) category III – airport with the highest volume of traffic in 2019 in each Member State where they are not already listed under category I or II;
- (d) category IV – other airport.

12.4.2.4 The appropriate authority may allow the use of standard 2 EDS as of 1 September 2021, in accordance with the following table, until:

	Standard 2 EDS equipment installed before 1 January 2011	Standard 2 EDS equipment installed between 1 January 2011 and 1 September 2014
Airports in Category I	1 March 2022	1 March 2023
Airports in Category II or Category III	1 September 2022	1 September 2023
Airports in Category IV	1 March 2023	1 March 2024

12.4.2.5 The appropriate authority shall inform the Commission when it allows the use of standard 2 EDS to continue as of 1 September 2021.

12.4.2.6 All EDS equipment designed to screen cabin baggage shall meet at least standard C1.

12.4.2.7 All EDS equipment designed to screen cabin baggage containing portable computers and other large electrical items shall meet at least standard C2.

12.4.2.8 All EDS equipment designed to screen cabin baggage containing portable computers and other large electrical items and LAGS shall meet at least standard C3.

12.4.2.9 All EDS equipment that meets standard C3 shall be considered as equivalent to LEDS equipment that meets standard 2 for the screening of LAGS.’.

COMMISSION IMPLEMENTING REGULATION (EU) 2021/256**of 18 February 2021****amending Annex I to Regulation (EC) No 798/2008 as regards the entry for the United Kingdom in the list of third countries, territories, zones or compartments from which certain poultry commodities may be imported into and transit through the Union in relation to highly pathogenic avian influenza****(Text with EEA relevance)**

THE EUROPEAN COMMISSION,

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

Having regard to Council Directive 2002/99/EC of 16 December 2002 laying down the animal health rules governing the production, processing, distribution and introduction of products of animal origin for human consumption ⁽¹⁾, and in particular the introductory phrase of Article 8, the first subparagraph of paragraph 1 of Article 8, paragraph 4 of Article 8 and Article 9(4) thereof,

Having regard to Council Directive 2009/158/EC of 30 November 2009 on animal health conditions governing intra-Community trade in, and imports from third countries of, poultry and hatching eggs ⁽²⁾, and in particular Articles 23(1), 24(2) and 25(2) thereof,

Whereas:

- (1) Commission Regulation (EC) No 798/2008 ⁽³⁾ lays down veterinary certification requirements for imports into and transit, including storage during transit, through the Union of poultry and poultry products ('the commodities'). It provides that the commodities are only to be imported into and transit through the Union from the third countries, territories, zones or compartments listed in columns 1 and 3 of the table in Part 1 of Annex I thereto.
- (2) Regulation (EC) No 798/2008 also lays down the conditions for a third country, territory, zone or compartment to be considered as free from highly pathogenic avian influenza (HPAI).
- (3) In accordance with the Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (Withdrawal Agreement), and in particular Article 5(4) of the Protocol on Ireland/Northern Ireland in conjunction with Annex 2 to that Protocol, Directives 2002/99/EC and 2009/158/EC, as well as the Commission acts based on them, apply to and in the United Kingdom in respect of Northern Ireland after the end of the transition period provided for in the Withdrawal Agreement.
- (4) Therefore, the United Kingdom, excluding Northern Ireland, is listed in the table in Part 1 of Annex I to Regulation (EC) No 798/2008 as a third country from which imports into and transit through the Union of certain poultry commodities are authorised from certain parts of its territory depending on the presence of HPAI. That regionalisation of the United Kingdom is set out in Part 1 of Annex I to Regulation (EC) No 798/2008, as amended by Commission Implementing Regulation (EU) 2021/169 ⁽⁴⁾.
- (5) On 12 February 2021, the United Kingdom confirmed the presence of HPAI of subtype H5N1 in a poultry holding in Glenrothes, Scotland.

⁽¹⁾ OJ L 18, 23.1.2003, p. 11.

⁽²⁾ OJ L 343, 22.12.2009, p. 74.

⁽³⁾ Commission Regulation (EC) No 798/2008 of 8 August 2008 laying down a list of third countries, territories, zones or compartments from which poultry and poultry products may be imported into and transit through the Community and the veterinary certification requirements (OJ L 226, 23.8.2008, p. 1).

⁽⁴⁾ Commission Implementing Regulation (EU) 2021/169 of 11 February 2021 amending Annex I to Regulation (EC) No 798/2008 as regards the entry for the United Kingdom in the list of third countries, territories, zones or compartments from which certain poultry commodities may be imported into and transit through the Union in relation to highly pathogenic avian influenza (OJ L 49, 12.2.2021, p. 18).

- (6) The veterinary authorities of the United Kingdom placed a 10 km control zone around the affected holding and implemented a stamping-out policy in order to control the presence of HPAI and limit the spread of that disease. Furthermore, the veterinary authorities of the United Kingdom confirmed that they immediately suspended issuing veterinary certificates for consignments of commodities intended for export to the Union from the whole of the territory of the United Kingdom, excluding Northern Ireland.
- (7) The United Kingdom has submitted information to the Commission on the epidemiological situation on its territory and the measures it has taken to prevent the further spread of HPAI which has now been evaluated by the Commission. On the basis of that evaluation, it is appropriate to place restrictions on the introduction into the Union of commodities from the area in Scotland affected by HPAI, which the veterinary authorities of the United Kingdom have placed under restrictions due to the current outbreak.
- (8) The entry for the United Kingdom in the table in Part 1 of Annex I to Regulation (EC) No 798/2008 should, therefore, be amended to take account of the current epidemiological situation in that third country.
- (9) Annex I to Regulation (EC) No 798/2008 should therefore be amended accordingly.
- (10) The measures provided for in this Regulation are in accordance with the opinion of the Standing Committee on Plants, Animals, Food and Feed,

HAS ADOPTED THIS REGULATION:

Article 1

Part 1 of Annex I to Regulation (EC) No 798/2008 is amended in accordance with the Annex to this Regulation.

Article 2

This Regulation shall enter into force on the third 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, 18 February 2021.

For the Commission
The President
Ursula VON DER LEYEN

In Part 1 of Annex I to Regulation (EC) No 798/2008, the entry for the United Kingdom is replaced by the following:

GB – United Kingdom (*)	GB-0	Whole country	SPF							
			EP, E							
	GB-1	The whole country of the United Kingdom, excluding area GB-2	BPP, BPR, DOC, DOR, HEP, HER, SRP, SRA, LT20		N			A		
			WGM							
			POU, RAT		N					
	GB-2	The territory of the United Kingdom corresponding to:								
	GB-2.1	North Yorkshire County: The area contained within a circle of a radius of 10 km, centered on WGS84 dec. coordinates N54.30 and W1.47	BPP, BPR, DOC, DOR, HEP, HER, SRP, SRA, LT20		N P2	1.1.2021	6.1.2021	A		
			WGM		P2	1.1.2021	6.1.2021			
			POU, RAT		N P2	1.1.2021	6.1.2021			
	GB-2.2	North Yorkshire County: The area contained within a circle of a radius of 10 km, centered on WGS84 dec. coordinates N54.29 and W1.45	BPP, BPR, DOC, DOR, HEP, HER, SRP, SRA, LT20		N P2	1.1.2021	8.1.2021	A		
			WGM		P2	1.1.2021	8.1.2021			
			POU, RAT		N P2	1.1.2021	8.1.2021			
	GB-2.3	Norfolk County: The area contained within a circle of a radius of 10 km, centered on WGS84 dec. coordinates N52.49 and E0.95	BPP, BPR, DOC, DOR, HEP, HER, SRP, SRA, LT20		N P2	1.1.2021	10.1.2021	A		
			WGM		P2	1.1.2021	10.1.2021			
			POU, RAT		N P2	1.1.2021	10.1.2021			
	GB-2.4	Norfolk County: The area contained within a circle of a radius of 10 km, centered on WGS84 dec. coordinates N52.72 and E0.15	BPP, BPR, DOC, DOR, HEP, HER, SRP, SRA, LT20		N P2	1.1.2021	11.1.2021	A		
			WGM		P2	1.1.2021	11.1.2021			
			POU, RAT		N P2	1.1.2021	11.1.2021			

GB-2.5	Derbyshire County: The area contained within a circle of a radius of 10 km, centered on WGS84 dec. coordinates N52.93 and W1.57	BPP, BPR, DOC, DOR, HEP, HER, SRP, SRA, LT20		N P2	1.1.2021	17.1.2021	A		
		WGM		P2	1.1.2021	17.1.2021			
		POU, RAT		N P2	1.1.2021	17.1.2021			
GB-2.6	North Yorkshire County: The area contained within a circle of a radius of 10 km, centered on WGS84 dec. coordinates N54.37 and W2.16	BPP, BPR, DOC, DOR, HEP, HER, SRP, SRA, LT20		N P2	1.1.2021	19.1.2021	A		
		WGM		P2	1.1.2021	19.1.2021			
		POU, RAT		N P2	1.1.2021	19.1.2021			
GB-2.7	Orkney Islands: The area contained within a circle of a radius of 10 km, centered on WGS84 dec. coordinates N59.28 and W2.44	BPP, BPR, DOC, DOR, HEP, HER, SRP, SRA, LT20		N P2	1.1.2021	20.1.2021	A		
		WGM		P2	1.1.2021	20.1.2021			
		POU, RAT		N P2	1.1.2021	20.1.2021			
GB-2.8	Dorset County: The area contained within a circle of a radius of 10 km, centered on WGS84 dec. coordinates N51.06 and W2.27	BPP, BPR, DOC, DOR, HEP, HER, SRP, SRA, LT20		N P2	1.1.2021	20.1.2021	A		
		WGM		P2	1.1.2021	20.1.2021			
		POU, RAT		N P2	1.1.2021	20.1.2021			
GB-2.9	Norfolk County: The area contained within a circle of a radius of 10 km, centered on WGS84 dec. coordinates N52.52 and E0.96	BPP, BPR, DOC, DOR, HEP, HER, SRP, SRA, LT20		N P2	1.1.2021	23.1.2021	A		
		WGM		P2	1.1.2021	23.1.2021			
		POU, RAT		N P2	1.1.2021	23.1.2021			
GB-2.10	Norfolk County: The area contained within a circle of a radius of 10 km, centered on WGS84 dec. coordinates N52.52 and E0.95	BPP, BPR, DOC, DOR, HEP, HER, SRP, SRA, LT20		N P2	1.1.2021	28.1.2021	A		
		WGM		P2	1.1.2021	28.1.2021			
		POU, RAT		N P2	1.1.2021	28.1.2021			

	GB-2.11	Norfolk County: The area contained within a circle of a radius of 10,4 km, centered on WGS84 dec. coordinates N52.53 and E0.66	BPP, BPR, DOC, DOR, HEP, HER, SRP, SRA, LT20		N P2	1.1.2021	7.2.2021	A		
			WGM		P2	1.1.2021	7.2.2021			
			POU, RAT		N P2	1.1.2021	7.2.2021			
	GB-2.12	Devon County: The area contained within a circle of a radius of 10 km, centred on WGS84 dec. coordinates N50.70 and W3.36	BPP, BPR, DOC, DOR, HEP, HER, SRP, SRA, LT20		N P2	1.1.2021	31.1.2021	A		
			WGM		P2	1.1.2021	31.1.2021			
			POU, RAT		N P2	1.1.2021	31.1.2021			
	GB-2.13	Near Amlwch, Isle of Anglesey, Wales: The area contained within a circle of a radius of 10 km, centred on WGS84 dec. coordinates N53.38 and W4.30	BPP, BPR, DOC, DOR, HEP, HER, SRP, SRA, LT20		N P2	27.1.2021		A		
			WGM		P2	27.1.2021				
			POU, RAT		N P2	27.1.2021				
	GB-2.14	Near Redcar, Redcar and Cleveland, England: The area contained within a circle of a radius of 10km, centred on WGS84 dec. coordinates N54.57 and W1.07	BPP, BPR, DOC, DOR, HEP, HER, SRP, SRA, LT20		N P2	8.2.2021		A		
			WGM		P2	8.2.2021				
			POU, RAT		N P2	8.2.2021				
	GB-2.15	Glenrothes, Fife, Scotland: The area contained within a circle of a radius of 10km, centred on WGS84 dec. coordinates N56.23 and W3.02	BPP, BPR, DOC, DOR, HEP, HER, SRP, SRA, LT20		N P2	12.2.2021		A		
			WGM		P2	12.2.2021				
			POU, RAT		N P2	12.2.2021				

(*) In accordance with the Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, and in particular Article 5(4) of the Protocol on Ireland/Northern Ireland in conjunction with Annex 2 to that Protocol, for the purposes of this Annex references to the United Kingdom do not include Northern Ireland.*.

DECISIONS

COUNCIL DECISION (CFSP) 2021/257

of 18 February 2021

in support of the Oslo Action Plan for the implementation of the 1997 Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Articles 28(1) and 31(1) thereof,

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

Whereas:

- (1) The Union should work towards a high degree of cooperation in all fields of international relations, in order, inter alia, to preserve peace, prevent conflicts and strengthen international security, in accordance with the purposes and principles of the Charter of the United Nations.
- (2) On 12 December 2003, the European Council adopted a European Security Strategy identifying global challenges and threats, and calling for a rule-based international order based on effective multilateralism and well-functioning international institutions.
- (3) The Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction (the 'Convention') entered into force on 1 March 1999. It constitutes the only comprehensive international instrument providing a comprehensive response to end the suffering and casualties caused by anti-personnel mines, including by prohibiting their use, stockpiling, production, trade and transfer and ensuring their destruction, as well as victim assistance. Since 1 June 2013, all Member States are party to the Convention.
- (4) On 23 June 2008, the Council adopted Joint Action 2008/487/CFSP ⁽¹⁾ in support of the universalisation and implementation of the Convention.
- (5) On 3 December 2009, at the Second Review Conference of the Convention, the States Parties to the Convention (the 'States Parties') adopted the Cartagena Action Plan 2010-2014 on the universalisation and implementation of all aspects of the Convention. At the Tenth Meeting of the States Parties in 2010, the States Parties adopted the Directive by the States Parties to the Implementation Support Unit, in which they agreed that the Convention's Implementation Support Unit (ISU) should provide advice and technical support to States Parties on the universalisation and implementation of the Convention, facilitate communication among the States Parties, and promote communication and information sharing regarding the Convention both to States not party to the Convention and to the public. At the Fourteenth Meeting of the States Parties in 2015, the States Parties adopted a Decision on strengthening financial governance and transparency within the ISU, setting out the conditions for the ISU to undertake activities or projects that do not feature in its yearly budget, including at the invitation of States Parties or States not party to the Convention.
- (6) On 13 November 2012, the Council adopted Decision 2012/700/CFSP ⁽²⁾ in support of the implementation of the Cartagena Action Plan 2010-2014.

⁽¹⁾ Council Joint Action 2008/487/CFSP of 23 June 2008 in support of the universalisation and implementation of the 1997 Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction, in the framework of the European Security Strategy (OJ L 165, 26.6.2008, p. 41).

⁽²⁾ Council Decision 2012/700/CFSP of 13 November 2012 in the framework of the European Security Strategy in support of the implementation of the Cartagena Action Plan 2010-2014, adopted by the States Parties to the 1997 Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction (OJ L 314, 14.11.2012, p. 40).

- (7) On 27 June 2014, at the Third Review Conference of the Convention, the States Parties adopted the Maputo Action Plan 2014-2019, which aimed to make significant and sustainable progress towards implementation of the Convention during the period 2014-2019, and made a joint declaration stating their aspiration to meet the goals of the Convention to the fullest extent possible by 2025.
- (8) In its conclusions of 16 and 17 June 2014 on the Third Review Conference of the Convention, the Council recalled the Union's unity in pursuing the objectives of the Convention and that the Union and its Member States have a long history of support for mine clearance and the destruction of stockpiled anti-personnel mines, as well as for assistance to victims of anti-personnel mines. Those conclusions reiterated the Union's unwavering support to States Parties in their full and effective implementation of the Convention, and its commitment to promote universalisation of the Convention, to provide resources to fund mine action, and concrete and sustainable assistance to anti-personnel mine victims, their families and communities.
- (9) On 4 August 2017, the Council adopted Decision (CFSP) 2017/1428 ⁽³⁾ in support of the implementation of the Maputo Action Plan 2014-2019.
- (10) On 25 June 2019, the Council adopted conclusions on an EU position on strengthening the ban against anti-personnel mines in light of the Fourth Review Conference of the Anti-Personnel Mine Ban Convention from 25 to 29 November 2019 in Oslo. The Council considered that, 20 years after its entry into force, the Convention has become a success story of disarmament diplomacy and an example of what the Union stands for: a rules-based international order, rooted in the respect for human rights and international humanitarian law. However, the Council acknowledged that the objectives of the Convention have not yet been achieved in full.
- (11) At the Fourth Review Conference of the Convention, held in Oslo in 2019, the States Parties adopted the Oslo Action Plan 2020-2024. The Oslo Action Plan 2020-2024 details the actions States Parties should take during the period 2020 to 2024 to support implementation of the Convention, building on the achievements of the previous Action Plans. As part of its mandate, the ISU supports the States Parties in the implementation of their obligations under the Convention and of their commitments under the Oslo Action Plan 2020-2024,

HAS ADOPTED THIS DECISION:

Article 1

1. To contribute to human security by supporting the implementation of the Oslo Action Plan 2020-2024 (the 'Oslo Action Plan') adopted by the States Parties at the Fourth Review Conference of the 1997 Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction (the 'Convention'), in the framework of the European Security Strategy and in accordance with relevant decisions of the international community, the Union shall pursue the following objectives:

- (a) to support the efforts of States Parties to implement the survey and clearance and mine risk education and reduction aspects of the Oslo Action Plan;
- (b) to support the efforts of States Parties to implement the victim assistance aspects of the Oslo Action Plan;
- (c) to promote the universalisation of the Convention and promote norms against any use, stockpiling, production and transfer of anti-personnel mines and on their destruction;

⁽³⁾ Council Decision (CFSP) 2017/1428 of 4 August 2017 in support of the implementation of the Maputo Action Plan for the implementation of the 1997 Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction (OJ L 204, 5.8.2017, p. 101).

- (d) to support the efforts of States Parties that retain anti-personnel mines for permitted purposes to increase reporting capabilities, ensure that the number of such mines retained does not exceed the minimum number absolutely necessary, and explore alternatives to live anti-personnel mines for training and research purposes where possible;
 - (e) to demonstrate the ongoing commitment of the Union and its Member States to the Convention and their resolve to cooperate with and extend assistance to those States Parties that need support in meeting their commitments under the Convention, thereby enhancing the leading role of the Union in pursuing the Convention's vision of a conclusive end to the suffering and casualties caused by anti-personnel mines.
2. The objectives referred to in paragraph 1 shall be pursued in such a way as to reinforce the Convention's tradition of partnership and collaboration between States, non-governmental organisations and other organisations, including representatives from mine-affected communities. All actions shall ensure an inclusive approach at all levels.
3. In order to achieve the objectives referred to in paragraph 1, the Union shall support the following projects:
- (a) support for implementation of Article 5 of the Convention, for international cooperation and assistance, and for transparency and exchange of information;
 - (b) support for implementation of victim assistance, for international cooperation and assistance, and for transparency and exchange of information;
 - (c) support for universalisation efforts and for promotion of the Convention's norms;
 - (d) support for alternatives to the use of live anti-personnel mines for training, and for increased cooperation and assistance;
 - (e) demonstrating the commitment of the Union and its Member States and ensuring their visibility, in particular through annual briefings to publicise the activities provided for in this Decision and their outcomes and through the organisation of a closing event, thereby underlining the Union's contribution to the implementation of the Convention.
4. A detailed description of the measures to be undertaken in order to meet the objectives referred to in paragraph 1 is set out in the Annex.

Article 2

1. The High Representative for the Union for Foreign Affairs and Security Policy (the 'High Representative') shall be responsible for the implementation of this Decision.
2. The technical implementation of the projects referred to in Article 1(3) shall be entrusted to the ISU, represented by the Geneva International Centre for Humanitarian Demining (GICHD).
3. The ISU shall implement the projects referred to in Article 1(3) under the responsibility of the High Representative. For that purpose, the High Representative shall enter into the necessary arrangements with the GICHD.

Article 3

1. The financial reference amount for the implementation of the projects referred to in Article 1(3) shall be EUR 2 658 139.
2. The expenditure financed by the amount set out in paragraph 1 shall be managed in accordance with the procedures and rules applicable to the general budget of the Union.
3. The Commission shall supervise the proper management of the expenditure financed by the amount set out in paragraph 1. For that purpose, it shall conclude a financing agreement with the GICHD, stipulating that the ISU is to ensure identity and visibility of the Union contribution, appropriate to its size.

4. The Commission shall endeavour to conclude the financing agreement referred to in paragraph 3 as soon as possible after the entry into force of this Decision. It shall inform the Council of any difficulties in the process and of the date of conclusion of the financing agreement.

5. The ISU shall implement the projects referred to in Article 1(3) in accordance with the Decision on strengthening financial governance and transparency within the ISU, taken at the Fourteenth Meeting of the States Parties in 2015. The ISU shall provide, amongst other reporting, narrative and quarterly reports, as well as a logical framework and activity matrix as set out in the Annex.

Article 4

The High Representative shall report to the Council on the implementation of this Decision on the basis of regular reports prepared by the ISU. Those reports shall form the basis for the evaluation by the Council. The Commission shall provide information on the financial aspects of the implementation of this Decision.

Article 5

1. This Decision shall enter into force on the date of its adoption.
2. This Decision shall expire 48 months after the date of conclusion of the financing agreement referred to in Article 3(3) or six months after the date of its adoption if no financing agreement has been concluded within that period.

Done at Brussels, 18 February 2021.

For the Council
The President
A. P. ZACARIAS

ANNEX

**PROJECT IN SUPPORT OF THE OSLO ACTION PLAN FOR THE IMPLEMENTATION OF THE 1997
CONVENTION ON THE PROHIBITION OF THE USE, STOCKPILING, PRODUCTION AND TRANSFER OF
ANTI-PERSONNEL MINES AND ON THEIR DESTRUCTION**

Background

To contribute to greater human security as envisioned through the European Security Strategy, by promoting acceptance of the norms and implementation of the Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction (the 'Convention'). The Union-backed project would support States Parties' efforts to implement various aspects of the Oslo Action Plan 2020-2024 (the 'OAP'), as adopted at the Fourth Review Conference of the Convention in November 2019.

The proposed Project would build on Joint Action 2008/487/CFSP and Council Decisions 2012/700/CFSP and (CFSP) 2017/1428, contributing inputs to preparations of the Fifth Review Conference of the Convention in 2024.

Project 1: Support for implementation of mine clearance (Article 5 of the Convention), for international cooperation and assistance (Article 6 of the Convention), and for transparency and exchange of information (Article 7 of the Convention)

1.1. Objectives

- To increase capacity to report and address contamination by anti-personnel mines including, where relevant, those of an improvised nature.
- To deliver context-specific mine risk education and reduction efforts.
- To establish sustainable national capacities to address previously unknown mined areas.
- To increase regular dialogue with stakeholders.
- To explore opportunities for cooperation (international, regional, triangular and south-south) to address remaining challenges.
- To improve reporting in line with the OAP and its indicators.

1.2. Description

With input from the Committee on Article 5 Implementation on the selection of beneficiary countries/regions, up to five national/regional events would be held in the Americas, Europe, Central or South-East Asia, the Middle East-North Africa (MENA) region, Horn of Africa and sub-Sahara regions.

The National or Regional Stakeholder Dialogues would seek to further improve cooperation and assistance on the implementation of OAP Actions related to Articles 5, 6, and 7 of the Convention. In some cases, those Dialogues would place special emphasis on the reporting of anti-personnel mines of an improvised nature. Priority for National Dialogues would be given to States with upcoming mine clearance deadlines that require support. In addition, Dialogues could be held in States that are close to completing mine clearance (Article 5 of the Convention) or that have recently done so in line with OAP Action 26.

Building on past successes, the events would consider and be informed by, at the design, management and implementation levels, the different needs and perspectives of women, girls, boys and men in mine-affected communities, and of mine action partners.

Dialogues would be organised and co-facilitated by the Implementation Support Unit (ISU) and beneficiary State Party together with relevant intergovernmental organisations partnering or co-hosting the event.

In the spirit of cooperation that has been a staple of the Convention, relevant Union entities and Member States, the Committee on Article 5 Implementation and the Committee on the Enhancement of Cooperation and Assistance, donor representatives, United Nations (UN) agencies, international and national mine clearance organisations, the International Campaign to Ban Landmines (ICBL) and other stakeholders would be involved. If resulting in sponsorship, such involvement would be subject to the conditions to be developed in the budgetary impact statement.

ISU-supported follow-up actions may be undertaken in response to recommendations resulting from the Dialogues or stemming from the relevant Committee's Observations and/or relevant Decisions of States Parties (e.g. Decisions on extension requests). Continuing with established practice, where beneficiary State Parties are involved in country coalitions or partnerships with the Union or its Member States, the ISU would work concertedly with all parties.

1.3. Results

- State representatives gain further knowledge of how to ensure OAP implementation through inclusive consultations with members of affected communities.
- State representatives gain awareness of the need to establish, as soon as possible and well ahead of completion, national capacities to address new or previously unknown mined areas following completion.
- State representatives build capacities to improve OAP reporting under the Guide of Reporting.
- State representatives learn about available cooperation and assistance to support their implementation efforts, as well as about steps they can take to encourage such cooperation and assistance, including through the establishment of National Mine Action Platforms.
- State representatives learn about challenges and gaps with regard to the implementation of their OAP commitments and evaluate in particular where they stand with respect to the OAP indicators.
- Based on the Dialogues, state representatives consider the revision, update or development of national mine clearance strategies or plans.
- The different perspectives of women, girls, boys and men and the needs of mine survivors and affected communities are considered and their meaningful participation is ensured.

1.4. Beneficiaries

- Women, girls, boys and men whose lives are affected by the presence or suspected presence of anti-personnel mines in States Parties that are in the process of implementing Article 5 obligations under the Convention or that have recently fulfilled such obligations.
- State representatives working on issues related to the implementation of the Convention, and in particular aspects related to mine clearance, and mine risk education and reduction.

Project 2: Support for implementation of victim assistance, for international cooperation and assistance (Article 6 of the Convention), and for transparency and exchange of information (Article 7 of the Convention)

2.1. Objectives

States Parties implement victim assistance ('VA') as part of wider disability rights and development approaches taking into account gender and mine survivors' diverse needs, including the needs of mine survivors in rural and remote areas.

2.2. Description

By adopting the OAP, the States Parties re-affirmed their commitment to 'ensuring the full, equal and effective participation of mine victims in society, based on respect for human rights, gender equality, inclusion and non-discrimination'.

Thanks to financial support provided through Decision (CFSP) 2017/1428, and as a follow-up to the global conference referred to in Decision 2012/700/CFSP, VA and disability rights practitioners from States Parties and not party with a significant number of survivors met at a global conference to further tie partnerships with the disability rights world at national and international levels.

This was achieved thanks to the participation of relevant national ministries, and vast expertise provided by the UN Secretary General's Special Envoy on Disability and Accessibility, the World Health Organization (WHO), the International Labour Organization (ILO), the International Committee of the Red Cross (ICRC), and expert ICBL-member organisations such as Humanity and Inclusion (HI), among others.

Building on that achievement, this Project would support a third global conference, with experienced VA practitioners, the UN Special Envoy on Disability and Accessibility and a Member of the Committee of the Convention on the Rights of Persons with Disabilities (CRPD), to review OAP implementation and contribute towards a new Action Plan to be adopted by the international community in 2024. Such a conference would take place at least a year prior to the Fifth Review Conference and would count on the participation and input of the Review Conference President-Designate.

With input from the Committee on Victim Assistance on the selection of the beneficiary countries/regions, the Project would extend its support to States Parties via National and/or Regional Stakeholders Dialogues in up to five events in the Americas, Europe, Central or South-East Asia, the MENA region, Horn of Africa and sub-Sahara regions. Those Dialogues would seek to support States Parties in strengthening their multi-sectoral efforts to ensure that VA implementation is in line with relevant CRPD provisions. The Dialogues would seek to strengthen and ensure inclusion and effective participation of mine victims and their representative organisations, in discussions to mobilise and secure resources and guarantee services from a rights-based perspective. In order to further strengthen those ties and maintain a cohesive plan to build and develop national capacities, the Project would also seek to host VA Experts Meetings prior to the Meetings of the States Parties as needed but, in any case, at least three times.

Building on past successes, the events would consider and be informed at the design, management and implementation levels by an inclusive process taking into consideration the different needs and perspectives of women, girls, boys and men who have survived the explosion of anti-personnel mines, mine-affected communities and the disability-rights community, including mine survivors in rural and remote areas. This would ensure added value to the efforts being undertaken at national levels.

The Dialogues would be organised and co-facilitated by the ISU and beneficiary State Party and, where relevant, with the regional intergovernmental organisation co-sponsoring the Dialogue. In the spirit of cooperation that has been a staple of the Convention, relevant Union entities and Member States, the Committee on Victim Assistance and the Committee on the Enhancement of Cooperation and Assistance, donor representatives, UN agencies including the WHO and the Office of the UN High Commissioner for Human Rights, international and national mine clearance organisations, the ICRC and other stakeholders such as the ICBL and member organisations such as HI would be involved. If resulting in sponsorship, such involvement would be subject to the conditions to be developed in the budgetary impact statement.

ISU-supported follow-up actions may be undertaken in response to recommendations resulting from the Dialogues or stemming from the relevant Committee's Observations and/or relevant conclusions of the National/Regional Dialogues. This would include sponsorship of relevant VA practitioners and/or representatives of mine survivor organisations to participate in technical exchange visits or to attend formal or informal meetings of the Convention. Continuing with established practice, where beneficiary State Parties are involved in country coalitions or partnerships with the Union or its Member States, the ISU would work concertedly with all parties.

2.3. Results

- State representatives increase knowledge on how best to ensure a multi-sectoral response to implement their VA obligations, and integrate VA into broader national policies, plans and legal frameworks.
- States gain understanding on the need to ensure that a relevant government entity is assigned to oversee VA integration into broader frameworks, and on the need to develop an action plan based on specific, measurable, realistic and time-bound objectives to support mine victims.
- States increase inclusion in their VA approach, in particular by including, or increasing participation of, mine survivors' or disability rights' organisations in national planning and as part of delegations following the Project's activities.

- State representatives learn about challenges and gaps with regard to the implementation of their OAP commitments and evaluate in particular where they stand with respect to the OAP indicators.
- Based on the Dialogues, state representatives consider the revision, update or development of their national strategies on persons with disabilities.
- Mine survivors' and disability rights' organisations further develop their capacities and/or are empowered following the Project's activities.
- State representatives build capacities to improve OAP reporting under the Guide of Reporting.
- States and victim representative organisations increase partnerships with relevant humanitarian, peacebuilding, development, and human rights communities bearing in mind the 2030 Agenda for Sustainable Development.

2.4. Beneficiaries

- Women, girls, boys and men injured by anti-personnel mines and other explosive remnants of war, and other mine victims, including in rural and remote areas.
- VA experts working on issues relevant to VA.
- Disability rights practitioners working in States with a significant number of mine survivors.

Project 3: Support for universalisation efforts and for promotion of the Convention's norms

3.1. Objective

States not party move closer to accession with relevant officials developing expressed affinity for the Convention and/or the international norms against anti-personnel mines.

3.2. Description

The Oslo Declaration on a Mine-Free World sees States pledge 'to promote and defend' the norms established by the Convention, and 'to spare no effort to universalise the Convention' based on their 'obligations under international law, including international humanitarian law and human rights law'.

The OAP identifies two Actions to ensure an increase in membership of the Convention and a strengthening of the norms of the Convention. OAP Actions 11 and 12 call on States Parties to 'use all available avenues to promote ratification of/accession to the Convention by States not party including by encouraging their participation in the work of the Convention' and 'to continue to promote universal observance of the Convention's norms and objectives'.

For that purpose, and with input from the Convention President and informal universalisation group, where relevant, the Project would carry out a variety of universalisation efforts. Those would include high-level visits, technical meetings and/or workshops, sponsorship of relevant officials from target States to attend Convention meetings, and ambassadorial-level meetings at the UN headquarters or any of its subsidiary regional headquarters.

At least five activities would be carried out with support of the Convention community including Union Member States and Union Delegations in target States. Continuing with established practice, where the Union or its Member States are involved in country coalitions or partnerships in target States, the ISU would work concertedly with all parties.

Whenever possible, a high-level political approach would be followed up with technical workshops informed by expert input from States leading universalisation efforts, ICBL, ICRC, UN Country Teams, and/or relevant organisations. Those workshops would be carried out at either national, sub-regional or regional levels with relevant ministry(ies) or institution(s) of the target States. The Project would seek to sponsor relevant delegates from target States to attend Convention meetings. This would ensure that States Parties can follow up with target States, and that Convention meetings remain on the target States' radar. The ISU would coordinate such sponsorship as permitted under the budgetary impact statement.

In addition, the ISU would host a technical 'follow-up' meeting at a national, sub-regional or regional level with a State not party previously targeted by either a Union Decision or a Union Joint Action.

3.3. Results

- Decision-makers in States not party gain increased knowledge of the Convention and its norms and/or of support available for accession.
- Relevant state officials gain increased understanding of the work of the Convention.
- States not party publicly express rapprochement with or affinity for the Convention and its norms (e.g. attend a formal or informal meeting of the Convention).
- As a result of the missions, national mine action and/or universalisation stakeholders are reinvigorated to push for universalisation.
- The role of the Union in advancing the Convention and its norms is highlighted among the Convention community, Union officials, and States not party.
- At least one target State not party provides a voluntary Article 7 report.

3.4. Beneficiaries

- States which have not yet ratified, approved, accepted or acceded to the Convention.
- States Parties and international and non-governmental organisations involved in efforts to promote the universalisation of the Convention.
- Women, girls, boys and men in States where a landmine ban is put into place.

Project 4: Support for alternatives to the use of live anti-personnel mines for training (Article 3 of the Convention), and for increased cooperation and assistance (Article 6)

4.1. Objective

States that retain anti-personnel mines for permitted purposes act upon OAP Action 16 including by increasing reporting, and OAP Action 17 by exploring alternatives to live anti-personnel mines.

4.2. Description

There are currently 66 States Parties retaining more than 150 000 anti-personnel mines for permitted purposes under Article 3 of the Convention. While information received from States Parties indicates that this number is decreasing, a handful of States Parties have not submitted annual transparency information on their retained anti-personnel mines for many years.

In order to support States Parties that may wish to act upon OAP Actions 16 and 17, the proposed Project, with input from the Convention President, would support a national or regional seminar with at least two States that request such assistance. States Parties, including Member States, and relevant organisations can provide lessons learnt and roadmaps to replace live anti-personnel mines for training. Continuing with established practice, where the Union or its Member States are involved in country coalitions or partnerships with beneficiary State Parties, the ISU would work concertedly with all parties.

The project would also support a technical workshop on alternatives to using live anti-personnel mines. Whenever relevant and/or possible, Union Member States and other States Parties would be invited to share lessons learnt on alternatives for training and research, and/or destruction of retained anti-personnel mines, further enhancing cooperation and assistance among the Convention community. For that purpose, the Project would involve the Committee on Cooperative Compliance and the Committee on the Enhancement of Cooperation and Assistance.

4.3. Results

- States Parties increase reporting on Article 3 of the Convention in annual transparency reports.
- States Parties in a position to do so engage in cooperation and assistance towards States Parties wanting to take action on Article 3 commitments, and in relation to OAP Actions 16 and 17.
- Updated knowledge is gained by States Parties retaining large number of anti-personnel mines with at least one State Party making inroads towards using alternatives for training.

4.4. Beneficiaries

- States Parties with Article 3 commitments.
- State officials with responsibility for mine clearance training programmes.
- Women, girls, boy and men in States Parties where retained anti-personnel mines are destroyed.

Project 5: Demonstrating the commitment of the Union and its Member States and ensuring their visibility

5.1. Objective

The Convention community and beneficiary State Parties gain understanding on the contribution of the Union and its Member States towards implementation of the Convention, while officials of the Union and of its Member States gain awareness of this Decision and how it may relate to their work.

5.2. Description

As per the previous Council Decisions and Joint Action, the ISU would undertake to highlight the role of the Union and its Member States among the Convention community and in beneficiary and target States. For that purpose and under the Communication and Visibility Plan, the ISU would hold regular briefings, in particular during Convention meetings, throughout the Project's implementation phase and hold a closing event.

The ISU would undertake media campaigns and publications promoting the Convention's accomplishment. The ISU would ensure that the role of the Union in this campaign is highlighted.

As established by prior practice, the ISU would submit narrative monthly reports to the Union and quarterly reports to the Union and its Member States on implementation of the project.

5.3. Results

- Officials of the Union and of its Member States would be aware of this Decision and how it may relate to their work.
 - The Union's and Member States' commitment to the Convention and mine action in general would be put in the spotlight before the States Parties and a global audience interested in human security.
 - Awareness of the objectives of the Convention among the international community would be strengthened.
-

COUNCIL DECISION (CFSP) 2021/258
of 18 February 2021
amending Decision 2011/101/CFSP concerning restrictive measures in view of the situation in Zimbabwe

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Article 29 thereof,

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

Whereas:

- (1) On 15 February 2011, the Council adopted Decision 2011/101/CFSP ⁽¹⁾ concerning restrictive measures in view of the situation in Zimbabwe.
- (2) The Council has carried out a review of Decision 2011/101/CFSP, taking into account the political situation in Zimbabwe.
- (3) The restrictive measures should be extended until 20 February 2022. The Council should keep them under constant review in the light of political and security developments in Zimbabwe.
- (4) The entry for one deceased person should be deleted from the list of designated persons and entities in Annex I to Decision 2011/101/CFSP. The restrictive measures should be renewed for three persons and one entity set out in that Annex, and the identifying information and grounds for designation for two persons set out in that Annex should be updated. The suspension of the restrictive measures should be renewed for three persons listed in Annex II to that Decision and one deceased person should be deleted from Annex II to that Decision.
- (5) Decision 2011/101/CFSP should therefore be amended accordingly,

HAS ADOPTED THIS DECISION:

Article 1

Decision 2011/101/CFSP is amended as follows:

- (1) Article 10 is replaced by the following:

'Article 10

1. This Decision shall enter into force on the date of its adoption.
 2. This Decision shall apply until 20 February 2022.
 3. The measures referred to in Article 4(1) and Article 5(1) and (2), in so far as they apply to persons listed in Annex II, shall be suspended until 20 February 2022.
 4. This Decision shall be kept under constant review and shall be renewed, or amended as appropriate, if the Council deems that its objectives have not been met.;
- (2) Annex I is replaced by Annex I to this Decision;
- (3) Annex II is amended as set out in Annex II to this Decision.

Article 2

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

⁽¹⁾ Council Decision 2011/101/CFSP of 15 February 2011 concerning restrictive measures against Zimbabwe (OJ L 42, 16.2.2011, p. 6).

Done at Brussels, 18 February 2021.

For the Council
The President
A. P. ZACARIAS

ANNEX I

PERSONS AND ENTITIES REFERRED TO IN ARTICLES 4 AND 5

I. Persons

	Name (and any aliases)	Identifying information	Grounds for designation
2.	MUGABE, Grace	Born 23.7.1965 Passport AD001159 ID 63-646650Q70	Former Secretary of the ZANU-PF (Zimbabwe African National Union – Patriotic Front) Women's league, involved in activities that seriously undermine democracy, respect for human rights and the rule of law. Took over the Iron Mask Estate in 2002; alleged to illicitly derive large profits from diamond mining.
5.	CHIWENGA, Constantine	Vice-President Former Commander of the Zimbabwe Defence Forces, retired General, born 25.8.1956 Passport AD000263 ID 63-327568M80	Vice-President and former Commander of the Zimbabwe Defence Forces. Member of Joint Operational Command and complicit in forming or directing repressive state policy. Used army for farm takeovers. During 2008 elections was a prime architect of the violence associated with the process of the Presidential run-off.
7.	SIBANDA, Phillip Valerio (a.k.a. Valentine)	Commander of the Zimbabwe Defence Forces Former Commander of the Zimbabwe National Army, General, born 25.8.1956 or 24.12.1954 ID 63-357671H26	Commander of the Zimbabwe Defence Forces and former Commander of the Zimbabwe National Army. Senior army figure with ties to the Government and complicit in forming or directing oppressive state policy.

II. Entities

	Name	Identifying information	Grounds for designation
1.	Zimbabwe Defence Industries	10th floor, Trustee House, 55 Samora Machel Avenue, PO Box 6597, Harare, Zimbabwe.	Associated with the Ministry of Defence and the ZANU-PF faction of Government.

ANNEX II

In Annex II to Decision 2011/101/CFSP, the entry for the following person is deleted:

‘4. Shiri, Perence (a.k.a. Bigboy) Samson Chikerema’.

COMMISSION DECISION (EU, Euratom) 2021/259**of 10 February 2021****laying down implementing rules on industrial security with regard to classified grants**

THE EUROPEAN COMMISSION,

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

Having regard to the Treaty establishing the European Atomic Energy Community, and in particular Article 106 thereof,

Having regard to Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 ⁽¹⁾,

Having regard to Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission ⁽²⁾,

Having regard to Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information ⁽³⁾,

Having regard to Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission ⁽⁴⁾,

After consulting the Commission Security Expert Group, in accordance with Article 41(5) of Decision (EU, Euratom) 2015/444,

Whereas:

- (1) Articles 41, 42, 47 and 48 of Decision (EU, Euratom) 2015/444 provide that more detailed provisions to supplement and support Chapter 6 of that Decision are to be laid down in implementing rules on industrial security, governing issues such as the award of classified grant agreements, facility security clearances, personnel security clearances, visits and transmission and carriage of European Union classified information ('EUCI').
- (2) Decision (EU, Euratom) 2015/444 states that classified grant agreements are to be implemented in close cooperation with the national security authority, the designated security authority or any other competent authority of the Member States concerned. The Member States have agreed to ensure that any entity under their jurisdiction which may receive or generate classified information originating in the Commission is appropriately security cleared and is capable of providing suitable protection equivalent to that afforded by the security rules of the Council of the European Union for protecting EU classified information bearing a corresponding classification marking, as provided for in the Agreement between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union (2011/C 202/05) ⁽⁵⁾.

⁽¹⁾ OJ L 193, 30.7.2018, p. 1.

⁽²⁾ OJ L 72, 17.3.2015, p. 41.

⁽³⁾ OJ L 72, 17.3.2015, p. 53.

⁽⁴⁾ OJ L 6, 11.1.2017, p. 40.

⁽⁵⁾ OJ C 202, 8.7.2011, p. 13.

- (3) The Council, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy have agreed to ensure maximum consistency in the application of security rules regarding their protection of EUCI, while taking into account their specific institutional and organisational needs, in accordance with the declarations attached to the minutes of the Council session at which Council Decision 2013/488/EU ⁽⁶⁾ on the security rules for protecting EU classified information was adopted.
- (4) The Commission's implementing rules on industrial security with regard to classified grants should therefore also ensure maximum consistency and take into account the Guidelines on Industrial Security approved by the Council Security Committee on 13 December 2016.
- (5) On 4 May 2016 the Commission adopted a decision ⁽⁷⁾ empowering the Member of the Commission responsible for security matters to adopt, on behalf of the Commission and under its responsibility, the implementing rules provided for in Article 60 of Decision (EU, Euratom) 2015/444,

HAS ADOPTED THIS DECISION:

CHAPTER 1

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. This Decision sets out implementing rules on industrial security with regard to classified grants within the meaning of Decision (EU, Euratom) 2015/444, and in particular Chapter 6 of that Decision.
2. This Decision lays down specific requirements to ensure the protection of EU classified information (EUCI) in the publication of calls, and when awarding grants and implementing the classified grant agreements concluded by the European Commission.
3. This Decision applies to grants involving information classified at the following levels:
 - (a) RESTREINT UE/EU RESTRICTED;
 - (b) CONFIDENTIEL UE/EU CONFIDENTIAL;
 - (c) SECRET UE/EU SECRET.
4. This Decision applies without prejudice to specific rules laid down in other legal acts, such as those concerning the European Defence Industrial Development Programme.

Article 2

Responsibilities within the Commission

1. As part of the responsibilities of the authorising officer of the granting authority referred to in Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council, he or she shall ensure that the classified grant complies with Decision (EU, Euratom) 2015/444 and its implementing rules.

⁽⁶⁾ Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information (OJ L 274, 15.10.2013, p. 1).

⁽⁷⁾ Commission Decision of 4.5.2016 on an empowerment relating to security (C(2016) 2797 final).

2. To that end, the authorising officer concerned shall, at all stages, seek the advice of the Commission security authority on issues regarding the security elements of a classified grant agreement, programme or project, and shall inform the local security officer about the signed classified grant agreements. The decision on the classification level of specific subjects shall rest with the granting authority and shall be taken with due regard to the security classification guide.
3. Where the programme or project security instructions referred to in Article 5(3) are applied, the granting authority and the Commission security authority shall discharge the responsibilities assigned to them in those instructions.
4. In respecting the requirements of these implementing rules, the Commission security authority shall cooperate closely with the national security authorities ('NSAs') and the designated security authorities ('DSAs') of the Member States concerned, in particular as regards facility security clearances ('FSCs') and personnel security clearances ('PSCs'), visit procedures and transportation plans.
5. Where grants are managed by EU executive agencies or other funding bodies and the specific rules laid down in other legal acts referred to in Article 1(4) do not apply:
 - (a) the delegating Commission department shall exercise the rights pertaining to the originator of EUCI generated in the context of the grants if the delegation arrangements so provide;
 - (b) the delegating Commission department shall be responsible for determining the security classification;
 - (c) requests for security clearance information and the notifications to NSAs and/or DSAs shall be sent through the Commission security authority.

CHAPTER 2

HANDLING OF CALLS FOR CLASSIFIED GRANTS

Article 3

Basic principles

1. Classified parts of the grants shall be implemented only by beneficiaries registered in a Member State, or by beneficiaries registered in a third country or established by an international organisation where that third country or international organisation has concluded a security of information agreement with the Union or entered into an administrative arrangement with the Commission ⁽⁸⁾.
2. Before launching a call for a classified grant, the granting authority shall determine the security classification of any information that could be provided to applicants. The granting authority shall also determine the maximum security classification of any information used or generated in the performance of the grant agreement or programme or project, or at least the anticipated volume and type of information to be produced or handled, and the need for a classified communication and information system (CIS).
3. The granting authority shall ensure that calls for classified grants provide information about the special security obligations related to classified information. The call documentation shall include clarifications about the timeline for beneficiaries to obtain the FSCs, where they are required. Annexes I and II contain sample templates for information regarding the call conditions.

⁽⁸⁾ The list of agreements concluded by the EU and of administrative arrangements entered into by the European Commission, under which EU classified information may be exchanged with third countries and international organisations, can be found on the Commission website.

4. The granting authority shall ensure that information classified RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET is disclosed to applicants only after they have signed a non-disclosure agreement, obliging applicants to handle and protect EUCI in accordance with Decision (EU, Euratom) 2015/444, its implementing rules and the applicable national rules.

5. Where RESTREINT UE/EU RESTRICTED information is provided to applicants, the minimum requirements mentioned in Article 5(7) of this Decision shall be included in the call or in the non-disclosure arrangements concluded at proposal stage.

6. All applicants and beneficiaries which are required to handle or store information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET within their facilities, either at the proposal stage or during the performance of the classified grant agreement itself, shall hold an FSC at the required level, except for cases mentioned in paragraph 9. The following identifies the three scenarios that may arise during the proposal stage for a classified grant involving EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level:

- (a) no access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level during the proposal stage:

Where the call concerns a grant that will involve EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level, but does not require the applicant to handle such information at the proposal stage, an applicant which does not hold an FSC at the required level shall not be excluded from the application process on the grounds that it does not hold an FSC;

- (b) access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level on the premises of the granting authority during the proposal stage:

Access shall be granted to applicant personnel who hold a PSC at the required level and who have a need-to-know;

- (c) handling or storage of EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level on the premises of the applicant during the proposal stage:

Where the call requires applicants to handle or store EUCI on their premises, the applicant shall hold an FSC at the required level. In such circumstances, the granting authority shall obtain, through the Commission security authority, an assurance from the relevant NSA or DSA that the applicant has been granted an appropriate FSC before any EUCI material is provided to the applicant. Access shall be granted to applicant personnel who hold a PSC at the required level and who have a need-to-know.

7. In principle, an FSC or PSC shall not be required for access to RESTREINT UE/EU RESTRICTED information, either at the proposal stage or for the performance of the grant agreement. Where Member States require an FSC or PSC for grant agreements or subcontracts at RESTREINT UE/EU RESTRICTED level under their national laws and regulations, as listed in Annex IV, those national requirements shall not place any additional obligations on other Member States or exclude applicants, beneficiaries or subcontractors from Member States that have no such FSC or PSC requirements for access to RESTREINT UE/EU RESTRICTED information from related grant agreements or subcontracts, or a competition for such. Those grant agreements shall be performed in Member States in accordance with their national laws and regulations.

8. Where an FSC is required in the handling of a call and for the implementation of a classified grant agreement, the granting authority shall submit, through the Commission security authority, a request to the beneficiary's NSA or DSA using a facility security clearance information sheet ('FSCIS') or any established equivalent electronic form. Annex III, Appendix D, contains an example of an FSCIS ⁽⁹⁾. Response to an FSCIS is provided, to the extent possible, within ten working days of the date of the request.

9. Where Member States' government establishments or establishments under the control of their government participate in classified grants that require FSCs, and where FSCs are not issued for those establishments under national laws, the granting authority shall verify with the NSA or DSA concerned, through the Commission security authority, whether those government establishments are capable of handling EUCI at the required level.

⁽⁹⁾ Other forms used may differ from the example provided in these implementing rules in their design.

10. Where a PSC is required for the performance of a classified grant agreement and where, according to national rules, an FSC is necessary before a PSC is granted, the granting authority shall check with the beneficiary's NSA or DSA, through the Commission security authority, using an FSCIS, that the beneficiary holds an FSC or that the FSC process is underway. In this case, the Commission shall not issue requests for PSCs using personnel security clearance information sheet ('PSCIS').

Article 4

Subcontracting in classified grants

1. The conditions under which beneficiaries may subcontract action tasks involving EUCI shall be defined in the call and in the grant agreement. These conditions shall include the requirement that all FSCISs shall be submitted through the Commission security authority. Subcontracting shall be subject to prior written consent from the granting authority. Where applicable, subcontracting shall comply with the basic act establishing the programme.
2. Classified parts of the grants shall be subcontracted only to entities registered in a Member State, or to entities registered in a third country or established by an international organisation where that third country or international organisation has concluded a security of information agreement with the Union or entered into an administrative arrangement with the Commission ⁽¹⁰⁾.

CHAPTER 3

HANDLING OF CLASSIFIED GRANTS

Article 5

Basic principles

1. When awarding a classified grant, the granting authority, together with the Commission security authority, shall ensure that the beneficiaries' obligations regarding the protection of EUCI used or generated in the performance of the grant agreement are an integral part of the grant agreement. Grant-specific security requirements shall take the form of a security aspects letter ('SAL'). A sample template for a SAL is set out in Annex III.
2. Before signing a classified grant, the granting authority shall approve a security classification guide ('SCG') for the tasks to be performed and information generated in the implementation of the grant, or at programme or project level, where applicable. The SCG shall be part of the SAL.
3. Programme- or project-specific security requirements shall take the form of a programme (or project) security instruction ('PSI'). The PSI may be drafted using the provisions of the SAL template as set out in Annex III. The PSI shall be developed by the Commission department managing the programme or project, in close cooperation with the Commission security authority, and submitted for advice to the Commission Security Expert Group. Where a grant agreement is part of a programme or project with its own PSI, the SAL of the grant agreement shall have a simplified form and shall include reference to the security provisions set out in the PSI of the programme or project.
4. Except for cases mentioned in Article 3(9), the classified grant agreement shall not be signed until the applicant's NSA or DSA has confirmed the applicant's FSC, or, where the classified grant agreement is awarded to a consortium, until the NSA or DSA of at least one applicant, within the consortium, or more if necessary, has confirmed that applicant's FSC.
5. In principle, and save provided otherwise in other relevant rules, the granting authority shall be considered the originator of EUCI generated in the performance of the grant agreement.

⁽¹⁰⁾ The list of agreements concluded by the EU and of administrative arrangements entered into by the European Commission, under which EU classified information may be exchanged with third countries and international organisations, can be found on the Commission website.

6. The granting authority, through the Commission security authority, shall notify the NSAs and/or DSAs of all beneficiaries and subcontractors about the signature of classified grant agreements or subcontracts and any extensions or early terminations of such grant agreements or subcontracts. A list of country requirements is provided in Annex IV.

7. Grant agreements involving information classified RESTREINT UE/EU RESTRICTED shall include a security clause making the provisions set out in Annex III, Appendix E binding upon beneficiaries. Those grant agreements shall include an SAL setting out, as a minimum, the requirements for handling RESTREINT UE/EU RESTRICTED information including information assurance aspects and specific requirements to be fulfilled by the beneficiaries regarding the accreditation of their CIS handling RESTREINT UE/EU RESTRICTED information.

8. Where this is required by Member States' national laws and regulations, NSAs or DSAs ensure that beneficiaries or subcontractors under their jurisdiction comply with the applicable security provisions for the protection of RESTREINT UE/EU RESTRICTED information and conduct verification visits to beneficiaries' or subcontractors' facilities located in their territory. Where the NSA or DSA is not under such an obligation, the granting authority shall ensure that the beneficiaries implement the required security provisions set out in Annex III, Appendix E.

Article 6

Access to EUCI by staff of beneficiaries and subcontractors

1. The granting authority shall ensure that classified grant agreements include provisions stating that staff of beneficiaries or subcontractors who, for the performance of the classified grant agreement or subcontract, require access to EUCI, may be granted that access only if:

- (a) it has been established that they have a need-to-know;
- (b) for information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, they have been security cleared at the relevant level by the respective NSA or DSA or any other competent security authority;
- (c) they have been briefed on the applicable security rules for protecting EUCI, and have acknowledged their responsibilities with regard to protecting such information.

2. Where applicable, access to EUCI shall also be in compliance with the basic act establishing the programme and take account of any additional markings defined in the SCG.

3. If a beneficiary or subcontractor wishes to employ a national of a non-EU country in a position that requires access to EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, it is the responsibility of the beneficiary or subcontractor to initiate the security clearance procedure of such a person in accordance with national laws and regulations applicable at the location where access to the EUCI is to be granted.

Article 7

Access to EUCI by experts participating in checks, reviews or audits

1. Where external persons ('experts') are involved in checks, reviews or audits conducted by the granting authority or in performance reviews of the beneficiaries that require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, they shall be provided with a contract only if they have been security cleared at the relevant level by the respective NSA or DSA or any other competent security authority. The granting authority, through the Commission security authority, shall check and, where necessary, ask the NSA or DSA to initiate the vetting process for experts at least six months prior to the start of their respective contracts.

2. Before signing their contracts, the experts shall be briefed on the applicable security rules for protecting EUCI, and shall have acknowledged their responsibilities with regard to protecting such information.

CHAPTER 4

VISITS IN CONNECTION WITH CLASSIFIED GRANT AGREEMENTS

*Article 8***Basic principles**

1. Where the granting authority, experts, beneficiaries or subcontractors require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET on each other's premises in the context of the implementation of a classified grant agreement, visits shall be arranged in liaison with the NSAs or DSAs or any other competent security authorities concerned.
2. The visits referred to in paragraph 1 shall be subject to the following requirements:
 - (a) the visit shall have an official purpose related to the classified grant;
 - (b) any visitor shall hold a PSC at the required level and shall have a need-to-know in order to access EUCI used or generated in the performance of the classified grant.

*Article 9***Requests for visits**

1. Visits by beneficiaries or subcontractors to other beneficiaries' or subcontractors' facilities, or to granting authority premises, that involve access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be arranged in accordance with the following procedure:
 - (a) the security officer of the facility sending the visitor shall complete all relevant parts of the request for visit (RFV) form and submit the request to the facility's NSA or DSA. A template for the RFV form is set out in Annex III, Appendix C;
 - (b) the sending facility's NSA or DSA needs to confirm the visitor's PSC before submitting the RFV to the host facility's NSA or DSA (or the Commission security authority if the visit is to the premises of a granting authority);
 - (c) the security officer of the sending facility shall then obtain from its NSA or DSA the reply of the host facility's NSA or DSA (or the Commission security authority) either authorising or denying the RFV;
 - (d) an RFV is considered approved if no objections are raised until five working days before the date of the visit.
2. Visits by granting authority officials or experts or auditors to beneficiaries' or subcontractors' facilities that involve access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be arranged in accordance with the following procedure:
 - (a) the visitor shall complete all relevant parts of the RFV form and submit it to the Commission security authority;
 - (b) the Commission security authority shall confirm the PSC of the visitor before submitting the RFV to the host facility's NSA or DSA;
 - (c) the Commission security authority shall obtain a reply from the host facility's NSA or DSA either authorising or denying the RFV;
 - (d) an RFV is considered approved if no objections are raised until five working days before the date of the visit.
3. An RFV may cover either a single visit or recurring visits. In the case of recurring visits, the RFV may be valid for up to one year from the start date requested.
4. The validity of any RFV shall not exceed the validity of the visitor's PSC.
5. As a general rule, an RFV should be submitted to the host facility's competent security authority at least 15 working days before the date of the visit.

*Article 10***Visit procedures**

1. Before allowing visitors to have access to EUCI, the security office of the host facility shall comply with all the visit-related security procedures and rules laid down by its NSA or DSA.
2. Visitors shall prove their identity upon arrival at the host facility by presenting a valid ID card or passport. That identification information shall correspond to the information supplied in the RFV.
3. The host facility shall ensure that records are kept of all visitors, including their names, the organisation they represent, the date of expiry of the PSC, the date of the visit and the names of the persons visited. Such records shall be retained for a period of at least five years, or longer if required by the national rules and regulations of the country where the host facility is located.

*Article 11***Visits arranged directly**

1. In the context of specific projects, the relevant NSAs or DSAs and the Commission security authority may agree on a procedure whereby visits for a specific classified grant can be arranged directly between the visitor's security officer and the security officer of the facility to be visited. A template of the form to be used for this purpose is set out in Annex III, Appendix C. Such an exceptional procedure shall be set out in the PSI or other specific arrangements. In such cases, the procedures set out in Article 9 and Article 10(1) shall not apply.
2. Visits involving access to information classified RESTREINT UE/EU RESTRICTED shall be arranged directly between the sending and receiving entity, without the need to follow the procedures set out in Article 9 and Article 10(1).

CHAPTER 5

TRANSMISSION AND CARRIAGE OF EUCI IN PERFORMANCE OF CLASSIFIED GRANT AGREEMENTS*Article 12***Basic principles**

The granting authority shall ensure that all decisions related to EUCI transfer and carriage are in accordance with Decision (EU, Euratom) 2015/444 and its implementing rules, and with the terms of the classified grant agreement, including the consent of the originator.

*Article 13***Electronic handling**

1. Electronic handling and transmission of EUCI shall be carried out in accordance with Chapters 5 and 6 of Decision (EU, Euratom) 2015/444 and its implementing rules.

The communication and information systems owned by a beneficiary and used to handle EUCI for the performance of the grant agreement ('beneficiary CIS') shall be subject to accreditation by the security accreditation authority responsible ('SAA'). Any electronic transmission of EUCI shall be protected by cryptographic products approved in accordance with Article 36(4) of Decision (EU, Euratom) 2015/444. TEMPEST security measures shall be implemented in accordance with Article 36(6) of that Decision.

2. The security accreditation of the beneficiary CIS handling EUCI at RESTREINT UE/EU RESTRICTED level and of any interconnection thereof may be delegated to the security officer of a beneficiary if this is permitted by national laws and regulations. Where that task is delegated, the beneficiary shall be responsible for implementing the minimum security requirements described in the SAL when handling RESTREINT UE/EU RESTRICTED information on its CIS. However, the relevant NSAs or DSAs, and SAAs retain responsibility for the protection of RESTREINT UE/EU RESTRICTED information handled by the beneficiary and the right to inspect the security measures taken by the beneficiary. In addition, the beneficiary shall provide the granting authority and, where required by national laws and regulations, the competent national SAA, with a statement of compliance certifying that the beneficiary CIS and related interconnections have been accredited for handling EUCI at RESTREINT UE/EU RESTRICTED level ⁽¹¹⁾.

Article 14

Transport by commercial couriers

The transport of EUCI by commercial couriers shall abide by the relevant provisions of Commission Decision (EU, Euratom) 2019/1962 ⁽¹²⁾ on implementing rules for handling RESTREINT UE/EU RESTRICTED information and Commission Decision (EU, Euratom) 2019/1961 ⁽¹³⁾ on implementing rules for handling CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information.

Article 15

Hand carriage

1. The carriage of classified information by hand shall be subject to strict security requirements.
2. RESTREINT UE/EU RESTRICTED information may be hand carried by beneficiary personnel within the Union, provided the following requirements are met:
 - (a) the envelope or packaging used is opaque and bears no indication of the classification of its contents;
 - (b) the classified information does not leave the possession of the bearer;
 - (c) the envelope or packaging is not opened *en route*.
3. For information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET, hand carriage by beneficiary personnel within a Member State is arranged in advance between the sending and receiving entities. The dispatching authority or facility informs the receiving authority or facility of the details of the consignment, including reference, classification, expected time of arrival and name of courier. Such hand carriage is permitted, provided the following requirements are met:
 - (a) the classified information is carried in a double envelope or packaging;
 - (b) the outer envelope or packaging is secured and bears no indication of the classification of its contents, while the inner envelope bears the level of classification;
 - (c) EUCI does not leave the possession of the bearer;
 - (d) the envelope or packaging is not opened *en route*;
 - (e) the envelope or packaging is carried in a lockable briefcase or similar approved container of such size and weight that it can be retained at all times in the personal possession of the bearer and not be consigned to a baggage hold;
 - (f) the courier carries a courier certificate issued by his or her competent security authority authorising the courier to carry the classified consignment as identified.

⁽¹¹⁾ The minimum requirements for communication and information systems handling EUCI at RESTREINT UE/EU RESTRICTED level are laid down in Annex III, Appendix E.

⁽¹²⁾ Commission Decision (EU, Euratom) 2019/1962 of 17 October 2019 on implementing rules for handling RESTREINT UE/EU RESTRICTED information (OJ L 311, 2.12.2019, p. 21).

⁽¹³⁾ Commission Decision (EU, Euratom) 2019/1961 of 17 October 2019 on implementing rules for handling CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information (OJ L 311, 2.12.2019, p. 1).

4. For hand carriage by beneficiary personnel of information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET from one Member State to another, the following additional rules shall apply:

- (a) the courier shall be responsible for the safe custody of the classified material carried until it is handed over to the recipient;
- (b) in the event of a security breach, the sender's NSA or DSA may request that the authorities in the country where the breach occurred carry out an investigation, report their findings and take legal or other action as appropriate;
- (c) the courier shall have been briefed on all the security obligations to be observed during carriage and shall have signed an appropriate acknowledgement;
- (d) the instructions for the courier shall be attached to the courier certificate;
- (e) the courier shall have been provided with a description of the consignment and an itinerary;
- (f) the documents shall be returned to the issuing NSA or DSA upon completion of the journey(s) or be kept available by the recipient for monitoring purposes;
- (g) if customs, immigration authorities or border police ask to examine and inspect the consignment, they shall be permitted to open and observe sufficient parts of the consignment so as to establish that it contains no material other than that which is declared;
- (h) customs authorities should be urged to honour the official authority of the shipping documents and of the authorisation documents carried by the courier.

If a consignment is opened by customs, this should be done out of sight of unauthorised persons and in the presence of the courier where possible. The courier shall request that the consignment be repacked and shall ask the authorities conducting the inspection to reseal the consignment and confirm in writing that it was opened by them.

5. Hand carriage by beneficiary personnel of information classified RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET to a third country or an international organisation shall be subject to the provisions of the security of information agreement or the administrative arrangement concluded between, respectively, the Union or the Commission and that third country or international organisation.

CHAPTER 6

BUSINESS CONTINUITY PLANNING

Article 16

Contingency plans and recovery measures

The granting authority shall ensure that the classified grant agreement requires the beneficiaries to set out business contingency plans ('BCP') for protecting EUCI handled in the context of the classified grant in emergency situations, and to put in place preventive and recovery measures in the context of business continuity planning to minimise the impact of incidents in relation to the handling and storage of EUCI. The beneficiaries shall confirm to the granting authority that their BCPs are in place.

Article 17

Entry into force

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

Done at Brussels, 10 February 2021.

*For the Commission,
On behalf of the President,
Johannes HAHN
Member of the Commission*

ANNEX I

STANDARD INFORMATION IN THE CALL

*(to be adapted to the call used)**Security*

Projects involving EU classified information must undergo security scrutiny to authorise funding and may be made subject to specific security rules (detailed in a security aspects letter (SAL) which is annexed to the Grant Agreement).

These rules (governed by Commission Decision (EU, Euratom) 2015/444 ⁽¹⁾ and/or national rules) provide for instance that:

- projects involving information classified TRES SECRET UE/EU TOP SECRET (or equivalent) can **NOT** be funded;
- classified information must be marked in accordance with the applicable security instructions in the SAL;
- information with classification levels CONFIDENTIEL UE/EU CONFIDENTIAL or above (and RESTREINT UE/EU RESTRICTED if required by national rules) may be:
 - created or accessed only on premises with facility security clearing from the competent national security authority (NSA), in accordance with the national rules;
 - handled only in a secured area accredited by the competent NSA;
 - accessed and handled only by persons with a valid personnel security clearance (PSC) and a need-to-know;
- at the end of the grant, the classified information must either be returned or continued to be protected in accordance with the applicable rules;
- action tasks involving EU classified information (EUCI) may be subcontracted only with prior written approval from the granting authority and only to entities established in an EU Member State or in a non-EU country with a security of information agreement with the EU (or an administrative arrangement with the Commission);
- disclosure of EUCI to third parties is subject to prior written approval from the granting authority.

Please note that, depending on the type of activity, facility security clearing may have to be provided before grant signature. The granting authority will assess the need for clearings in each case and will establish their delivery date during grant preparation. Please note that in **no circumstances** can we sign any grant agreement until at least one of the beneficiaries in a consortium has facility security clearing.

Further security recommendations may be added to the Grant Agreement in the form of security deliverables (*e.g. create security advisory group, limit level of detail, use fake scenario, exclude use of classified information, etc.*).

Beneficiaries must ensure that their projects are not subject to national/third-country security requirements that could affect implementation or put into question the award of the grant (*e.g. technology restrictions, national security classification, etc.*). The granting authority must be notified immediately of any potential security issues.

[*additional OPTION for FPAs: For framework partnerships, both the framework partnership applications and the grant applications may have to undergo security scrutiny.*]

⁽¹⁾ See Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

ANNEX II

STANDARD GRANT AGREEMENT CLAUSES

(to be adapted to the grant agreement used)

13.2 Security – Classified information

The parties must handle classified information (EU or national) in accordance with the applicable EU or national law on classified information (in particular, Commission Decision (EU, Euratom) 2015/444 ⁽¹⁾ and its implementing rules).

Specific security rules (if any) are set out in Annex 5.

ANNEX 5

Security – EU classified information

[OPTION for actions with EU classified information (standard): If EU classified information is used or generated by the action, it must be treated in accordance with the security classification guide (SCG) and security aspect letter (SAL) set out in Annex 1 and Decision (EU, Euratom) 2015/444 and its implementing rules – until it is declassified.]

Deliverables which contain EU classified information must be submitted according to special procedures agreed with the granting authority.

Action tasks involving EU classified information may be subcontracted only with prior explicit written approval from the granting authority and only to entities established in an EU Member State or in a non-EU country with a security of information agreement with the EU (or an administrative arrangement with the Commission).

EU classified information may not be disclosed to any third party (including participants involved in the action implementation) without prior explicit written approval from the granting authority.]

⁽¹⁾ Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

*ANNEX III***[Annex IV (to the)]****SECURITY ASPECTS LETTER (SAL) ⁽¹⁾****[Model]**

⁽¹⁾ This model of SAL applies where the Commission is considered the originator of classified information created and handled for the performance of the grant agreement. Where the originator of classified information created and handled for the performance of the grant agreement is not the Commission, and where a specific security framework is set up by the Member States participating in the grant, other models of SAL may apply.

Appendix A

SECURITY REQUIREMENTS

The granting authority must include the following security requirements in the security aspects letter (SAL). Some clauses may not be applicable to the grant agreement. These are shown in square brackets.

The list of clauses is not exhaustive. Further clauses may be added depending on the nature of the classified grant.

GENERAL CONDITIONS [N.B.: applicable to all classified grant agreements]

1. This security aspects letter (SAL) is an integral part of the classified grant agreement [or subcontract] and describes grant agreement-specific security requirements. Failure to meet these requirements may constitute sufficient grounds to terminate the grant agreement.
2. Grant beneficiaries are subject to all obligations set out in Commission Decision (EU, Euratom) 2015/444 ⁽²⁾ (hereinafter 'CD 2015/444') and its implementing rules ⁽³⁾. If the grant beneficiary faces a problem of application of the applicable legal framework in a Member State, it must refer to the Commission security authority and the national security authority (NSA) or designated security authority (DSA).
3. Classified information generated when performing the grant agreement must be marked as EU classified information (EUCI) at security classification level, as determined in the security classification guide (SCG) in Appendix B to this letter. Deviation from the security classification level stipulated by the SCG is permissible only with the written authorisation of the granting authority.
4. The rights pertaining to the originator of any EUCI created and handled for the performance of the classified grant agreement are exercised by the Commission, as the granting authority.
5. Without the written consent of the granting authority, the beneficiary or subcontractor must not make use of any information or material furnished by the granting authority or produced on behalf of that authority for any purpose other than that of the grant agreement.
6. Where a facility security clearance (FSC) is required for the performance of a grant agreement, the beneficiary must ask the granting authority to proceed with the FSC request.
7. The beneficiary must investigate all security breaches related to EUCI and report them to the granting authority as soon as is practicable. The beneficiary or subcontractor must immediately report to its NSA or DSA, and, where national laws and regulations so permit, to the Commission security authority, all cases in which it is known or there is reason to suspect that EUCI provided or generated pursuant to the grant agreement has been lost or disclosed to unauthorised persons.

⁽²⁾ Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

⁽³⁾ The granting authority should insert the references once these implementing rules have been adopted.

8. After the end of the grant agreement, the beneficiary or subcontractor must return any EUCI it holds to the granting authority as soon as possible. Where practicable, the beneficiary or subcontractor may destroy EUCI instead of returning it. This must be done in accordance with the national laws and regulations of the country where the beneficiary is based, with the prior agreement of the Commission security authority, and under the latter's instruction. EUCI must be destroyed in such a way that it cannot be reconstructed, either wholly or in part.
9. Where the beneficiary or subcontractor is authorised to retain EUCI after termination or conclusion of the grant agreement, the EUCI must continue to be protected in accordance with CD 2015/444 and with its implementing rules ⁽⁴⁾.
10. Any electronic handling, processing and transmission of EUCI must abide by the provisions laid down in Chapters 5 and 6 of CD 2015/444. These include, *inter alia*, the requirement that communication and information systems owned by the beneficiary and used to handle EUCI for the purpose of the grant agreement (hereinafter 'beneficiary CIS') must be subject to accreditation ⁽⁵⁾; that any electronic transmission of EUCI must be protected by cryptographic products approved in accordance with Article 36(4) of CD 2015/444, and that TEMPEST security measures must be implemented in accordance with Article 36(6) of CD 2015/444.
11. The beneficiary or subcontractor shall have business contingency plans (BCPs) to protect any EUCI handled in the performance of the classified grant agreement in emergency situations and shall put in place preventive and recovery measures to minimise the impact of incidents associated with the handling and storage of EUCI. The beneficiary or subcontractor must inform the granting authority of its BCP.

**GRANT AGREEMENTS REQUIRING ACCESS TO INFORMATION CLASSIFIED RESTREINT UE/EU
RESTRICTED**

12. In principle, personnel security clearance (PSC) is not required for compliance with the grant agreement ⁽⁶⁾. However, information or material classified RESTREINT UE/EU RESTRICTED must be accessible only to beneficiary personnel who require such information to perform the grant agreement (*need-to-know principle*), who have been briefed by the beneficiary's security officer on their responsibilities and on the consequences of any compromise or breach of security of such information, and who have acknowledged in writing the consequences of a failure to protect EUCI.
13. Except where the granting authority has given its written consent, the beneficiary or subcontractor must not provide access to information or material classified RESTREINT UE/EU RESTRICTED to any entity or person other than those of its personnel who have a need-to-know.
14. The beneficiary or subcontractor must maintain the security classification markings of classified information generated by or provided during the performance of a grant agreement and must not declassify information without written consent from the granting authority.
15. Information or material classified RESTREINT UE/EU RESTRICTED must be stored in locked office furniture when not in use. When in transit, documents must be carried inside an opaque envelope. The documents must not leave the possession of the bearer and they must not be opened *en route*.

⁽⁴⁾ The granting authority should insert the references once these implementing rules have been adopted.

⁽⁵⁾ The party undertaking the accreditation will have to provide the granting authority with a statement of compliance, through the Commission security authority, and in co-ordination with the relevant national security accreditation authority (SAA).

⁽⁶⁾ Where beneficiaries are from Member States requiring PSCs and/or FSCs for grants classified RESTREINT UE/EU RESTRICTED, the granting authority lists in the SAL these PSC and FSC requirements for the beneficiaries in question.

16. The beneficiary or subcontractor may transmit documents classified RESTREINT UE/EU RESTRICTED to the granting authority using commercial courier companies, postal services, hand carriage or electronic means. To this end, the beneficiary or subcontractor must follow the programme (or project) security instruction (PSI) issued by the Commission and/or the Commission implementing rules on industrial security with regard to classified grants ⁽⁷⁾.
17. When no longer required, documents classified RESTREINT UE/EU RESTRICTED must be destroyed in such a way that they cannot be reconstructed, either wholly or in part.
18. The security accreditation of beneficiary CIS handling EUCI at RESTREINT UE/EU RESTRICTED level and any interconnection thereof may be delegated to the beneficiary's security officer if national laws and regulations so permit. Where accreditation is thus delegated, the NSAs, DSAs or security accreditation authorities (SAAs) retain responsibility for protecting any RESTREINT UE/EU RESTRICTED information that is handled by the beneficiary and the right to inspect the security measures taken by the beneficiary. In addition, the beneficiary shall provide the granting authority and, where required by national laws and regulations, the competent national SAA with a statement of compliance certifying that the beneficiary CIS and the related interconnections have been accredited for handling EUCI at RESTREINT UE/EU RESTRICTED level.

HANDLING OF INFORMATION CLASSIFIED RESTREINT UE/EU RESTRICTED IN COMMUNICATION AND INFORMATION SYSTEMS (CIS)

19. Minimum requirements for CIS handling information classified RESTREINT UE/EU RESTRICTED are laid down in Appendix E to this SAL.

CONDITIONS UNDER WHICH THE BENEFICIARY MAY SUBCONTRACT

20. The beneficiary must obtain permission from the granting authority before subcontracting any part of a classified grant agreement.
21. No subcontract may be awarded to an entity registered in a non-EU country or to an entity belonging to an international organisation, if that non-EU country or international organisation has not concluded a security of information agreement with the EU or an administrative arrangement with the Commission.
22. Where the beneficiary has let a subcontract, the security provisions of the grant agreement shall apply *mutatis mutandis* to the subcontractor(s) and its (their) personnel. In such a case, it is the beneficiary's responsibility to ensure that all subcontractors apply these principles to their own subcontracting arrangements. To ensure appropriate security oversight, the beneficiary's and subcontractor's NSAs and/or DSAs shall be notified by the Commission security authority of the letting of all related classified subcontracts at the levels of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET. Where appropriate, the beneficiary's and subcontractor's NSAs and/or DSAs shall be provided with a copy of the subcontract-specific security provisions. NSAs and DSAs requiring notification about the security provisions of classified grant agreements at RESTREINT UE/EU RESTRICTED level are listed in the annex to the Commission's implementing rules on industrial security with regard to classified grant agreements ⁽⁸⁾.
23. The beneficiary may not release any EUCI to a subcontractor without the prior written approval of the granting authority. If EUCI to subcontractors is to be sent frequently or as a matter of routine, then the granting authority may give its approval for a specified length of time (e.g. 12 months) or for the duration of the subcontract.

⁽⁷⁾ The granting authority should insert the references once these implementing rules have been adopted.

⁽⁸⁾ The granting authority should insert the references once these implementing rules have been adopted.

VISITS

If the standard request for visit (RFV) procedure is to be applied to visits involving information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, the granting authority must include paragraphs 24, 25 and 26 and delete paragraph 27. If visits involving information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET are arranged directly between the sending and receiving establishments, the granting authority must delete paragraphs 25 and 26 and include paragraph 27 only.

24. Visits involving access or potential access to information classified RESTREINT UE/EU RESTRICTED shall be arranged directly between the sending and receiving establishments without the need to follow the procedure described in paragraphs 25 to 27 below.
- [25. Visits involving access or potential access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be subject to the following procedure:
 - (a) the security officer of the facility sending the visitor shall complete all relevant parts of the RFV form (Appendix C) and submit the request to the facility's NSA or DSA;
 - (b) the sending facility's NSA or DSA needs to confirm the visitor's PSC before submitting the RFV to the host facility's NSA or DSA (or to the Commission security authority if the visit is to the premises of the granting authority);
 - (c) the security officer of the sending facility shall then obtain from its NSA or DSA the reply of the host facility's NSA or DSA (or the Commission security authority) either authorising or denying the RFV;
 - (d) an RFV is considered approved if no objections are raised until five working days before the date of the visit.]
- [26. Before giving the visitor(s) access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, the host facility must have received authorisation from its NSA or DSA.]
- [27. Visits involving access or potential access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be arranged directly between the sending and receiving establishments (an example of the form that may be used for this purpose is provided in Appendix C).]
28. Visitors must prove their identity on arrival at the host facility by presenting a valid ID card or passport.
29. The facility hosting the visit must ensure that records are kept of all visitors. These must include their names, the organisation they represent, the date of expiry of the PSC (if applicable), the date of the visit and the name(s) of the person(s) visited. Without prejudice to European data protection rules, such records are to be retained for a period of no less than five years or in accordance with national rules and regulations, as appropriate.

ASSESSMENT VISITS

30. The Commission security authority may, in cooperation with the relevant NSAs or DSAs, conduct visits to beneficiaries' or subcontractors' facilities to check that the security requirements for handling EUCI are being complied with.

SECURITY CLASSIFICATION GUIDE

31. A list of all the elements in the grant agreement which are classified or to be classified in the course of the performance of the grant agreement, the rules for so doing and the specification of the applicable security classification levels are contained in the security classification guide (SCG). The SCG is an integral part of this grant agreement and can be found in Appendix B to this Annex.

*Appendix B***SECURITY CLASSIFICATION GUIDE**

[specific text to be adjusted depending on the subject of the grant agreement]

Appendix C

REQUEST FOR VISIT (MODEL)

DETAILED INSTRUCTIONS FOR COMPLETION OF REQUEST FOR VISIT

(The application must be submitted in English only)

HEADING	Check boxes for visit type, information type, and indicate how many sites are to be visited and the number of visitors.
4. ADMINISTRATIVE DATA	To be completed by requesting NSA/DSA.
5. REQUESTING ORGANISATION OR INDUSTRIAL FACILITY	Give full name and postal address. Include city, state and post code as applicable.
6. ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED	Give full name and postal address. Include city, state, post code, telex or fax number (if applicable), telephone number and e-mail. Give the name and telephone/fax numbers and e-mail of your main point of contact or the person with whom you have made the appointment for the visit. Remarks: (1) Giving the correct post code (zip code) is important because a company may have various different facilities. (2) When applying manually, Annex 1 can be used when two or more facilities have to be visited in connection with the same subject. When an Annex is used, item 3 should state: 'SEE ANNEX 1, NUMBER OF FAC:...' (state number of facilities).
7. DATES OF VISIT	Give the actual date or period (date-to-date) of the visit in the format 'day – month – year'. Where applicable, give an alternate date or period in brackets.
8. TYPE OF INITIATIVE	Specify whether the visit has been initiated by the requesting organisation or facility or by invitation of the facility to be visited.
9. THE VISIT RELATES TO:	Specify the full name of the project, contract or call for tender using commonly used abbreviations only.
10. SUBJECT TO BE DISCUSSED/ JUSTIFICATION	Give a brief description of the reason(s) for the visit. Do not use unexplained abbreviations. Remarks: In the case of recurring visits this item should state 'Recurring visits' as the first words in the data element (e. g. Recurring visits to discuss_____).
11. ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED	State SECRET UE/EU SECRET (S-UE/EU-S) or CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C), as appropriate.

12. PARTICULARS OF VISITOR	Remark: when more than two visitors are involved in the visit, Annex 2 should be used.
13. THE SECURITY OFFICER OF THE REQUESTING ENTITY	This item requires the name, telephone number, fax number and e-mail of the requesting facility's Security Officer.
14. CERTIFICATION OF SECURITY CLEARANCE	This field is to be completed by the certifying authority. Notes for the certifying authority: a. Give name, address, telephone number, fax number and e-mail (can be pre-printed). b. This item should be signed and stamped (if applicable).
15. REQUESTING SECURITY AUTHORITY	This field is to be completed by the NSA/DSA. Note for the NSA/DSA: a. Give name, address, telephone number, fax number and e-mail (can be pre-printed). b. This item should be signed and stamped (if applicable).

All fields must be completed and the form submitted via Government-to-Government channels ⁽⁹⁾

REQUEST FOR VISIT (MODEL)		
TO: _____		
1. TYPE OF VISIT REQUEST	2. TYPE OF INFORMATION	3. SUMMARY
☐ Single ☐ Recurring ☐ Emergency ☐ Amendment ☐ Dates ☐ Visitors ☐ Facility For an amendment, insert the NSA/DSA original RFV Reference No _____	☐ C-UE/EU-C ☐ S-UE/EU-S	No of sites: _____ No of visitors: _____
4. ADMINISTRATIVE DATA:		
Requester:	NSA/DSA RFV Reference No _____	
To:	Date (dd/mm/yyyy): ____/____/____	

⁽⁹⁾ If it has been agreed that visits involving access or potential access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET level can be arranged directly, the completed form can be submitted directly to the Security Officer of the establishment to be visited.

5. REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:

NAME:

POSTAL ADDRESS:

E-MAIL ADDRESS:

FAX NO:

TELEPHONE NO:

6. ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED (*Annex 1 to be completed*)**7. DATE OF VISIT (dd/mm/yyyy): FROM ____/____/____ TO ____/____/____****8. TYPE OF INITIATIVE:**

- ☐ Initiated by requesting organisation or facility
- ☐ By invitation of the facility to be visited

9. THE VISIT RELATES TO CONTRACT:**10. SUBJECT TO BE DISCUSSED/REASONS/PURPOSE (Include details of host entity and any other relevant information. Abbreviations should be avoided):****11. ANTICIPATED HIGHEST CLASSIFICATION LEVEL OF INFORMATION/MATERIAL OR SITE ACCESS TO BE INVOLVED:****12. PARTICULARS OF VISITOR(S) (*Annex 2 to be completed*)****13. THE SECURITY OFFICER OF THE REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

14. CERTIFICATION OF SECURITY CLEARANCE LEVEL:

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

DATE (dd/mm/yyyy):
____/____/____

STAMP

15. REQUESTING NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY:

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

DATE (dd/mm/yyyy):

____/____/____

STAMP

16. REMARKS (*Mandatory justification required in the case of an emergency visit*):

<Placeholder for reference to applicable personal data legislation and link to mandatory information for the data subject, e.g. how Article 13 of the General Data Protection Regulation ⁽¹⁰⁾ is implemented.>

⁽¹⁰⁾ 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).

ANNEX 1 to RFV FORM

ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED
1. NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:
2. NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO: (Continue as required)

<Placeholder for reference to applicable personal data legislation and link to mandatory information for the data subject, e.g. how Article 13 of the General Data Protection Regulation ⁽¹⁾ is implemented.>

⁽¹⁾ 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).

ANNEX 2 to RFV FORM

PARTICULARS OF VISITOR(S)
1. SURNAME: FIRST NAMES (<i>as per passport</i>): DATE OF BIRTH (<i>dd/mm/yyyy</i>): ____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/ORGANISATION:
2. SURNAME: FIRST NAMES (<i>as per passport</i>): DATE OF BIRTH (<i>dd/mm/yyyy</i>): ____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/ORGANISATION: (Continue as required)

<Placeholder for reference to applicable personal data legislation and link to mandatory information for the data subject, e.g. how Article 13 of the General Data Protection Regulation ⁽¹²⁾ is implemented.>

⁽¹²⁾ 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).

Appendix D

FACILITY SECURITY CLEARANCE INFORMATION SHEET (FSCIS) (MODEL)**1. INTRODUCTION**

- 1.1. Attached is a sample Facility Security Clearance Information Sheet (FSCIS) for the rapid exchange of information between the National Security Authority (NSA) or Designated Security Authority (DSA), other competent national security authorities and the Commission Security Authority (acting on behalf of granting authorities) with regard to the Facility Security Clearance (FSC) of a facility involved in application for, and implementation of, classified grants or subcontracts.
- 1.2. The FSCIS is valid only if stamped by the relevant NSA, DSA or other competent authority.
- 1.3. The FSCIS is divided into a request and reply section and can be used for the purposes identified above or for any other purposes for which the FSC status of a particular facility is required. The reason for the enquiry must be identified by the requesting NSA or DSA in field 7 of the request section.
- 1.4. The details contained in the FSCIS are not normally classified; accordingly, when an FSCIS is to be sent between the respective NSAs/DSAs/Commission this should preferably be done by electronic means.
- 1.5. NSAs/DSAs should make every effort to respond to an FSCIS request within ten working days.
- 1.6. Should any classified information be transferred or a grant or subcontract awarded in relation to this assurance, the issuing NSA or DSA must be informed.

Procedures and instructions for the use of the Facility Security Clearance Information Sheet (FSCIS)

These detailed instructions are for the NSA or DSA, or the granting authority and the Commission Security Authority that complete the FSCIS. The request should preferably be typed in capital letters.

HEADER	The requester inserts full NSA/DSA and country name.
1. REQUEST TYPE	The requesting granting authority selects the appropriate checkbox for the type of FSCIS request. Include the level of security clearance requested. The following abbreviations should be used: SECRET UE/EU SECRET = S-UE/EU-S CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C CIS = Communication and information systems for processing classified information.
2. SUBJECT DETAILS	Fields 1 to 6 are self-evident. In field 4 the standard two-letter country code should be used. Field 5 is optional.
3. REASON FOR REQUEST	Give the specific reason for the request, provide project indicators, number of the call or grant. Please specify the need for storage capability, CIS classification level, etc. Any deadline/expiry/award dates which may have a bearing on the completion of an FSC should be included.

4. REQUESTING NSA/DSA	State the name of the actual requester (on behalf of the NSA/DSA) and the date of the request in number format (dd/mm/yyyy).
5. REPLY SECTION	Fields 1-5: select appropriate fields. Field 2: if an FSC is in progress, it is recommended to give the requester an indication of the required processing time (if known). Field 6: (a) Although validation differs by country or even by facility, it is recommended that the expiry date of the FSC be given. (b) In cases where the expiry date of the FSC assurance is indefinite, this field may be crossed out. (c) In compliance with respective national rules and regulations, the requester or either the beneficiary or subcontractor is responsible for applying for a renewal of the FSC.
6. REMARKS	May be used for additional information with regard to the FSC, the facility or the foregoing items.
7. ISSUING NSA/DSA	State the name of the providing authority (on behalf of the NSA/DSA) and the date of the reply in number format (dd/mm/yyyy).

FACILITY SECURITY CLEARANCE INFORMATION SHEET (FSCIS) (MODEL)

All fields must be completed and the form communicated via Government-to-Government or Government-to-international organisation channels.

REQUEST FOR A FACILITY SECURITY CLEARANCE ASSURANCE

TO: _____

(NSA/DSA Country name)

Please complete the reply boxes, where applicable:

[] Provide an FSC assurance at the level of: [] S-UE/EU-S [] C-UE/EU-C

for the facility listed below

[] Including safeguarding of classified material/information

[] Including Communication and Information Systems (CIS) for processing classified information

[] Initiate, directly or upon a corresponding request of a beneficiary or subcontractor, the process of obtaining an FSC up to and including the level of with level of safeguarding and level of CIS, if the facility does not currently hold these levels of capabilities.

Confirm accuracy of the details of the facility listed below and provide corrections/additions as required.

1. Full facility name:

Corrections/Additions:

.....

.....

2. Full facility address:

.....

.....

3. Postal address (if different from 2)

.....

.....

4. Zip/post code/city/country

.....

.....

5. Name of the Security Officer

.....

.....

6. Telephone/Fax/E-mail of the Security Officer

.....

.....

7. This request is made for the following reason(s): (provide details of the pre-contractual (proposal selection) stage, grant or subcontract, programme/project, etc.)

.....

Requesting NSA/DSA/granting authority:

Date: (dd/mm/yyyy).....

Name:

REPLY (within ten working days)

This is to certify that:

1. ☐ the abovementioned facility holds an FSC up to and including the level of ☐ S-UE/EU-S
☐ C-UE/EU-C.
2. The abovementioned facility has the capability to safeguard classified information/material:
☐ yes, level: ☐ no.
3. the abovementioned facility has accredited/authorised CIS:
☐ yes, level: ☐ no.
4. ☐ in relation to the abovementioned request, the FSC process has been initiated. You will be informed when the FSC has been established or refused.
5. ☐ the abovementioned facility does not hold an FSC.
6. This FSC assurance expires on: (dd/mm/yyyy), or as advised otherwise by the NSA/DSA. In the case of earlier invalidation or any changes to the information listed above, you will be informed.
7. Remarks:
.....

Issuing NSA/DSA Name:..... Date:(dd/mm/yyyy).....

<Placeholder for reference to applicable personal data legislation and link to mandatory information for the data subject, e.g. how Article 13 of the General Data Protection Regulation ⁽¹³⁾ is implemented.>

⁽¹³⁾ 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).

*Appendix E***Minimum requirements for protection of EUCI in electronic form at RESTREINT UE/EU RESTRICTED level handled in the beneficiary's CIS*****General***

1. The beneficiary must be responsible for ensuring that the protection of RESTREINT UE/EU RESTRICTED information complies with the minimum security requirements as laid down in this security clause and with any other additional requirements advised by the granting authority or, if applicable, by the national security authority (NSA) or designated security authority (DSA).
2. It is the beneficiary's responsibility to implement the security requirements identified in this document.
3. For the purpose of this document, a communication and information system (CIS) covers all equipment used to handle, store and transmit EUCI, including workstations, printers, copiers, fax machines, servers, network management systems, network controllers and communications controllers, laptops, notebooks, tablet PCs, smart phones and removable storage devices such as USB-sticks, CDs, SD-cards, etc.
4. Special equipment, such as cryptographic products, must be protected in accordance with its dedicated security operating procedures (SecOPs).
5. Beneficiary must establish a structure responsible for the security management of the CIS handling information classified RESTREINT UE/EU RESTRICTED and appoint a security officer responsible for the facility concerned.
6. The use of IT solutions (hardware, software or services) privately owned by beneficiary staff for storing or processing RESTREINT UE/EU RESTRICTED information is not permitted.
7. Accreditation of the beneficiary's CIS handling information classified RESTREINT UE/EU RESTRICTED must be approved by the security accreditation authority (SAA) of the Member State concerned or delegated to the beneficiary's security officer as permitted by national laws and regulations.
8. Only information classified RESTREINT UE/EU RESTRICTED that is encrypted using approved cryptographic products may be handled, stored or transmitted (by wired or wireless means) as any other unclassified information under the grant agreement. Such cryptographic products must be approved by the EU or a Member State.
9. External facilities involved in maintenance/repair work must be contractually obliged to comply with the applicable provisions for handling of information classified RESTREINT UE/EU RESTRICTED, as set out in this document.
10. At the request of the granting authority or relevant NSA, DSA, or SAA, the beneficiary must provide evidence of compliance with the security clause of the grant agreement. If an audit and inspection of the beneficiary's processes and facilities are also requested, to ensure compliance with these requirements, beneficiaries shall permit representatives of the granting authority, the NSA, DSA and/or SAA, or the relevant EU security authority to conduct such an audit and inspection.

Physical security

11. Areas in which CIS are used to display, store, process or transmit RESTREINT UE/EU RESTRICTED information or areas housing servers, network management systems, network controllers and communications controllers for such CIS should be established as separate and controlled areas with an appropriate access control system. Access to these separate and controlled areas should be restricted to individuals with specific authorisation. Without prejudice to paragraph 8, equipment as described in paragraph 3 must be stored in such separate and controlled areas.

12. Security mechanisms and/or procedures must be implemented to regulate the introduction or connection of removable computer storage media (such as USBs, mass storage devices or CD-RWs) to components on the CIS.

Access to CIS

13. Access to a beneficiary's CIS handling EUCI is allowed on a basis of strict need-to-know and authorisation of personnel.
14. All CIS must have up-to-date lists of authorised users. All users must be authenticated at the start of each processing session.
15. Passwords, which are part of most identification and authentication security measures, must be at least nine characters long and must include numeric and 'special' characters (if permitted by the system) as well as alphabetic characters. Passwords must be changed at least every 180 days. They must be changed as soon as possible if they have been compromised or disclosed to an unauthorised person, or if such compromise or disclosure is suspected.
16. All CIS must have internal access controls to prevent unauthorised users from accessing or modifying information classified RESTREINT UE/EU RESTRICTED and from modifying system and security controls. Users are to be automatically logged off the CIS if their terminals have been inactive for some predetermined period of time, or the CIS must activate a password-protected screen saver after 15 minutes of inactivity.
17. Each user of the CIS is allocated a unique user account and ID. User accounts must be automatically locked once at least five successive incorrect login attempts have been made.
18. All users of the CIS must be made aware of their responsibilities and the procedures to be followed to protect information classified RESTREINT UE/EU RESTRICTED on the CIS. The responsibilities and procedures to be followed must be documented and acknowledged by users in writing.
19. SecOPs must be available for the users and administrators and must include descriptions of security roles and associated list of tasks, instructions and plans.

Accounting, audit and incident response

20. Any access to the CIS must be logged.
21. The following events must be recorded:
 - (a) all attempts to log on, whether successful or failed;
 - (b) logging off (including being timed out, where applicable);
 - (c) creation, deletion or alteration of access rights and privileges;
 - (d) creation, deletion or alteration of passwords.
22. For all of the events listed above, the following information must be communicated as a minimum:
 - (a) type of event;
 - (b) user ID;
 - (c) date and time;
 - (d) device ID.

23. The accounting records should provide help to a security officer to examine the potential security incidents. They can also be used to support any legal investigations in the event of a security incident. All security records should be regularly checked to identify potential security incidents. The accounting records must be protected from unauthorised deletion or modification.
24. The beneficiary must have an established response strategy to deal with security incidents. Users and administrators must be instructed on how to respond to incidents, how to report them and what to do in the event of emergency.
25. The compromise or suspected compromise of information classified RESTREINT UE/EU RESTRICTED must be reported to the granting authority. The report must contain a description of the information involved and a description of the circumstances of the compromise or suspected compromise. All users of the CIS must be made aware of how to report any actual or suspected security incident to the security officer.

Networking and interconnection

26. When a beneficiary CIS that handles information classified RESTREINT UE/EU RESTRICTED is interconnected to a CIS that is not accredited, this significantly increases the threat to both the security of the CIS and the RESTREINT UE/EU RESTRICTED information that is handled by that CIS. This includes the internet and other public or private CIS, such as other CIS owned by the beneficiary or subcontractor. In this case, the beneficiary must perform a risk assessment to identify the additional security requirements that need to be implemented as part of the security accreditation process. The beneficiary shall provide to the granting authority, and where required by national laws and regulations, the competent SAA, a statement of compliance certifying that the beneficiary CIS and the related interconnections have been accredited for handling EUCI at RESTREINT UE/EU RESTRICTED level.
27. Remote access from other systems to LAN services (e.g. remote access to email and remote SYSTEM support) is prohibited unless special security measures are implemented and agreed by the granting authority, and where required by national laws and regulations, approved by the competent SAA.

Configuration management

28. A detailed hardware and software configuration, as reflected in the accreditation/approval documentation (including system and network diagrams), must be available and regularly maintained.
29. The beneficiary's security officer must conduct configuration checks on hardware and software to ensure that no unauthorised hardware or software has been introduced.
30. Changes to the beneficiary CIS configuration must be assessed for their security implications and must be approved by the security officer, and where required by national laws and regulations, the SAA.
31. The system must be scanned for any security vulnerabilities at least once a quarter. Software to detect malware must be installed and kept up-to-date. If possible, such software should have a national or recognised international approval, otherwise it should be a widely accepted industry standard.
32. The beneficiary must develop a business continuity plan. Back-up procedures must be established to address the following:
 - (a) frequency of back-ups;
 - (b) storage requirements on-site (fireproof containers) or off-site;
 - (c) control of authorised access to back-up copies.

Sanitisation and destruction

33. For CIS or data storage media that have at any time held RESTREINT UE/EU RESTRICTED information the following sanitisation must be performed to the entire system or to storage media before its disposal:
- (a) flash memory (e.g. USB sticks, SD cards, solid state drives, hybrid hard drives) must be overwritten at least three times and then verified to ensure that the original content cannot be recovered, or be deleted using approved deletion software;
 - (b) magnetic media (e.g. hard disks) must be overwritten or degaussed;
 - (c) optical media (e.g. CDs and DVDs) must be shredded or disintegrated;
 - (d) for any other storage media, the granting authority or, if appropriate, the NSA, DSA or SAA should be consulted on the security requirements to be met.
34. Information classified RESTREINT UE/EU RESTRICTED must be sanitised on any data storage media before it is given to any entity that is not authorised to access information classified RESTREINT UE/EU RESTRICTED (e.g. for maintenance work).
-

ANNEX IV

Facility and personnel security clearance for beneficiaries or subcontractors involving RESTREINT UE/EU RESTRICTED information and NSAs/DSAs requiring notification of classified grant agreements at RESTREINT UE/EU RESTRICTED level ⁽¹⁾

Member State	FSC		Notification of grant agreement or subcontract involving R-UE/EU-R information to NSA and/or DSA		PSC	
	YES	NO	YES	NO	YES	NO
Belgium		X		X		X
Bulgaria		X		X		X
Czechia		X		X		X
Denmark	X		X		X	
Germany		X		X		X
Estonia	X		X			X
Ireland		X		X		X
Greece	X			X	X	
Spain		X	X			X
France		X		X		X
Croatia		X	X			X
Italy		X	X			X
Cyprus		X	X			X
Latvia		X		X		X
Lithuania	X		X			X
Luxembourg	X		X		X	
Hungary		X		X		X
Malta		X		X		X
Netherlands	X (only for defence-related grant agreements and subcontracts)		X (only for defence-related grant agreements and subcontracts)			X
Austria		X		X		X
Poland		X		X		X

⁽¹⁾ These national requirements for FSC/PSC and notifications for grant agreements involving RESTREINT UE/EU RESTRICTED information must not place any additional obligations on other Member States or beneficiaries and subcontractors under their jurisdiction.
N.B. Notifications of grant agreements involving CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information are obligatory.

Portugal		X		X		X
Romania		X		X		X
Slovenia	X		X			X
Slovakia	X		X			X
Finland		X		X		X
Sweden		X		X		X

ANNEX V

**LIST OF NATIONAL SECURITY AUTHORITY / DESIGNATED SECURITY AUTHORITY DEPARTMENTS
RESPONSIBLE FOR HANDLING PROCEDURES ASSOCIATED WITH INDUSTRIAL SECURITY****BELGIUM**

National Security Authority
FPS Foreign Affairs
Rue des Petits Carmes 15
1000 Brussels

Tel.: +32 25014542 (Secretariat)

Fax: +32 25014596

Email: nvo-ans@diplobel.fed.be

BULGARIA

1. State Commission on Information Security – National Security Authority

4 Kozloduy Street

1202 Sofia

Tel.: +359 29835775

Fax: +359 29873750

Email: dksi@government.bg

2. Defence Information Service at the Ministry of Defence (security service)

3 Dyakon Ignatiy Street

1092 Sofia

Tel.: +359 29227002

Fax: +359 29885211

Email: office@iksbg.org

3. State Intelligence Agency (security service)

12 Hajdushka Polyana Street

1612 Sofia

Tel.: +359 29813221

Fax: +359 29862706

Email: office@dar.bg

4. State Agency for Technical Operations (security service)

29 Shesti Septemvri Street

1000 Sofia

Tel.: +359 29824971

Fax: +359 29461339

Email: dato@dato.bg

(The competent authorities listed above conduct the vetting procedures for issuing FSCs to legal entities applying to conclude a classified contract, and PSCs to individuals implementing a classified contract for the needs of these authorities.)

5. State Agency National Security (security service)

45 Cherni Vrah Blvd.

1407 Sofia

Tel.: +359 28147109

Fax: +359 29632188, +359 28147441

Email: dans@dans.bg

(The above security service conducts the vetting procedures for issuing FSCs and PSCs to all other legal entities and individuals in the country applying to conclude a classified contract or classified grant agreement or implementing a classified contract or classified grant agreement.)

CZECHIA

National Security Authority
Industrial Security Department
PO BOX 49
150 06 Praha 56

Tel.: +420 257283129

Email: sbr@nbu.cz

DENMARK

1. Politiets Efterretningstjeneste
(Danish Security Intelligence Service)

Klausdalsbrovej 1

2860 Søborg

Tel.: +45 33148888

Fax: +45 33430190

2. Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)

Kastellet 30

2100 Copenhagen Ø

Tel.: +45 33325566

Fax: +45 33931320

GERMANY

1. For matters concerning industrial security policy, FSCs, transportation plans (except for crypto/CCI):
Federal Ministry for Economic Affairs and Energy

Industrial Security Division – RS3

Villemombler Str. 76

53123 Bonn

Tel.: +49 228996154028

Fax: +49 228996152676

Email: dsagermany-rs3@bmwi.bund.de (office email address)

2. For standard visit requests from/to German companies:
Federal Ministry for Economic Affairs and Energy
Industrial Security Division – RS2
Villemombler Str. 76
53123 Bonn
Tel.: +49 228996152401
Fax: +49 228996152603
Email: rs2-international@bmwi.bund.de (office email address)
3. Transportation plans for crypto material:
Federal Office for Information Security (BSI)
National Distribution Agency / NDA-EU DEU
Mainzer Str. 84
53179 Bonn
Tel.: +49 2289995826052
Fax: +49 228991095826052
Email: NDAEU@bsi.bund.de

ESTONIA

National Security Authority Department
Estonian Foreign Intelligence Service
Rahumäe tee 4B
11316 Tallinn
Tel.: +372 6939211
Fax: +372 6935001
Email: nsa@fis.gov.ee

IRELAND

National Security Authority Ireland
Department of Foreign Affairs and Trade
76-78 Harcourt Street
Dublin 2
D02 DX45
Tel.: +353 14082724
Email: nsa@dfa.ie

GREECE

Hellenic National Defence General Staff
E' Division (Security INTEL, CI BRANCH)
E3 Directorate
Industrial Security Office
227-231 Mesogeion Avenue
15561 Hologos, Athens
Tel.: +30 2106572022, +30 2106572178
Fax: +30 2106527612
Email: daa.industrial@hndgs.mil.gr

SPAIN

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Calle Argentona 30
28023 Madrid

Tel.: +34 912832583, +34 912832752, +34 913725928

Fax: +34 913725808

Email: nsa-sp@areatec.com

For information concerning classified programmes: programas.ons@areatec.com

For matters concerning personnel security clearances: hps.ons@areatec.com

For Transportation plans and international visits: sp-ivtco@areatec.com

FRANCE

National Security Authority (NSA) (for policy and for implementation in fields other than the defence industry)
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 boulevard de la Tour-Maubourg
75700 Paris 07 SP

Tel.: +33 171758193

Fax: +33 171758200

Email: ANSFrance@sgdsn.gouv.fr

Designated Security Authority (for implementation in the defence industry)
Direction Générale de l'Armement
Service de la Sécurité de Défense et des systèmes d'Information (DGA/SSDI)
60 boulevard du général Martial Valin
CS 21623
75509 Paris CEDEX 15

Tel.: +33 988670421

Email: for forms and outgoing RFVs: dga-ssdi.ai.fct@intradef.gouv.fr

for incoming RFVs: dga-ssdi.visit.fct@intradef.gouv.fr

CROATIA

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb

Tel.: +385 14681222

Fax: +385 14686049

Email: NSACroatia@uvns.hr

ITALY

Presidenza del Consiglio dei Ministri
D.I.S. – U.C.Se.
Via di Santa Susanna 15
00187 Roma

Tel.: +39 0661174266

Fax: +39 064885273

CYPRUS

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ

Εθνική Αρχή Ασφάλειας (ΕΑΑ)

Λεωφόρος Στροβόλου, 172-174

Στρόβολος, 2048, Λευκωσία

Τηλέφωνα: +357 22807569, +357 22807764

Τηλεομοιότυπο: +357 22302351

Email: cynsa@mod.gov.cy

Ministry of Defence

National Security Authority (NSA)

172-174, Strovolos Avenue

2048 Strovolos, Nicosia

Tel.: +357 22807569, +357 22807764

Fax: +357 22302351

Email: cynsa@mod.gov.cy

LATVIA

National Security Authority

Constitution Protection Bureau of the Republic of Latvia

P.O. Box 286

Riga LV-1001

Tel.: +371 67025418, +371 67025463

Fax: +371 67025454

Email: ndi@sab.gov.lv, ndi@zd.gov.lv

LITHUANIA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija

(The Commission for Secrets Protection Coordination of the Republic of Lithuania)

National Security Authority

Pilaitės pr. 19

LT-06264 Vilnius

Tel.: +370 70666128

Email: nsa@vds.lt

LUXEMBOURG

Autorité Nationale de Sécurité

207, route d'Esch

L-1471 Luxembourg

Tel.: +352 24782210

Email: ans@me.etat.lu

HUNGARY

National Security Authority of Hungary

H-1399 Budapest P.O. Box 710/50

H-1024 Budapest, Szilágyi Erzsébet fasor 11/B

Tel.: +36 13911862

Fax: +36 13911889

Email: nbf@nbf.hu

MALTA

Director of Standardisation
Designated Security Authority for Industrial Security
Standards & Metrology Institute
Malta Competition and Consumer Affairs Authority
Mizzi House
National Road
Blata I-Bajda HMR9010
Tel.: +356 23952000
Fax: +356 21242406
Email: certification@mccaa.org.mt

NETHERLANDS

1. Ministry of the Interior and Kingdom Relations
PO Box 20010
2500 EA The Hague
Tel.: +31 703204400
Fax: +31 703200733
Email: nsa-nl-industry@minbzk.nl
2. Ministry of Defence
Industrial Security Department
PO Box 20701
2500 ES The Hague
Tel.: +31 704419407
Fax: +31 703459189
Email: indussec@mindef.nl

AUSTRIA

1. Federal Chancellery of Austria
Department I/10, Federal Office for Information Security
Ballhausplatz 2
10104 Vienna
Tel.: +43 153115202594
Email: isk@bka.gv.at
2. DSA in the military sphere:
BMLV/Abwehramt
Postfach 2000
1030 Vienna
Email: abwa@bmlvs.gv.at

POLAND

Internal Security Agency
Department for the Protection of Classified Information
Rakowiecka 2A
00-993 Warsaw
Tel.: +48 225857944
Fax: +48 225857443
Email: nsa@abw.gov.pl

PORTUGAL

Gabinete Nacional de Segurança
Serviço de Segurança Industrial
Rua da Junqueira nº 69
1300-342 Lisbon
Tel.: +351 213031710
Fax: +351 213031711
Email: sind@gns.gov.pt, franco@gns.gov.pt

ROMANIA

Oficiul Registrului Național al Informațiilor Secrete de Stat – ORNISS
Romanian NSA – ORNISS – National Registry Office for Classified Information
4th Mures Street
012275 Bucharest
Tel.: +40 212075115
Fax: +40 212245830
Email: relatii publice@orniss.ro, nsa.romania@nsa.ro

SLOVENIA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Tel.: +386 14781390
Fax: +386 14781399
Email: gp.uvtp@gov.si

SLOVAKIA

Národný bezpečnostný úrad
(National Security Authority)
Security Clearance Department
Budatínska 30
851 06 Bratislava
Tel.: +421 268691111
Fax: +421 268691700
Email: podatelna@nbu.gov.sk

FINLAND

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Email: NSA@formin.fi

SWEDEN

1. National Security Authority
Utrikesdepartementet (Ministry for Foreign Affairs)
UD SÄK / NSA
SE-103 39 Stockholm
Tel.: +46 84051000
Fax: +46 87231176
Email: ud-nsa@gov.se

 2. DSA
Försvarets Materielverk (Swedish Defence Materiel Administration)
FMV Säkerhetsskydd
SE-115 88 Stockholm
Tel.: +46 87824000
Fax: +46 87826900
Email: security@fmv.se
-

ISSN 1977-0677 (electronic edition)
ISSN 1725-2555 (paper edition)



Publications Office
of the European Union
L-2985 Luxembourg
LUXEMBOURG

EN