Official Journal of the European Union

L 151

English edition

Legislation

Volume 62

7 June 2019

Contents

[1] Text with EEA relevance.

EN

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

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

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2019/880 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 17 April 2019

on the introduction and the import of cultural goods

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 207(2) thereof,

Having regard to the proposal from the European Commission,

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

Acting in accordance with the ordinary legislative procedure [1],

Whereas:

(1) In light of the Council Conclusions of 12 February 2016 on the fight against the financing of terrorism, the Communication from the Commission to the European Parliament and the Council of 2 February 2016 on an Action Plan for strengthening the fight against terrorist financing and Directive (EU) 2017/541 of the European Parliament and of the Council [2], common rules on trade with third countries should be adopted so as to ensure the effective protection against illicit trade in cultural goods and against their loss or destruction, the preservation of humanity's cultural heritage and the prevention of terrorist financing and money laundering through the sale of pillaged cultural goods to buyers in the Union.

(2) The exploitation of peoples and territories can lead to the illicit trade in cultural goods, in particular when such illicit trade originates from a context of armed conflict. In this respect, this Regulation should take into account regional and local characteristics of peoples and territories, rather than the market value of cultural goods.

(3) Cultural goods are a part of cultural heritage and are often of major cultural, artistic, historical and scientific importance. Cultural heritage constitutes one of the basic elements of civilisation having, inter alia, symbolic value, and forming part of the cultural memory of humankind. It enriches the cultural life of all peoples and unites people through shared memory, knowledge and development of civilisation. It should therefore be protected from unlawful appropriation and pillage. Pillaging of archaeological sites has always happened, but has now reached an industrial scale and, together with trade in illegally excavated cultural goods, is a serious crime that causes significant suffering to those directly or indirectly affected. The illicit trade in cultural goods in many cases contributes to forceful cultural homogenisation or forceful loss of cultural identity, while the pillage of cultural goods leads, inter alia, to the disintegration of cultures. As long as it is possible to engage in lucrative trade in illegally excavated cultural goods and to profit therefrom without any notable risk, such excavations and pillaging will continue. Due to the economic and artistic value of cultural goods they are in high demand on the international market. The absence of strong international legal measures and the ineffective enforcement of any measures that do exist, lead to the transfer of such goods to the shadow economy. The Union should accordingly

[1] Position of the European Parliament of 12 March 2019 (not yet published in the Official Journal) and decision of the Council of 9 April 2019.

[2] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6).

prohibit the introduction into the customs territory of the Union of cultural goods unlawfully exported from third countries, with particular emphasis on cultural goods from third countries affected by armed conflict, in particular where such cultural goods have been illicitly traded by terrorist or other criminal organisations. While that general prohibition should not entail systematic controls, Member States should be allowed to intervene when receiving intelligence regarding suspicious shipments and to take all appropriate measures to intercept illicitly exported cultural goods.

(4) In view of different rules applying in Member States regarding the import of cultural goods into the customs territory of the Union, measures should be taken in particular to ensure that certain imports of cultural goods are subject to uniform controls upon their entry into the customs territory of the Union, on the basis of existing processes, procedures and administrative tools aiming to achieve a uniform implementation of Regulation (EU) No 952/2013 of the European Parliament and of the Council ([3]).

(5) The protection of cultural goods which are considered national treasures of the Member States is already covered by Council Regulation (EC) No 116/2009 ([4]) and Directive 2014/60/EU of the European Parliament and of the Council ([5]). Consequently, this Regulation should not apply to cultural goods which were created or discovered in the customs territory of the Union. The common rules introduced by this Regulation should cover the customs treatment of non-Union cultural goods entering the customs territory of the Union. For the purposes of this Regulation, the relevant customs territory should be the customs territory of the Union at the time of import.

(6) Control measures to be put in place regarding free zones and so-called 'free ports' should have as broad a scope as possible in terms of the customs procedures concerned in order to prevent circumvention of this Regulation through the exploitation of those free zones, which have the potential to be used for the continued proliferation of illicit trade. Those control measures should therefore not only concern cultural goods released for free circulation but also cultural goods placed under a special customs procedure. However, the scope should not go beyond the objective of preventing illicitly exported cultural goods from entering the customs territory of the Union. Accordingly, while encompassing the release for free circulation and some of the special customs procedures under which goods entering the customs territory of the Union may be placed, systematic control measures should exclude transit.

(7) Many third countries and most Member States are familiar with the definitions used in the Unesco Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property signed in Paris on 14 November 1970 ('the 1970 Unesco Convention') to which a significant number of Member States are a party, and in the UNIDROIT Convention on Stolen or Illegally Exported Cultural Objects signed in Rome on 24 June 1995. For that reason the definitions used in this Regulation are based on those definitions.

(8) The legality of export of cultural goods should be primarily examined based on the laws and regulations of the country where those cultural goods were created or discovered. However, in order not to impede legitimate trade unreasonably, a person who seeks to import cultural goods into the customs territory of the Union should, in certain cases, be exceptionally allowed to demonstrate instead the licit export from a different third country where the cultural goods were located before their dispatch to the Union. That exception should apply in cases where the country in which the cultural goods were created or discovered cannot be reliably determined or when the export of the cultural goods in question took place before the 1970 Unesco Convention entered into force, namely 24 April 1972. In order to prevent circumvention of this Regulation by simply sending illicitly exported cultural goods to another third country prior to importing them into the Union, the exceptions should be applicable where the cultural goods have been located in a third country for a period of more than five years for purposes other than temporary use, transit, re-export or transhipment. Where those conditions are fulfilled for more than one country, the relevant country should be the last of those countries before the introduction of the cultural goods into the customs territory of the Union.

(9) Article 5 of the 1970 Unesco Convention calls on the States Parties to establish one or more national services for the protection of cultural goods against illicit import, export and transfer of ownership. Such national services should be equipped with qualified staff sufficient in number to ensure that protection in accordance with that Convention, and should also enable the necessary active collaboration between the competent authorities of Member States which are Parties to that Convention in the area of security and in the fight against the illegal import of cultural goods, especially from areas affected by armed conflict.

([3]) 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).

([4]) Council Regulation (EC) No 116/2009 of 18 December 2008 on the export of cultural goods (OJ L 39, 10.2.2009, p. 1).

([5]) Directive 2014/60/EU of the European Parliament and of the Council of 15 May 2014 on the return of cultural objects unlawfully removed from the territory of a Member State and amending Regulation (EU) No 1024/2012 (OJ L 159, 28.5.2014, p. 1).

(10) In order not to disproportionately impede trade in cultural goods across the Union's external border, this Regulation should only apply to cultural goods above a certain age limit, which is established by this Regulation. It also seems appropriate to set a financial threshold in order to exclude cultural goods of lower value from the application of the conditions and procedures for import into the customs territory of the Union. Those thresholds will ensure that the measures provided for in this Regulation focus on those cultural goods most likely to be targeted by pillagers in conflict areas, without excluding other goods the control of which is necessary for ensuring the protection of cultural heritage.

(11) Illicit trade in pillaged cultural goods has been identified as a possible source of terrorist financing and money laundering activities in the context of the supranational risk assessment on money laundering and terrorist financing risks affecting the internal market.

(12) Since certain categories of cultural goods, namely archaeological objects and elements of monuments, are particularly vulnerable to pillage and destruction, it seems necessary to provide for a system of increased scrutiny before they are permitted to enter the customs territory of the Union. Such a system should require the presentation of an import licence issued by the competent authority of a Member State prior to the release for free circulation of those cultural goods into the Union or their placement under a special customs procedure other than transit. Persons seeking to obtain such a licence should be able to prove licit export from the country where the cultural goods were created or discovered with the appropriate supportive documents and evidence, such as export certificates, ownership titles, invoices, sales contracts, insurance documents, transport documents and experts appraisals. Based on complete and accurate applications, the competent authorities of the Member States should decide whether to issue a licence without undue delay. All import licences should be stored in an electronic system.

(13) An icon is any representation of a religious figure or a religious event. It can be produced in various media and sizes and can be monumental or portable. In cases where an icon was once part, for example, of the interior of a church, a monastery, a chapel, either free-standing or as part of architectural furniture, for example an iconostasis or icon stand, it is a vital and inseparable part of divine worship and liturgical life, and should be considered as forming an integral part of a religious monument which has been dismembered. Even in cases where the specific monument that the icon belonged to is unknown, but where there is evidence that it once formed an integral part of a monument, in particular when there are signs or elements present which indicate that it was once part of an iconostasis or an icon stand, the icon should still be covered by the category 'elements of artistic or historical monuments or archaeological sites which have been dismembered' listed in the Annex.

(14) Taking into account the particular nature of the cultural goods, the role of the customs authorities is extremely relevant and they should be able, where necessary, to require additional information from the declarant and to analyse the cultural goods by means of a physical examination.

(15) For categories of cultural goods the import of which does not require an import licence, the persons seeking to import such goods into the customs territory of the Union should, by means of a statement, certify and assume responsibility for their lawful export from the third country and should provide sufficient information for those cultural goods to be identified by the customs authorities. In order to facilitate the procedure and for reasons of legal certainty, the information about the cultural goods should be provided using a standardised document. The Object ID standard, recommended by Unesco, could be used to describe the cultural goods. The holder of the goods should register those details in an electronic system, in order to facilitate identification by the customs authorities, to allow for risk analysis and targeted controls and to ensure traceability after the cultural goods enter the internal market.

(16) In the context of the EU Single Window environment for customs, the Commission should be responsible for the establishment of a centralised electronic system for the submission of applications for import licences and of importer statements, as well as the storage and the exchange of information between the authorities of the Member States, in particular regarding importer statements and import licences.

(17) It should be possible for the processing of data under this Regulation to also cover personal data and such processing should be carried out in accordance with Union law. Member States and the Commission should process personal data only for the purposes of this Regulation or in duly justified circumstances for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Any collection, disclosure,

transmission, communication and other processing of personal data within the scope of this Regulation should be subject to the requirements of Regulations (EU) 2016/679 ([6]) and (EU) 2018/1725 ([7]) of the European Parliament and of the Council. The processing of personal data for the purposes of this Regulation should also respect the right to respect for private and family life recognised by Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe, as well as the right to respect for private and family life, and the right to the protection of personal data recognised, respectively, by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

(18) Cultural goods which were not created or discovered in the customs territory of the Union but which have been exported as Union goods should not be subject to the presentation of an import licence or of an importer statement when they are returned to that territory as returned goods within the meaning of Regulation (EU) No 952/2013.

(19) The temporary admission of cultural goods for the purpose of education, science, conservation, restoration, exhibition, digitisation, performing arts, research conducted by academic institutions or cooperation between museums or similar institutions should not be subject to the presentation of an import licence or of an importer statement.

(20) The storage of cultural goods from countries affected by armed conflict or a natural disaster for the exclusive purpose of ensuring their safe keeping and preservation by, or under the supervision of, a public authority should not be subject to the presentation of an import licence or an importer statement.

(21) In order to facilitate the presentation of cultural goods at commercial art fairs, an import licence should not be necessary where the cultural goods are under temporary admission, within the meaning of Article 250 of Regulation (EU) No 952/2013, and where an importer statement has been provided instead of the import licence. However, the presentation of an import licence should be required where such cultural goods are to remain in the Union after the art fair.

(22) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to adopt detailed arrangements for: cultural goods that are returned goods or, the temporary admission of cultural goods into the customs territory of the Union and their safe keeping, the templates for import licence applications and for import licence forms, the templates for importer statements and their accompanying documents, and further procedural rules on their submission and processing. Implementing powers should also be conferred on the Commission to make arrangements for the establishment of an electronic system for the submission of applications for import licences and importer statements and for the storage of information and the exchange of information between Member States. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council ([8]).

(23) In order to ensure effective coordination and to avoid duplication of efforts when organising training, capacity building activities and awareness-raising campaigns, as well as to commission relevant research and the development of standards, where appropriate, the Commission and the Member States should cooperate with international organisations and bodies, such as Unesco, INTERPOL, EUROPOL, the World Customs Organization, the International Centre for the Preservation and Restoration of Cultural Property and the International Council of Museums (ICOM).

(24) Relevant information on trade flows of cultural goods should be electronically collected and shared by Member States and the Commission in order to support the efficient implementation of this Regulation and to provide the basis for its future evaluation. In the interest of transparency and public scrutiny, as much information as possible should be made public. Trade flows of cultural goods cannot be efficiently monitored by their value or weight only. It is essential to electronically collect information on the number of items declared. As no supplementary measurement unit is specified in the Combined Nomenclature for cultural goods, it is necessary to require that the number of items is declared.

([6]) 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).

([7]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

([8]) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(25) The EU Strategy and Action Plan for customs Risk Management aims, inter alia, to strengthen capacities of customs authorities to increase the responsiveness to risks in the area of cultural goods. The common risk management framework laid down in Regulation (EU) No 952/2013 should be used and relevant risk information should be exchanged between customs authorities.

(26) In order to benefit from the expertise of international organisations and bodies which are active in cultural matters and from their experience with illicit trade in cultural goods, recommendations and guidance issued from those organisations and bodies should be taken into consideration in the common risk management framework when identifying risks related to cultural goods. In particular, the Red Lists published by ICOM should serve as guidance to identify those third countries whose heritage is most at risk and the objects exported from there that would more often be the object of illicit trade.

(27) It is necessary to establish awareness-raising campaigns targeted at buyers of cultural goods regarding the risk of illicit trade and to assist market actors in their understanding and application of this Regulation. Member States should involve relevant national contact points and other information provision services in the dissemination of that information.

(28) The Commission should ensure that micro, small and medium-sized enterprises (SMEs) benefit from adequate technical assistance and should facilitate the provision of information to them in order to efficiently implement this Regulation. SMEs established in the Union which import cultural goods should therefore benefit from current and future Union programmes in support of the competitiveness of small and medium-sized enterprises.

(29) In order to encourage compliance and deter circumvention, Member States should introduce effective, proportionate and dissuasive penalties for failing to comply with the provisions of this Regulation and communicate those penalties to the Commission. Penalties introduced by Member States for infringements of this Regulation should have an equivalent deterrent effect across the Union.

(30) Member States should ensure that the customs authorities and the competent authorities agree on measures under Article 198 of Regulation (EU) No 952/2013. The details of those measures should be subject to national law.

(31) The Commission should, without delay, adopt rules implementing this Regulation, in particular those regarding the appropriate electronic standardised forms to be used to apply for an import licence or to prepare an importer statement, and establish the electronic system afterwards within the shortest possible timeframe. The application of the provisions regarding import licences and importer statements should be deferred accordingly.

(32) In accordance with the principle of proportionality, it is necessary and appropriate for the achievement of the basic objectives of this Regulation to lay down rules on the introduction, and the conditions and procedures for the import, of cultural goods into the customs territory of the Union. This Regulation does not go beyond what is necessary in order to achieve the objectives pursued, in accordance with Article 5(4) of the Treaty on European Union,

HAVE ADOPTED THIS REGULATION:

Article 1

Subject matter and scope

1. This Regulation sets out the conditions for the introduction of cultural goods and the conditions and procedures for the import of cultural goods for the purpose of safeguarding humanity's cultural heritage and preventing the illicit trade in cultural goods, in particular where such illicit trade could contribute to terrorist financing.

2. This Regulation does not apply to cultural goods which were either created or discovered in the customs territory of the Union.

Article 2

Definitions

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

(1) 'cultural goods' means any item which is of importance for archaeology, prehistory, history, literature, art or science as listed in the Annex;

(2) 'introduction of cultural goods' means any entry into the customs territory of the Union of cultural goods which are subject to customs supervision or customs control within the customs territory of the Union in accordance with Regulation (EU) No 952/2013;

(3) 'import of cultural goods' means:

(a) the release of cultural goods for free circulation as referred to in Article 201 of Regulation (EU) No 952/2013; or

(b) the placing of cultural goods under one of the following categories of special procedures referred to in Article 210 of Regulation (EU) No 952/2013:

(i) storage, comprising customs warehousing and free zones;

(ii) specific use, comprising temporary admission and end-use;

(iii) inward processing;

(4) 'holder of the goods' means holder of the goods as defined in point (34) of Article 5 of Regulation (EU) No 952/2013;

(5) 'competent authorities' means the public authorities designated by the Member States to issue import licences.

Article 3

Introduction and import of cultural goods

1. The introduction of cultural goods referred to in Part A of the Annex which were removed from the territory of the country where they were created or discovered in breach of the laws and regulations of that country shall be prohibited.

The customs authorities and the competent authorities shall take any appropriate measure when there is an attempt to introduce cultural goods as referred to in the first subparagraph.

2. The import of cultural goods listed in Parts B and C of the Annex shall be permitted only upon the provision of either:

(a) an import licence issued in accordance with Article 4; or

(b) an importer statement submitted in accordance with Article 5.

3. The import licence or the importer statement referred to in paragraph 2 of this Article shall be provided to the customs authorities in accordance with Article 163 of Regulation (EU) No 952/2013. In the event that the cultural goods are placed under the free zone procedure, the holder of the goods shall provide the import licence or the importer statement upon presentation of the goods in accordance with points (a) and (b) of Article 245(1) of Regulation (EU) No 952/2013.

4. Paragraph 2 of this Article shall not apply to:

(a) cultural goods that are returned goods within the meaning of Article 203 of Regulation (EU) No 952/2013;

(b) the import of cultural goods for the exclusive purpose of ensuring their safekeeping by, or under the supervision of, a public authority, with the intent to return those cultural goods, when the situation so allows;

(c) the temporary admission of cultural goods, within the meaning of Article 250 of Regulation (EU) No 952/2013, into the customs territory of the Union for the purpose of education, science, conservation, restoration, exhibition, digitisation, performing arts, research conducted by academic institutions or cooperation between museums or similar institutions.

5. An import licence shall not be required for cultural goods that have been placed under the temporary admission procedure within the meaning of Article 250 of Regulation (EU) No 952/2013, where such goods are to be presented at commercial art fairs. In such cases an importer statement shall be provided in accordance with the procedure in Article 5 of this Regulation.

However, if those cultural goods are subsequently placed under another customs procedure referred to in point (3) of Article 2 of this Regulation, an import licence issued in accordance with Article 4 of this Regulation shall be required.

6. The Commission shall lay down, by means of implementing acts, detailed arrangements for cultural goods that are returned goods, for the import of cultural goods for their safe keeping and for the temporary admission of cultural goods as referred to in paragraphs 4 and 5 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 13(2).

7. Paragraph 2 of this Article shall be without prejudice to other measures adopted by the Union in accordance with Article 215 of the Treaty on the Functioning of the European Union.

8. When submitting a customs declaration for the import of cultural goods listed in Parts B and C of the Annex, the number of items shall be indicated using the supplementary unit, as set out in that Annex. Where the cultural goods are placed under the free zone procedure, the holder of the goods shall indicate the number of items upon presentation of the goods in accordance with points (a) and (b) of Article 245(1) of Regulation (EU) No 952/2013.

Article 4

Import licence

1. The import of cultural goods listed in Part B of the Annex other than those referred to in Article 3(4) and (5) shall require an import licence. That import licence shall be issued by the competent authority of the Member State in which the cultural goods are placed under one of the customs procedures referred to in point (3) of Article 2 for the first time.

2. Import licences issued by the competent authorities of a Member State in accordance with this Article shall be valid throughout the Union.

3. An import licence issued in accordance with this Article shall not be construed to be evidence of licit provenance or ownership of the cultural goods in question.

4. The holder of the goods shall apply for an import licence to the competent authority of the Member State referred to in paragraph 1 of this Article via the electronic system referred to in Article 8. The application shall be accompanied by any supporting documents and information providing evidence that the cultural goods in question have been exported from the country where they were created or discovered in accordance with the laws and regulations of that country or providing evidence of the absence of such laws and regulations at the time they were taken out of its territory.

By way of derogation from the first subparagraph, the application may be accompanied instead by any supporting documents and information providing evidence that the cultural goods in question have been exported in accordance with the laws and regulations of the last country where they were located for a period of more than five years and for purposes other than temporary use, transit, re-export or transhipment, in the following cases:

(a) the country where the cultural goods were created or discovered cannot be reliably determined; or

(b) the cultural goods were taken out of the country where they were created or discovered before 24 April 1972.

5. Evidence that the cultural goods in question have been exported in accordance with paragraph 4 shall be provided in the form of export certificates or export licences where the country in question has established such documents for the export of cultural goods at the time of the export.

6. The competent authority shall check whether the application is complete. It shall request any missing or additional information or document from the applicant within 21 days of receipt of the application.

7. Within 90 days of receipt of the complete application, the competent authority shall examine it and decide whether to issue the import licence or to reject the application.

The competent authority shall reject the application where:

(a) it has information or reasonable grounds to believe that the cultural goods were removed from the territory of the country where they were created or discovered in breach of the laws and regulations of that country;

(b) the evidence required by paragraph 4 has not been provided;

(c) it has information or reasonable grounds to believe that the holder of the goods did not acquire them lawfully; or

(d) it has been informed that there are pending claims for the return of the cultural goods by the authorities of the country where they were created or discovered.

8. In the event that the application is rejected, the administrative decision referred to in paragraph 7, together with a statement of reasons and information on the appeal procedure, shall be communicated to the applicant without delay.

9. Where an application is made for an import licence relating to cultural goods for which such an application has been previously rejected, the applicant shall inform the competent authority to which the application is submitted of the previous rejection.

10. Where a Member State rejects an application, that rejection, as well as the grounds on which it was based, shall be communicated to the other Member States and to the Commission via the electronic system referred to in Article 8.

11. Member States shall designate without delay the competent authorities for the issuing of import licences in accordance with this Article. The Member States shall communicate the details of the competent authorities as well as any changes in that respect to the Commission.

The Commission shall publish the details of the competent authorities and any changes thereto in the 'C' series of the *Official Journal of the European Union*.

12. The Commission shall lay down, by means of implementing acts, the template for and the format of the application for the import licence and shall indicate possible supporting documents to prove licit provenance of the cultural goods in question as well as the procedural rules on the submission and processing of such an application. In establishing those elements, the Commission shall endeavour to achieve uniform application by competent authorities of the import licencing procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 13(2).

Article 5

Importer statement

1. The import of the cultural goods listed in Part C of the Annex shall require an importer statement which the holder of the goods shall submit via the electronic system referred to in Article 8.

2. The importer statement shall consist of:

(a) a declaration signed by the holder of the goods stating that the cultural goods have been exported from the country where they were created or discovered in accordance with the laws and regulations of that country at the time they were taken out of its territory; and

(b) a standardised document describing the cultural goods in question in sufficient detail for them to be identified by the authorities and to perform risk analysis and targeted controls.

By way of derogation from point (a) of the first subparagraph, the declaration may instead state that the cultural goods in question have been exported in accordance with the laws and regulations of the last country where they were located for a period of more than five years and for purposes other than temporary use, transit, re-export or transhipment, in the following cases:

(a) the country where the cultural goods were created or discovered cannot be reliably determined; or

(b) the cultural goods were taken out of the country where they were created or discovered before 24 April 1972.

3. The Commission shall lay down, by means of implementing acts, the standardised template for and the format of the importer statement as well as the procedural rules on its submission and shall indicate possible supporting documents to prove licit provenance of the cultural goods in question that should be in the possession of the holder of the goods and the rules on processing of the importer statement. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 13(2).

Article 6

Competent customs offices

Member States may restrict the number of customs offices competent to handle the import of cultural goods subject to this Regulation. Where Member States apply such a restriction, they shall communicate the details of those customs offices as well as any changes in that respect to the Commission.

The Commission shall publish the details of the competent customs offices and any changes thereto in the 'C' series of the *Official Journal of the European Union*.

Article 7

Administrative cooperation

For the purposes of implementing this Regulation, Member States shall ensure cooperation between their customs authorities and with the competent authorities referred to in Article 4.

Article 8

Use of an electronic system

1. The storage and the exchange of information between the authorities of the Member States, in particular regarding import licences and importer statements, shall be carried out by means of a centralised electronic system.

In the event of a temporary failure of the electronic system, other means for the storage and exchange of information may be used on a temporary basis.

2. The Commission shall lay down, by means of implementing acts:

(a) the arrangements for the deployment, operation and maintenance of the electronic system referred to in paragraph 1;

(b) the detailed rules regarding the submission, processing, storage and exchange of information between the authorities of the Member States by means of the electronic system or by other means referred to in paragraph 1.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 13(2) by 28 June 2021.

Article 9

Establishment of an electronic system

The Commission shall establish the electronic system referred to in Article 8. The electronic system shall be operational at the latest four years after the entry into force of the first of the implementing acts referred to in Article 8(2).

Article 10

Personal data protection and data retention periods

1. The customs authorities and competent authorities of the Member States shall act as controllers of the personal data obtained pursuant to Articles 4, 5 and 8.

2. The processing of personal data on the basis of this Regulation shall take place only for the purpose defined in Article 1(1).

3. The personal data obtained in accordance with Articles 4, 5 and 8 shall be accessed only by duly authorised staff of the authorities and shall be adequately protected against unauthorised access or communication. The data shall not be disclosed or communicated without the express written authorisation of the authority which originally obtained the information. However, such authorisation shall not be necessary where the authorities are required to disclose or communicate that information pursuant to legal provisions in force in the Member State in question, particularly in connection with legal proceedings.

4. The authorities shall store personal data obtained pursuant to Articles 4, 5 and 8 for a period of 20 years from the date on which the data were obtained. Those personal data shall be erased upon the expiry of that period.

Article 11

Penalties

Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.

By 28 December 2020, Member States shall notify the Commission of the rules on penalties applicable to the introduction of cultural goods in breach of Article 3(1), and of the related measures.

By 28 June 2025, Member States shall notify the Commission of the rules on penalties applicable to other infringements of this Regulation, in particular the making of false statements and the submission of false information, and of the related measures.

The Member States shall notify the Commission without delay of any subsequent amendment affecting those rules.

Article 12

Cooperation with third countries

The Commission may, in matters covered by its activities and to the extent required for the fulfilment of its tasks under this Regulation, organise training and capacity building activities for third countries in cooperation with Member States.

Article 13

Committee procedure

1. The Commission shall be assisted by the committee established by Article 8 of Council Regulation (EC) No 116/2009. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 14

Reporting and evaluation

1. Member States shall provide information to the Commission on the implementation of this Regulation.

For that purpose, the Commission shall address relevant questionnaires to the Member States. Member States shall have six months from receipt of the questionnaire to communicate the requested information to the Commission.

2. Within three years of the date on which this Regulation becomes applicable in its entirety, and every five years thereafter, the Commission shall present a report to the European Parliament and to the Council on the implementation of this Regulation. That report shall be publicly available and shall include relevant statistical information at both Union and national level, such as the number of import licences issued, of applications rejected and of importer statements submitted. It shall include a consideration of practical implementation, including the impact on Union economic operators, particularly SMEs.

3. By 28 June 2020 and every 12 months thereafter until the electronic system as set out in Article 9 has been established, the Commission shall present a report to the European Parliament and to the Council on the progress made in adopting the implementing acts as set out in Article 8(2) and in establishing the electronic system as set out in Article 9.

Article 15

Entry into force

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

Article 16

Application

1. This Regulation shall apply from the date of its entry into force.

2. Notwithstanding paragraph 1:

(a) Article 3(1) shall apply from 28 December 2020;

(b) Article 3(2) to (5), (7) and (8), Article 4(1) to (10), Article 5(1) and (2) and Article 8(1) shall apply from the date on which the electronic system referred to in Article 8 becomes operational or at the latest from 28 June 2025. The Commission shall publish the date on which the conditions of this paragraph have been fulfilled in the 'C' series of the *Official Journal of the European Union*.

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

Done at Strasbourg, 17 April 2019.

For the European Parliament	*For the Council*
The President	*The President*
A. TAJANI	G. CIAMBA

ANNEX

Part A. Cultural goods covered by Article 3(1)

(a) rare collections and specimens of fauna, flora, minerals and anatomy, and objects of palaeontological interest;
(b) property relating to history, including the history of science and technology and military and social history, to the life of national leaders, thinkers, scientists and artists and to events of national importance;
(c) products of archaeological excavations (including regular and clandestine) or of archaeological discoveries on land or underwater;
(d) elements of artistic or historical monuments or archaeological sites which have been dismembered [1];
(e) antiquities more than one hundred years old, such as inscriptions, coins and engraved seals;
(f) objects of ethnological interest;
(g) objects of artistic interest, such as: (i) pictures, paintings and drawings produced entirely by hand on any support and in any material (excluding industrial designs and manufactured articles decorated by hand); (ii) original works of statuary art and sculpture in any material; (iii) original engravings, prints and lithographs; (iv) original artistic assemblages and montages in any material;
(h) rare manuscripts and incunabula;
(i) old books, documents and publications of special interest (historical, artistic, scientific, literary, etc.) singly or in collections;
(j) postage, revenue and similar stamps, singly or in collections;
(k) archives, including sound, photographic and cinematographic archives;
(l) articles of furniture more than one hundred years old and old musical instruments.

[1] Liturgical icons and statues, even free-standing, are to be considered as cultural goods belonging to this category.

Part B. Cultural goods covered by Article 4

Categories of cultural goods according to Part A	Combined Nomenclature (CN) Chapter, Heading or Subheading	Minimum age threshold	Minimum financial threshold (customs value)	Supplementary units
(c) products of archaeological excavations (including regular and clandestine) or of archaeological discoveries on land or underwater;	ex 9705; ex 9706	More than 250 years old	Whatever the value	number of items (p/st)
(d) elements of artistic or historical monuments or archaeological sites which have been dismembered [1];	ex 9705; ex 9706	More than 250 years old	Whatever the value	number of items (p/st)

[1] Liturgical icons and statues, even free-standing, are to be considered as cultural goods belonging to this category.

Part C. Cultural goods covered by Article 5

Categories of cultural goods according to Part A	Combined Nomenclature (CN) Chapter, Heading or Subheading	Minimum age threshold	Minimum financial threshold (customs value)	Supplementary units
(a) rare collections and specimens of fauna, flora, minerals and anatomy, and objects of palaeontological interest;	ex 9705	More than 200 years old	EUR 18 000 or more per item	number of items (p/st)
(b) property relating to history, including the history of science and technology and military and social history, to the life of national leaders, thinkers, scientists and artists and to events of national importance;	ex 9705	More than 200 years old	EUR 18 000 or more per item	number of items (p/st)
(e) antiquities, such as inscriptions, coins and engraved seals;	ex 9706	More than 200 years old	EUR 18 000 or more per item	number of items (p/st)
(f) objects of ethnological interest;	ex 9705	More than 200 years old	EUR 18 000 or more per item	number of items (p/st)
(g) objects of artistic interest, such as:				
(i) pictures, paintings and drawings produced entirely by hand on any support and in any material (excluding industrial designs and manufactured articles decorated by hand);	ex 9701	More than 200 years old	EUR 18 000 or more per item	number of items (p/st)

Categories of cultural goods according to Part A	Combined Nomenclature (CN) Chapter, Heading or Subheading	Minimum age threshold	Minimum financial threshold (customs value)	Supplementary units
(ii) original works of statuary art and sculpture in any material;	ex 9703	More than 200 years old	EUR 18 000 or more per item	number of items (p/st)
(iii) original engravings, prints and lithographs;	ex 9702;	More than 200 years old	EUR 18 000 or more per item	number of items (p/st)
(iv) original artistic assemblages and montages in any material;	ex 9701	More than 200 years old	EUR 18 000 or more per item	number of items (p/st)
(h) rare manuscripts and incunabula;	ex 9702; ex 9706	More than 200 years old	EUR 18 000 or more per item	number of items (p/st)
(i) old books, documents and publications of special interest (historical, artistic, scientific, literary, etc.) singly or in collections.	ex 9705; ex 9706	More than 200 years old	EUR 18 000 or more per item	number of items (p/st)

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 17 April 2019

on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

(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 114 thereof,

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Economic and Social Committee [1],

Having regard to the opinion of the Committee of the Regions [2],

Acting in accordance with the ordinary legislative procedure [3],

Whereas:

(1) Network and information systems and electronic communications networks and services play a vital role in society and have become the backbone of economic growth. Information and communications technology (ICT) underpins the complex systems which support everyday societal activities, keep our economies running in key sectors such as health, energy, finance and transport, and, in particular, support the functioning of the internal market.

(2) The use of network and information systems by citizens, organisations and businesses across the Union is now pervasive. Digitisation and connectivity are becoming core features in an ever growing number of products and services and with the advent of the internet of Things (IoT) an extremely high number of connected digital devices are expected to be deployed across the Union during the next decade. While an increasing number of devices is connected to the internet, security and resilience are not sufficiently built in by design, leading to insufficient cybersecurity. In that context, the limited use of certification leads to individual, organisational and business users having insufficient information about the cybersecurity features of ICT products, ICT services and ICT processes, which undermines trust in digital solutions. Network and information systems are capable of supporting all aspects of our lives and drive the Union's economic growth. They are the cornerstone for achieving the digital single market.

(3) Increased digitisation and connectivity increase cybersecurity risks, thus making society as a whole more vulnerable to cyber threats and exacerbating the dangers faced by individuals, including vulnerable persons such as children. In order to mitigate those risks, all necessary actions need to be taken to improve cybersecurity in the Union so that network and information systems, communications networks, digital products, services and devices used by citizens, organisations and businesses – ranging from small and medium-sized enterprises (SMEs), as defined in Commission Recommendation 2003/361/EC [4], to operators of critical infrastructure – are better protected from cyber threats.

[1] OJ C 227, 28.6.2018, p. 86.
[2] OJ C 176, 23.5.2018, p. 29.
[3] Position of the European Parliament of 12 March 2019 (not yet published in the Official Journal) and decision of the Council of 9 April 2019.
[4] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

(4) By making the relevant information available to the public, the European Union Agency for Network and Information Security (ENISA), as established by Regulation (EU) No 526/2013 of the European Parliament and of the Council ([5]) contributes to the development of the cybersecurity industry in the Union, in particular SMEs and start-ups. ENISA should strive for closer cooperation with universities and research entities in order to contribute to reducing dependence on cybersecurity products and services from outside the Union and to reinforce supply chains inside the Union.

(5) Cyberattacks are on the increase and a connected economy and society that is more vulnerable to cyber threats and attacks requires stronger defences. However, while cyberattacks often take place across borders, the competence of, and policy responses by, cybersecurity and law enforcement authorities are predominantly national. Large-scale incidents could disrupt the provision of essential services across the Union. This necessitates effective and coordinated responses and crisis management at Union level, building on dedicated policies and wider instruments for European solidarity and mutual assistance. Moreover, a regular assessment of the state of cybersecurity and resilience in the Union, based on reliable Union data, as well as systematic forecasts of future developments, challenges and threats, at Union and global level, are important for policy makers, industry and users.

(6) In light of the increased cybersecurity challenges faced by the Union, there is a need for a comprehensive set of measures that would build on previous Union action and would foster mutually reinforcing objectives. Those objectives include further increasing the capabilities and preparedness of Member States and businesses, as well as improving cooperation, information sharing and coordination across Member States and Union institutions, bodies, offices and agencies. Furthermore, given the borderless nature of cyber threats, there is a need to increase capabilities at Union level that could complement the action of Member States, in particular in cases of large-scale cross-border incidents and crises, while taking into account the importance of maintaining and further enhancing the national capabilities to respond to cyber threats of all scales.

(7) Additional efforts are also needed to increase citizens', organisations' and businesses' awareness of cybersecurity issues. Moreover, given that incidents undermine trust in digital service providers and in the digital single market itself, especially among consumers, trust should be further strengthened by offering information in a transparent manner on the level of security of ICT products, ICT services and ICT processes that stresses that even a high level of cybersecurity certification cannot guarantee that an ICT product, ICT service or ICT process is completely secure. An increase in trust can be facilitated by Union-wide certification providing for common cybersecurity requirements and evaluation criteria across national markets and sectors.

(8) Cybersecurity is not only an issue related to technology, but one where human behaviour is equally important. Therefore, 'cyber-hygiene', namely, simple, routine measures that, where implemented and carried out regularly by citizens, organisations and businesses, minimise their exposure to risks from cyber threats, should be strongly promoted.

(9) For the purpose of strengthening Union cybersecurity structures, it is important to maintain and develop the capabilities of Member States to comprehensively respond to cyber threats, including to cross-border incidents.

(10) Businesses and individual consumers should have accurate information regarding the assurance level with which the security of their ICT products, ICT services and ICT processes has been certified. At the same time, no ICT product or ICT service is wholly cyber-secure and basic rules of cyber-hygiene have to be promoted and prioritised. Given the growing availability of IoT devices, there is a range of voluntary measures that the private sector can take to reinforce trust in the security of ICT products, ICT services and ICT processes.

(11) Modern ICT products and systems often integrate and rely on one or more third-party technologies and components such as software modules, libraries or application programming interfaces. This reliance, which is referred to as a 'dependency', could pose additional cybersecurity risks as vulnerabilities found in third-party components could also affect the security of the ICT products, ICT services and ICT processes. In many cases, identifying and documenting such dependencies enables end users of ICT products, ICT services and ICT processes to improve their cybersecurity risk management activities by improving, for example, users' cybersecurity vulnerability management and remediation procedures.

([5]) Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (OJ L 165, 18.6.2013, p. 41).

(12) Organisations, manufacturers or providers involved in the design and development of ICT products, ICT services or ICT processes should be encouraged to implement measures at the earliest stages of design and development to protect the security of those products, services and processes to the highest possible degree, in such a way that the occurrence of cyberattacks is presumed and their impact is anticipated and minimised ('security-by-design'). Security should be ensured throughout the lifetime of the ICT product, ICT service or ICT process by design and development processes that constantly evolve to reduce the risk of harm from malicious exploitation.

(13) Undertakings, organisations and the public sector should configure the ICT products, ICT services or ICT processes designed by them in a way that ensures a higher level of security which should enable the first user to receive a default configuration with the most secure settings possible ('security by default'), thereby reducing the burden on users of having to configure an ICT product, ICT service or ICT process appropriately. Security by default should not require extensive configuration or specific technical understanding or non-intuitive behaviour on the part of the user, and should work easily and reliably when implemented. If, on a case-by-case basis, a risk and usability analysis leads to the conclusion that such a setting by default is not feasible, users should be prompted to opt for the most secure setting.

(14) Regulation (EC) No 460/2004 of the European Parliament and of the Council ([6]) established ENISA with the purposes of contributing to the goals of ensuring a high and effective level of network and information security within the Union, and developing a culture of network and information security for the benefit of citizens, consumers, enterprises and public administrations. Regulation (EC) No 1007/2008 of the European Parliament and of the Council ([7]) extended ENISA's mandate until March 2012. Regulation (EU) No 580/2011 of the European Parliament and of the Council ([8]) further extended ENISA's mandate until 13 September 2013. Regulation (EU) No 526/2013 extended ENISA's mandate until 19 June 2020.

(15) The Union has already taken important steps to ensure cybersecurity and to increase trust in digital technologies. In 2013, the Cybersecurity Strategy of the European Union was adopted to guide the Union's policy response to cyber threats and risks. In an effort to better protect citizens online, the Union's first legal act in the field of cybersecurity was adopted in 2016 in the form of Directive (EU) 2016/1148 of the European Parliament and of the Council ([9]). Directive (EU) 2016/1148 put in place requirements concerning national capabilities in the field of cybersecurity, established the first mechanisms to enhance strategic and operational cooperation between Member States, and introduced obligations concerning security measures and incident notifications across sectors which are vital for the economy and society, such as energy, transport, drinking water supply and distribution, banking, financial market infrastructures, healthcare, digital infrastructure as well as key digital service providers (search engines, cloud computing services and online marketplaces).

A key role was attributed to ENISA in supporting the implementation of that Directive. In addition, fighting effectively against cybercrime is an important priority in the European Agenda on Security, contributing to the overall aim of achieving a high level of cybersecurity. Other legal acts such as Regulation (EU) 2016/679 of the European Parliament and of the Council ([10]) and Directives 2002/58/EC ([11]) and (EU) 2018/1972 ([12]) of the European Parliament and of the Council also contribute to a high level of cybersecurity in the digital single market.

([6]) Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (OJ L 77, 13.3.2004, p. 1).

([7]) Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration (OJ L 293, 31.10.2008, p. 1).

([8]) Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration (OJ L 165, 24.6.2011, p. 3).

([9]) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

([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).

([11]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

([12]) Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).

(16) Since the adoption of the Cybersecurity Strategy of the European Union in 2013 and the last revision of ENISA's mandate, the overall policy context has changed significantly as the global environment has become more uncertain and less secure. Against that background and in the context of the positive development of the role of ENISA as a reference point for advice and expertise, as a facilitator of cooperation and of capacity-building as well as within the framework of the new Union cybersecurity policy, it is necessary to review ENISA's mandate, to establish its role in the changed cybersecurity ecosystem and to ensure that it contributes effectively to the Union's response to cybersecurity challenges emanating from the radically transformed cyber threat landscape, for which, as recognised during the evaluation of ENISA, the current mandate is not sufficient.

(17) ENISA as established by this Regulation should succeed ENISA as established by Regulation (EU) No 526/2013. ENISA should carry out the tasks conferred on it by this Regulation and other legal acts of the Union in the field of cybersecurity, among other things, by providing advice and expertise and by acting as a Union centre of information and knowledge. It should promote the exchange of best practices between Member States and private stakeholders, offer policy suggestions to the Commission and the Member States, act as a reference point for Union sectoral policy initiatives with regard to cybersecurity matters, and foster operational cooperation, both between Member States and between the Member States and Union institutions, bodies, office and agencies.

(18) Within the framework of Decision 2004/97/EC, Euratom taken by common agreement between the Representatives of the Member States, meeting at Head of State or Government level ([13]), the representatives of the Member States decided that ENISA would have its seat in a town in Greece to be determined by the Greek Government. ENISA's host Member State should ensure the best possible conditions for the smooth and efficient operation of ENISA. It is imperative for the proper and efficient performance of its tasks, for staff recruitment and retention and for enhancing the efficiency of networking activities that ENISA be based in an appropriate location, among other things providing appropriate transport connections and facilities for spouses and children accompanying members of staff of ENISA. The necessary arrangements should be laid down in an agreement between ENISA and the host Member State concluded after obtaining the approval of the Management Board of ENISA.

(19) Given the increasing cybersecurity risks and challenges the Union is facing, the financial and human resources allocated to ENISA should be increased to reflect its enhanced role and tasks, and its critical position in the ecosystem of organisations defending the digital ecosystem of the Union, allowing ENISA to effectively carry out the tasks conferred on it by this Regulation.

(20) ENISA should develop and maintain a high level of expertise and operate as a reference point, establishing trust and confidence in the single market by virtue of its independence, the quality of the advice it delivers, the quality of information it disseminates, the transparency of its procedures, the transparency of its methods of operation, and its diligence in carrying out its tasks. ENISA should actively support national efforts and should proactively contribute to Union efforts while carrying out its tasks in full cooperation with the Union institutions, bodies, offices and agencies and with the Member States, avoiding any duplication of work and promoting synergy. In addition, ENISA should build on input from and cooperation with the private sector as well as other relevant stakeholders. A set of tasks should establish how ENISA is to accomplish its objectives while allowing flexibility in its operations.

(21) In order to be able to provide adequate support to the operational cooperation between Member States, ENISA should further strengthen its technical and human capabilities and skills. ENISA should increase its know-how and capabilities. ENISA and Member States, on a voluntary basis, could develop programmes for seconding national experts to ENISA, creating pools of experts and staff exchanges.

(22) ENISA should assist the Commission by means of advice, opinions and analyses regarding all Union matters related to policy and law development, updates and reviews in the field of cybersecurity and sector-specific aspects thereof in order to enhance the relevance of Union policies and laws with a cybersecurity dimension and to enable consistency in the implementation of those policies and laws at national level. ENISA should act as a reference point for advice and expertise for Union sector-specific policy and law initiatives where matters related to cybersecurity are involved. ENISA should regularly inform the European Parliament about its activities.

([13]) Decision 2004/97/EC, Euratom taken by common agreement between the Representatives of the Member States, meeting at Head of State or Government level, of 13 December 2003 on the location of the seats of certain offices and agencies of the European Union (OJ L 29, 3.2.2004, p. 15).

(23) The public core of the open internet, namely its main protocols and infrastructure, which are a global public good, provides the essential functionality of the internet as a whole and underpins its normal operation. ENISA should support the security of the public core of the open internet and the stability of its functioning, including, but not limited to, key protocols (in particular DNS, BGP, and IPv6), the operation of the domain name system (such as the operation of all top-level domains), and the operation of the root zone.

(24) The underlying task of ENISA is to promote the consistent implementation of the relevant legal framework, in particular the effective implementation of Directive (EU) 2016/1148 and other relevant legal instruments containing cybersecurity aspects, which is essential to increasing cyber resilience. In light of the fast evolving cyber threat landscape, it is clear that Member States have to be supported by more comprehensive, cross-policy approach to building cyber resilience.

(25) ENISA should assist the Member States and Union institutions, bodies, offices and agencies in their efforts to build and enhance capabilities and preparedness to prevent, detect and respond to cyber threats and incidents and in relation to the security of network and information systems. In particular, ENISA should support the development and enhancement of national and Union computer security incident response teams ('CSIRTs') provided for in Directive (EU) 2016/1148, with a view to achieving a high common level of their maturity in the Union. Activities carried out by ENISA relating to the operational capacities of Member States should actively support actions taken by Member States to comply with their obligations under Directive (EU) 2016/1148 and therefore should not supersede them.

(26) ENISA should also assist with the development and updating of strategies on the security of network and information systems at Union level and, upon request, at Member State level, in particular on cybersecurity, and should promote the dissemination of such strategies and follow the progress of their implementation. ENISA should also contribute to covering the need for training and training materials, including the needs of public bodies, and where appropriate, to a high extent, 'train the trainers', building on the Digital Competence Framework for Citizens with a view to assisting Member States and Union institutions, bodies, offices and agencies in developing their own training capabilities.

(27) ENISA should support Member States in the field of cybersecurity awareness-raising and education by facilitating closer coordination and the exchange of best practices between Member States. Such support could consist in the development of a network of national education points of contact and the development of a cybersecurity training platform. The network of national education points of contact could operate within the National Liaison Officers Network and be a starting point for future coordination within the Members States.

(28) ENISA should assist the Cooperation Group created by Directive (EU) 2016/1148 in the execution of its tasks, in particular by providing expertise, advice and by facilitating the exchange of best practices, inter alia, with regard to the identification of operators of essential services by Member States, as well as in relation to cross-border dependencies, regarding risks and incidents.

(29) With a view to stimulating cooperation between the public and private sector and within the private sector, in particular to support the protection of the critical infrastructures, ENISA should support information sharing within and among sectors, in particular the sectors listed in Annex II to Directive (EU) 2016/1148, by providing best practices and guidance on available tools and on procedure, as well as by providing guidance on how to address regulatory issues related to information sharing, for example through facilitating the establishment of sectoral information sharing and analysis centres.

(30) Whereas the potential negative impact of vulnerabilities in ICT products, ICT services and ICT processes is constantly increasing, finding and remedying such vulnerabilities plays an important role in reducing the overall cybersecurity risk. Cooperation between organisations, manufacturers or providers of vulnerable ICT products, ICT services and ICT processes and members of the cybersecurity research community and governments who find vulnerabilities has been proven to significantly increase both the rate of discovery and the remedy of vulnerabilities in ICT products, ICT services and ICT processes. Coordinated vulnerability disclosure specifies a structured process of cooperation in which vulnerabilities are reported to the owner of the information system, allowing the organisation the opportunity to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or to the public. The process also provides for coordination between the finder and the organisation as regards the publication of those vulnerabilities. Coordinated vulnerability disclosure policies could play an important role in Member States' efforts to enhance cybersecurity.

(31) ENISA should aggregate and analyse voluntarily shared national reports from CSIRTs and the inter-institutional computer emergency response team for the Union's institutions, bodies and agencies established by the Arrangement between the European Parliament, the European Council, the Council of the European Union, the European Commission, the Court of Justice of the European Union, the European Central Bank, the European Court of Auditors, the European External Action Service, the European Economic and Social Committee, the European Committee of the Regions and the European Investment Bank on the organisation and operation of a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU) ([14]) in order to contribute to the setting up of common procedures, language and terminology for the exchange of information. In that context ENISA should involve the private sector within the framework of Directive (EU) 2016/1148 which lays down the grounds for the voluntary exchange of technical information at the operational level, in the computer security incident response teams network ('CSIRTs network') created by that Directive.

(32) ENISA should contribute to responses at Union level in the case of large-scale cross-border incidents and crises related to cybersecurity. That task should be performed in accordance with ENISA's mandate under this Regulation and an approach to be agreed by Member States in the context of Commission Recommendation (EU) 2017/1584 ([15]) and the Council conclusions of 26 June 2018 on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises. That task could include gathering relevant information and acting as a facilitator between the CSIRTs network and the technical community, as well as between decision makers responsible for crisis management. Furthermore, ENISA should support operational cooperation among Member States, where requested by one or more Member States, in the handling of incidents from a technical perspective, by facilitating relevant exchanges of technical solutions between Member States, and by providing input into public communications. ENISA should support operational cooperation by testing the arrangements for such cooperation through regular cybersecurity exercises.

(33) In supporting operational cooperation, ENISA should make use of the available technical and operational expertise of CERT-EU through structured cooperation. Such structured cooperation could build on ENISA's expertise. Where appropriate, dedicated arrangements between the two entities should be established to define the practical implementation of such cooperation and to avoid the duplication of activities.

(34) In performing its task to support operational cooperation within the CSIRTs network, ENISA should be able to provide support to Member States at their request, such as by providing advice on how to improve their capabilities to prevent, detect and respond to incidents, by facilitating the technical handling of incidents having a significant or substantial impact or by ensuring that cyber threats and incidents are analysed. ENISA should facilitate the technical handling of incidents having a significant or substantial impact in particular by supporting the voluntary sharing of technical solutions between Member States or by producing combined technical information, such as technical solutions voluntarily shared by the Member States. Recommendation (EU) 2017/1584 recommends that Member States cooperate in good faith and share among themselves and with ENISA information on large-scale incidents and crises related to cybersecurity without undue delay. Such information would further help ENISA in performing its task of supporting operational cooperation.

(35) As part of the regular cooperation at technical level to support Union situational awareness, ENISA, in close cooperation with the Member States, should prepare a regular in-depth EU Cybersecurity Technical Situation Report on incidents and cyber threats, based on publicly available information, its own analysis and reports shared with it by Member States' CSIRTs or the national single points of contact on the security of network and information systems ('single points of contact') provided for in Directive (EU) 2016/1148, both on a voluntary basis, the European Cybercrime Centre (EC3) at Europol, CERT-EU and, where appropriate, the European Union Intelligence and Situation Centre (EU INTCEN) at the European External Action Service. That report should be made available to the Council, the Commission, the High Representative of the Union for Foreign Affairs and Security Policy and the CSIRTs network.

(36) The support by ENISA for *ex-post* technical inquiries of incidents having a significant or substantial impact undertaken at the request of the Member States concerned should focus on the prevention of future incidents. The Member States concerned should provide the necessary information and assistance in order to enable ENISA to support the *ex-post* technical inquiry effectively.

([14]) OJ C 12, 13.1.2018, p. 1.
([15]) Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

(37) Member States may invite the undertakings concerned by the incident to cooperate by providing necessary information and assistance to ENISA without prejudice to their right to protect commercially sensitive information and information that is relevant to public security.

(38) To understand better the challenges in the area of cybersecurity, and with a view to providing strategic long-term advice to Member States and Union institutions, bodies, offices and agencies, ENISA needs to analyse current and emerging cybersecurity risks. For that purpose, ENISA should, in cooperation with Member States and, as appropriate, with statistical bodies and other bodies, collect relevant publicly available or voluntarily shared information and perform analyses of emerging technologies and provide topic-specific assessments on the expected societal, legal, economic and regulatory impact of technological innovations on network and information security, in particular cybersecurity. ENISA should, furthermore, support Member States and Union institutions, bodies, offices and agencies in identifying emerging cybersecurity risks and preventing incidents, by performing analyses of cyber threats, vulnerabilities and incidents.

(39) In order to increase the resilience of the Union, ENISA should develop expertise in the field of cybersecurity of infrastructures, in particular to support the sectors listed in Annex II to Directive (EU) 2016/1148 and those used by the providers of the digital services listed in Annex III to that Directive, by providing advice, issuing guidelines and exchanging best practices. With a view to ensuring easier access to better-structured information on cybersecurity risks and possible remedies, ENISA should develop and maintain the 'information hub' of the Union, a one-stop-shop portal providing the public with information on cybersecurity originating in Union and national institutions, bodies, offices and agencies. Facilitating access to better-structured information on cybersecurity risks and possible remedies could also help Member States bolster their capacities and align their practices, thus increasing their overall resilience to cyberattacks.

(40) ENISA should contribute to raising the public's awareness of cybersecurity risks, including through an EU-wide awareness-raising campaign by promoting education, and to providing guidance on good practices for individual users aimed at citizens, organisations and businesses. ENISA should also contribute to promoting best practices and solutions, including cyber-hygiene and cyber-literacy at the level of citizens, organisations and businesses by collecting and analysing publicly available information regarding significant incidents, and by compiling and publishing reports and guidance for citizens, organisations and businesses, to improve their overall level of preparedness and resilience. ENISA should also strive to provide consumers with relevant information on applicable certification schemes, for example by providing guidelines and recommendations. ENISA should furthermore organise, in line with the Digital Education Action Plan established in the Commission Communication of 17 January 2018 and in cooperation with the Member States and Union institutions, bodies, offices and agencies regular outreach and public education campaigns directed at end users, to promote safer online behaviour by individuals and digital literacy, to raise awareness of potential cyber threats, including online criminal activities such as phishing attacks, botnets, financial and banking fraud, data fraud incidents, and to promote basic multi-factor authentication, patching, encryption, anonymisation and data protection advice.

(41) ENISA should play a central role in accelerating end-user awareness of the security of devices and the secure use of services, and should promote security-by-design and privacy-by-design at Union level. In pursuing that objective, ENISA should make use of available best practices and experience, especially the best practices and experience of academic institutions and IT security researchers.

(42) In order to support the businesses operating in the cybersecurity sector, as well as the users of cybersecurity solutions, ENISA should develop and maintain a 'market observatory' by performing regular analyses and disseminating information on the main trends in the cybersecurity market, on both the demand and supply sides.

(43) ENISA should contribute to the Union's efforts to cooperate with international organisations as well as within relevant international cooperation frameworks in the field of cybersecurity. In particular, ENISA should contribute, where appropriate, to cooperation with organisations such as the OECD, the OSCE and NATO. Such cooperation could include joint cybersecurity exercises and joint incident response coordination. Those activities are to be carried out in full respect of the principles of inclusiveness, reciprocity and the decision-making autonomy of the Union, without prejudice to the specific character of the security and defence policy of any Member State.

(44) In order to ensure that it fully achieves its objectives, ENISA should liaise with the relevant Union supervisory authorities and with other competent authorities in the Union, Union institutions, bodies, offices and agencies, including CERT-EU, EC3, the European Defence Agency (EDA), the European Global Navigation Satellite Systems Agency (European GNSS Agency), the Body of European Regulators for Electronic Communications (BEREC), the European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), the European Central Bank (ECB), the European Banking Authority (EBA), the European Data Protection Board, the Agency for the Cooperation of Energy Regulators (ACER), the European Union Aviation Safety Agency (EASA) and any other Union agency involved in cybersecurity. ENISA should also liaise with authorities that deal with data protection in order to exchange know-how and best practices and should provide advice on cybersecurity issues that might have an impact on their work. Representatives of national and Union law enforcement and data protection authorities should be eligible to be represented in the ENISA Advisory Group. In liaising with law enforcement authorities regarding network and information security issues that might have an impact on their work, ENISA should respect existing channels of information and established networks.

(45) Partnerships could be established with academic institutions that have research initiatives in relevant fields, and there should be appropriate channels for input from consumer organisations and other organisations, which should be taken into consideration.

(46) ENISA, in its role as the secretariat of the CSIRTs network, should support Member States' CSIRTs and the CERT-EU in the operational cooperation in relation to the relevant tasks of the CSIRTs network, as referred to in Directive (EU) 2016/1148. Furthermore, ENISA should promote and support cooperation between the relevant CSIRTs in the event of incidents, attacks or disruptions of networks or infrastructure managed or protected by the CSIRTs and involving or being capable of involving at least two CSIRTs while taking due account of the Standard Operating Procedures of the CSIRTs network.

(47) With a view to increasing Union preparedness in responding to incidents, ENISA should regularly organise cybersecurity exercises at Union level, and, at their request, support Member States and Union institutions, bodies, offices and agencies in organising such exercises. Large-scale comprehensive exercises which include technical, operational or strategic elements should be organised on a biennial basis. In addition, ENISA should be able to regularly organise less comprehensive exercises with the same goal of increasing Union preparedness in responding to incidents.

(48) ENISA should further develop and maintain its expertise on cybersecurity certification with a view to supporting the Union policy in that area. ENISA should build on existing best practices and should promote the uptake of cybersecurity certification within the Union, including by contributing to the establishment and maintenance of a cybersecurity certification framework at Union level (European cybersecurity certification framework) with a view to increasing the transparency of the cybersecurity assurance of ICT products, ICT services and ICT processes, thereby strengthening trust in the digital internal market and its competitiveness.

(49) Efficient cybersecurity policies should be based on well-developed risk assessment methods, in both the public and private sectors. Risk assessment methods are used at different levels, with no common practice regarding how to apply them efficiently. Promoting and developing best practices for risk assessment and for interoperable risk management solutions in public-sector and private-sector organisations will increase the level of cybersecurity in the Union. To that end, ENISA should support cooperation between stakeholders at Union level and facilitate their efforts relating to the establishment and take-up of European and international standards for risk management and for the measurable security of electronic products, systems, networks and services which, together with software, comprise the network and information systems.

(50) ENISA should encourage Member States, manufacturers or providers of ICT products, ICT services or ICT processes to raise their general security standards so that all internet users can take the necessary steps to ensure their own personal cybersecurity and should give incentives to do so. In particular, manufacturers and providers of ICT products, ICT services or ICT processes should provide any necessary updates and should recall, withdraw or recycle ICT products, ICT services or ICT processes that do not meet cybersecurity standards, while importers and distributors should make sure that the ICT products, ICT services and ICT processes they place on the Union market comply with the applicable requirements and do not present a risk to Union consumers.

(51) In cooperation with competent authorities, ENISA should be able to disseminate information regarding the level of the cybersecurity of the ICT products, ICT services and ICT processes offered in the internal market, and should issue warnings targeting manufacturers or providers of ICT products, ICT services or ICT processes and requiring them to improve the security of their ICT products, ICT services and ICT processes, including the cybersecurity.

(52) ENISA should take full account of the ongoing research, development and technological assessment activities, in particular those activities carried out by the various Union research initiatives to advise Union institutions, bodies, offices and agencies and where relevant, the Member States at their request, on research needs and priorities in the field of cybersecurity. In order to identify the research needs and priorities, ENISA should also consult the relevant user groups. More specifically, cooperation with the European Research Council, the European Institute for Innovation and Technology and the European Union Institute for Security Studies could be established.

(53) ENISA should regularly consult standardisation organisations, in particular European standardisation organisations, when preparing the European cybersecurity certification schemes.

(54) Cyber threats are a global issue. There is a need for closer international cooperation to improve cybersecurity standards, including the need for definitions of common norms of behaviour, the adoption of codes of conduct, the use of international standards, and information sharing, promoting swifter international collaboration in response to network and information security issues and promoting a common global approach to such issues. To that end, ENISA should support further Union involvement and cooperation with third countries and international organisations by providing the necessary expertise and analysis to the relevant Union institutions, bodies, offices and agencies, where appropriate.

(55) ENISA should be able to respond to ad hoc requests for advice and assistance by Member States and Union institutions, bodies, offices and agencies on matters falling within ENISA's mandate.

(56) It is sensible and recommended to implement certain principles regarding the governance of ENISA in order to comply with the Joint Statement and Common Approach agreed upon in July 2012 by the Inter-Institutional Working Group on EU decentralised agencies, the purpose of which is to streamline the activities of decentralised agencies and improve their performance. The recommendations in the Joint Statement and Common Approach should also be reflected, as appropriate, in ENISA's work programmes, evaluations of ENISA, and ENISA's reporting and administrative practice.

(57) The Management Board, composed of the representatives of the Member States and of the Commission, should establish the general direction of ENISA's operations and ensure that it carries out its tasks in accordance with this Regulation. The Management Board should be entrusted with the powers necessary to establish the budget, verify the execution of the budget, adopt appropriate financial rules, establish transparent working procedures for decision making by ENISA, adopt ENISA's single programming document, adopt its own rules of procedure, appoint the Executive Director and decide on the extension and termination of the Executive Director's term of office.

(58) In order for ENISA to function properly and effectively, the Commission and the Member States should ensure that persons to be appointed to the Management Board have appropriate professional expertise and experience. The Commission and the Member States should also make efforts to limit the turnover of their respective representatives on the Management Board in order to ensure continuity in its work.

(59) The smooth functioning of ENISA requires that its Executive Director be appointed on grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant to cybersecurity. The duties of the Executive Director should be carried out with complete independence. The Executive Director should prepare a proposal for ENISA's annual work programme, after prior consultation with the Commission, and should take all steps necessary to ensure the proper implementation of that work programme. The Executive Director should prepare an annual report to be submitted to the Management Board, covering the implementation of ENISA's annual work programme, draw up a draft statement of estimates of revenue and expenditure for ENISA, and implement the budget. Furthermore, the Executive Director should have the option of setting up ad hoc working groups to address specific matters, in particular matters of a scientific, technical, legal or socioeconomic nature. In particular, in relation to the preparation of a specific candidate European cybersecurity certification scheme ('candidate scheme'), the setting up of an ad hoc working group is considered to be necessary. The

Executive Director should ensure that the members of ad hoc working groups are selected according to the highest standards of expertise, aiming to ensure gender balance and an appropriate balance, according to the specific issues in question, between the public administrations of the Member States, the Union institutions, bodies, offices and agencies and the private sector, including industry, users, and academic experts in network and information security.

(60) The Executive Board should contribute to the effective functioning of the Management Board. As part of its preparatory work related to Management Board decisions, the Executive Board should examine relevant information in detail, explore available options and offer advice and solutions to prepare the decisions of the Management Board.

(61) ENISA should have an ENISA Advisory Group as an advisory body to ensure regular dialogue with the private sector, consumers' organisations and other relevant stakeholders. The ENISA Advisory Group, established by the Management Board on a proposal from the Executive Director, should focus on issues relevant to stakeholders and should bring them to the attention of ENISA. The ENISA Advisory Group should be consulted in particular with regard to ENISA's draft annual work programme. The composition of the ENISA Advisory Group and the tasks assigned to it should ensure sufficient representation of stakeholders in the work of ENISA.

(62) The Stakeholder Cybersecurity Certification Group should be established in order to help ENISA and the Commission facilitate the consultation of relevant stakeholders. The Stakeholder Cybersecurity Certification Group should be composed of members representing industry in balanced proportions, both on the demand side and the supply side of ICT products and ICT services, and including, in particular, SMEs, digital service providers, European and international standardisation bodies, national accreditation bodies, data protection supervisory authorities and conformity assessment bodies pursuant to Regulation (EC) No 765/2008 of the European Parliament and of the Council ([16]), and academia as well as consumer organisations.

(63) ENISA should have rules in place regarding the prevention and the management of conflicts of interest. ENISA should also apply the relevant Union provisions concerning public access to documents as set out in Regulation (EC) No 1049/2001 of the European Parliament and of the Council ([17]). The processing of personal data by ENISA should be subject to Regulation (EU) 2018/1725 of the European Parliament and of the Council ([18]). ENISA should comply with the provisions applicable to the Union institutions, bodies, offices and agencies, and with national legislation regarding the handling of information, in particular sensitive non-classified information and European Union classified information (EUCI).

(64) In order to guarantee the full autonomy and independence of ENISA and to enable it to perform additional tasks, including unforeseen emergency tasks, ENISA should be granted a sufficient and autonomous budget whose revenue should primarily come from a contribution from the Union and contributions from third countries participating in ENISA's work. An appropriate budget is paramount for ensuring that ENISA has sufficient capacity to perform all of its growing tasks and to achieve its objectives. The majority of ENISA's staff should be directly engaged in the operational implementation of ENISA's mandate. The host Member State, and any other Member State, should be allowed to make voluntary contributions to ENISA's budget. The Union's budgetary procedure should remain applicable as far as any subsidies chargeable to the general budget of the Union are concerned. Moreover, the Court of Auditors should audit ENISA's accounts to ensure transparency and accountability.

(65) Cybersecurity certification plays an important role in increasing trust and security in ICT products, ICT services and ICT processes. The digital single market, and in particular the data economy and the IoT, can thrive only if there is general public trust that such products, services and processes provide a certain level of cybersecurity. Connected and automated cars, electronic medical devices, industrial automation control systems and smart grids are only some examples of sectors in which certification is already widely used or is likely to be used in the near future. The sectors regulated by Directive (EU) 2016/1148 are also sectors in which cybersecurity certification is critical.

([16]) Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

([17]) Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

([18]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

(66) In the 2016 Communication 'Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry', the Commission outlined the need for high-quality, affordable and interoperable cybersecurity products and solutions. The supply of ICT products, ICT services and ICT processes within the single market remains very fragmented geographically. This is because the cybersecurity industry in Europe has developed largely on the basis of national governmental demand. In addition, the lack of interoperable solutions (technical standards), practices and Union-wide mechanisms of certification are among the other gaps affecting the single market in the field of cybersecurity. This makes it difficult for European businesses to compete at national, Union and global level. It also reduces the choice of viable and usable cybersecurity technologies that individuals and businesses have access to. Similarly, in the 2017 Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy – A Connected Digital Single Market for All, the Commission highlighted the need for safe connected products and systems, and indicated that the creation of a European ICT security framework setting rules on how to organise ICT security certification in the Union could both preserve trust in the internet and tackle the current fragmentation of the internal market.

(67) Currently, the cybersecurity certification of ICT products, ICT services and ICT processes is used only to a limited extent. When it exists, it mostly occurs at Member State level or in the framework of industry driven schemes. In that context, a certificate issued by a national cybersecurity certification authority is not in principle recognised in other Member States. Companies thus may have to certify their ICT products, ICT services and ICT processes in several Member States where they operate, for example, with a view to participating in national procurement procedures, which thereby adds to their costs. Moreover, while new schemes are emerging, there seems to be no coherent and holistic approach to horizontal cybersecurity issues, for instance in the field of the IoT. Existing schemes present significant shortcomings and differences in terms of product coverage, levels of assurance, substantive criteria and actual use, impeding mutual recognition mechanisms within the Union.

(68) Some efforts have been made in order to ensure the mutual recognition of certificates within the Union. However, they have been only partly successful. The most important example in this regard is the Senior Officials Group – Information Systems Security (SOG-IS) Mutual Recognition Agreement (MRA). While it represents the most important model for cooperation and mutual recognition in the field of security certification, SOG-IS includes only some of the Member States. That fact has limited the effectiveness of SOG-IS MRA from the point of view of the internal market.

(69) Therefore, it is necessary to adopt a common approach and to establish a European cybersecurity certification framework that lays down the main horizontal requirements for European cybersecurity certification schemes to be developed and allows European cybersecurity certificates and EU statements of conformity for ICT products, ICT services or ICT processes to be recognised and used in all Member States. In doing so, it is essential to build on existing national and international schemes, as well as on mutual recognition systems, in particular SOG-IS, and to make possible a smooth transition from the existing schemes under such systems to schemes under the new European cybersecurity certification framework. The European cybersecurity certification framework should have a twofold purpose. First, it should help increase trust in ICT products, ICT services and ICT processes that have been certified under European cybersecurity certification schemes. Second, it should help avoid the multiplication of conflicting or overlapping national cybersecurity certification schemes and thus reduce costs for undertakings operating in the digital single market. The European cybersecurity certification schemes should be non-discriminatory and based on European or international standards, unless those standards are ineffective or inappropriate to fulfil the Union's legitimate objectives in that regard.

(70) The European cybersecurity certification framework should be established in a uniform manner in all Member States in order to prevent 'certification shopping' based on different levels of stringency in different Member States.

(71) European cybersecurity certification schemes should be built on what already exists at international and national level and, if necessary, on technical specifications from forums and consortia, learning from current strong points and assessing and correcting weaknesses.

(72) Flexible cybersecurity solutions are necessary for the industry to stay ahead of cyber threats, and therefore any certification scheme should be designed in a way that avoids the risk of being outdated quickly.

(73) The Commission should be empowered to adopt European cybersecurity certification schemes concerning specific groups of ICT products, ICT services and ICT processes. Those schemes should be implemented and supervised by national cybersecurity certification authorities, and certificates issued under those schemes should be valid and recognised throughout the Union. Certification schemes operated by the industry or by other private organisations should fall outside of the scope of this Regulation. However, the bodies operating such schemes should be able to propose that the Commission consider such schemes as a basis for approving them as a European cybersecurity certification scheme.

(74) The provisions of this Regulation should be without prejudice to Union law providing specific rules on the certification of ICT products, ICT services and ICT processes. In particular, Regulation (EU) 2016/679 lays down provisions for the establishment of certification mechanisms and of data protection seals and marks, for the purpose of demonstrating the compliance of processing operations by controllers and processors with that Regulation. Such certification mechanisms and data protection seals and marks should allow data subjects to quickly assess the level of data protection of the relevant ICT products, ICT services and ICT processes. This Regulation is without prejudice to the certification of data processing operations under Regulation (EU) 2016/679, including when such operations are embedded in ICT products, ICT services and ICT processes.

(75) The purpose of European cybersecurity certification schemes should be to ensure that ICT products, ICT services and ICT processes certified under such schemes comply with specified requirements that aim to protect the availability, authenticity, integrity and confidentiality of stored, transmitted or processed data or of the related functions of or services offered by, or accessible via those products, services and processes throughout their life cycle. It is not possible to set out in detail the cybersecurity requirements relating to all ICT products, ICT services and ICT processes in this Regulation. ICT products, ICT services and ICT processes and the cybersecurity needs related to those products, services and processes are so diverse that it is very difficult to develop general cybersecurity requirements that are valid in all circumstances. It is therefore necessary to adopt a broad and general notion of cybersecurity for the purpose of certification, which should be complemented by a set of specific cybersecurity objectives that are to be taken into account when designing European cybersecurity certification schemes. The arrangements by which such objectives are to be achieved in specific ICT products, ICT services and ICT processes should then be further specified in detail at the level of the individual certification scheme adopted by the Commission, for example by reference to standards or technical specifications if no appropriate standards are available.

(76) The technical specifications to be used in European cybersecurity certification schemes should respect the requirements set out in Annex II to Regulation (EU) No 1025/2012 of the European Parliament and of the Council ([19]). Some deviations from those requirements could, however, be considered to be necessary in duly justified cases where those technical specifications are to be used in a European cybersecurity certification scheme referring to assurance level 'high'. The reasons for such deviations should be made publicly available.

(77) A conformity assessment is a procedure for evaluating whether specified requirements relating to an ICT product, ICT service or ICT process have been fulfilled. That procedure is carried out by an independent third party that is not the manufacturer or provider of the ICT products, ICT services or ICT processes that are being assessed. A European cybersecurity certificate should be issued following the successful evaluation of an ICT product, ICT service or ICT process. A European cybersecurity certificate should be considered to be a confirmation that the evaluation has been properly carried out. Depending on the assurance level, the European cybersecurity certification scheme should indicate whether the European cybersecurity certificate is to be issued by a private or public body. Conformity assessment and certification cannot guarantee per se that certified ICT products, ICT services and ICT processes are cyber secure. They are instead procedures and technical methodologies for attesting that ICT products, ICT services and ICT processes have been tested and that they comply with certain cybersecurity requirements laid down elsewhere, for example in technical standards.

(78) The choice of the appropriate certification and associated security requirements by the users of European cybersecurity certificates should be based on an analysis of the risks associated with the use of the ICT products, ICT services or ICT processes. Accordingly, the assurance level should be commensurate with the level of the risk associated with the intended use of an ICT product, ICT service or ICT process.

([19]) Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

(79) European cybersecurity certification schemes could provide for a conformity assessment to be carried out under the sole responsibility of the manufacturer or provider of ICT products, ICT services or ICT processes ('conformity self-assessment'). In such cases, it should be sufficient that the manufacturer or provider of ICT products, ICT services or ICT processes itself carry out all of the checks to ensure that the ICT products, ICT services or ICT processes conform with the European cybersecurity certification scheme. Conformity self-assessment should be considered to be appropriate for low complexity ICT products, ICT services or ICT processes that present a low risk to the public, such as simple design and production mechanisms. Moreover, conformity self-assessment should be permitted for ICT products, ICT services or ICT processes only where they correspond to assurance level 'basic'.

(80) European cybersecurity certification schemes could allow for both conformity self-assessments and certifications of ICT products, ICT services or ICT processes. In such a case, the scheme should provide for clear and understandable means for consumers or other users to differentiate between ICT products, ICT services or ICT processes with regard to which the manufacturer or provider of ICT products, ICT services or ICT processes is responsible for the assessment, and ICT products, ICT services or ICT processes that are certified by a third party.

(81) The manufacturer or provider of ICT products, ICT services or ICT processes who carry out a conformity self-assessment should be able to issue and sign the EU statement of conformity as part of the conformity assessment procedure. An EU statement of conformity is a document that states that a specific ICT product, ICT service or ICT process complies with the requirements of the European cybersecurity certification scheme. By issuing and signing the EU statement of conformity, the manufacturer or provider of ICT products, ICT services or ICT processes assumes responsibility for the compliance of the ICT product, ICT service or ICT process with the legal requirements of the European cybersecurity certification scheme. A copy of the EU statement of conformity should be submitted to the national cybersecurity certification authority and to ENISA.

(82) Manufacturers or providers of ICT products, ICT services or ICT processes should make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity of the ICT products, ICT services or ICT processes with a European cybersecurity certification scheme available to the competent national cybersecurity certification authority for a period provided for in the relevant European cybersecurity certification scheme. The technical documentation should specify the requirements applicable under the scheme and should cover the design, manufacture and operation of the ICT product, ICT service or ICT process to the extent relevant to the conformity self-assessment. The technical documentation should be so compiled as to enable the assessment of whether an ICT product or ICT service complies with the requirements applicable under that scheme.

(83) The governance of the European cybersecurity certification framework takes into account the involvement of Member States as well as the appropriate involvement of stakeholders, and establishes the role of the Commission during the planning and proposing, requesting, preparing, adopting and reviewing of European cybersecurity certification schemes.

(84) The Commission should prepare, with the support of the European Cybersecurity Certification Group (the 'ECCG') and the Stakeholder Cybersecurity Certification Group and after an open and wide consultation, a Union rolling work programme for European cybersecurity certification schemes and should publish it in the form of a non-binding instrument. The Union rolling work programme should be a strategic document that allows industry, national authorities and standardisation bodies, in particular, to prepare in advance for future European cybersecurity certification schemes. The Union rolling work programme should include a multiannual overview of the requests for candidate schemes which the Commission intends to submit to ENISA for preparation on the basis of specific grounds. The Commission should take into account the Union rolling work programme while preparing its Rolling Plan for ICT Standardisation and standardisation requests to European standardisation organisations. In light of the rapid introduction and uptake of new technologies, the emergence of previously unknown cybersecurity risks, and legislative and market developments, the Commission or the ECCG should be entitled to request ENISA to prepare candidate schemes which have not been included in the Union rolling work programme. In such cases, the Commission and the ECCG should also assess the necessity of such a request, taking into account the overall aims and objectives of this Regulation and the need to ensure continuity as regards ENISA's planning and use of resources.

Following such a request, ENISA should prepare the candidate schemes for specific ICT products, ICT services and ICT processes without undue delay. The Commission should evaluate the positive and negative impact of its request on the specific market in question, especially its impact on SMEs, on innovation, on barriers to entry to that market and on costs to end users. The Commission, on the basis of the candidate scheme prepared by ENISA, should be empowered to adopt the European cybersecurity certification scheme by means of implementing acts. Taking account of the general purpose and security objectives laid down in this Regulation, European cybersecurity certification schemes adopted by the Commission should specify a minimum set of elements concerning the subject matter, scope and functioning of the individual scheme. Those elements should include, among other things, the scope and object of the cybersecurity certification, including the categories of ICT products, ICT services and ICT processes covered, the detailed specification of the cybersecurity requirements, for example by reference to standards or technical specifications, the specific evaluation criteria and evaluation methods, as well as the intended assurance level ('basic', 'substantial' or 'high') and the evaluation levels where applicable. ENISA should be able to refuse a request by the ECCG. Such decisions should be taken by the Management Board and should be duly reasoned.

(85) ENISA should maintain a website providing information on and publicising European cybersecurity certification schemes, which should include, among other things, the requests for the preparation of a candidate scheme as well as the feedback received in the consultation process carried out by ENISA in the preparation phase. The website should also provide information about the European cybersecurity certificates and EU statements of conformity issued under this Regulation including information regarding the withdrawal and expiry of such European cybersecurity certificates and EU statements of conformity. The website should also indicate the national cybersecurity certification schemes that have been replaced by a European cybersecurity certification scheme.

(86) The assurance level of a European certification scheme is a basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme. In order to ensure the consistency of the European cybersecurity certification framework, a European cybersecurity certification scheme should be able to specify assurance levels for European cybersecurity certificates and EU statements of conformity issued under that scheme. Each European cybersecurity certificate might refer to one of the assurance levels: 'basic', 'substantial' or 'high', while the EU statement of conformity might only refer to the assurance level 'basic'. The assurance levels would provide the corresponding rigour and depth of the evaluation of the ICT product, ICT service or ICT process and would be characterised by reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to mitigate or prevent incidents. Each assurance level should be consistent among the different sectorial domains where certification is applied.

(87) A European cybersecurity certification scheme might specify several evaluation levels depending on the rigour and depth of the evaluation methodology used. Evaluation levels should correspond to one of the assurance levels and should be associated with an appropriate combination of assurance components. For all assurance levels, the ICT product, ICT service or ICT process should contain a number of secure functions, as specified by the scheme, which may include: a secure out-of-the-box configuration, a signed code, secure update and exploit mitigations and full stack or heap memory protections. Those functions should have been developed, and be maintained, using security-focused development approaches and associated tools to ensure that effective software and hardware mechanisms are reliably incorporated.

(88) For assurance level 'basic', the evaluation should be guided at least by the following assurance components: the evaluation should at least include a review of the technical documentation of the ICT product, ICT service or ICT process by the conformity assessment body. Where the certification includes ICT processes, the process used to design, develop and maintain an ICT product or ICT service should also be subject to the technical review. Where a European cybersecurity certification scheme provides for a conformity self-assessment, it should be sufficient that the manufacturer or provider of ICT products, ICT services or ICT processes has carried out a self-assessment of the compliance of the ICT product, ICT service or ICT process with the certification scheme.

(89) For assurance level 'substantial', the evaluation, in addition to the requirements for assurance level 'basic', should be guided at least by the verification of the compliance of the security functionalities of the ICT product, ICT service or ICT process with its technical documentation.

(90) For assurance level 'high', the evaluation, in addition to the requirements for assurance level 'substantial', should be guided at least by an efficiency testing which assesses the resistance of the security functionalities of ICT product, ICT service or ICT process against elaborate cyberattacks performed by persons who have significant skills and resources.

(91) Recourse to European cybersecurity certification and to EU statements of conformity should remain voluntary, unless otherwise provided for in Union law, or in Member State law adopted in accordance with Union law. In the absence of harmonised Union law, Member States are able to adopt national technical regulations providing for mandatory certification under a European cybersecurity certification scheme in accordance with Directive (EU) 2015/1535 of the European Parliament and of the Council ([20]). Member States also have recourse to European cybersecurity certification in the context of public procurement and of Directive 2014/24/EU of the European Parliament and of the Council ([21]).

(92) In some areas, it could be necessary in the future to impose specific cybersecurity requirements and make the certification thereof mandatory for certain ICT products, ICT services or ICT processes, in order to improve the level of cybersecurity in the Union. The Commission should regularly monitor the impact of adopted European cybersecurity certification schemes on the availability of secure ICT products, ICT services and ICT processes in the internal market and should regularly assess the level of use of the certification schemes by the manufacturers or providers of ICT products, ICT services or ICT processes in the Union. The efficiency of the European cybersecurity certification schemes, and whether specific schemes should be made mandatory, should be assessed in light of the cybersecurity-related legislation of the Union, in particular Directive (EU) 2016/1148, taking into consideration the security of the network and information systems used by operators of essential services.

(93) European cybersecurity certificates and EU statements of conformity should help end users to make informed choices. Therefore, ICT products, ICT services and ICT processes that have been certified or for which an EU statement of conformity has been issued should be accompanied by structured information that is adapted to the expected technical level of the intended end user. All such information should be available online, and, where appropriate, in physical form. The end user should have access to information regarding the reference number of the certification scheme, the assurance level, the description of the cybersecurity risks associated with the ICT product, ICT service or ICT process, and the issuing authority or body, or should be able to obtain a copy of the European cybersecurity certificate. In addition, the end user should be informed of the cybersecurity support policy, namely for how long the end user can expect to receive cybersecurity updates or patches, of the manufacturer or provider of ICT products, ICT services or ICT processes. Where applicable, guidance on actions or settings that the end user can implement to maintain or increase the cybersecurity of the ICT product or of the ICT service and contact information of a single point of contact to report and receive support in the case of cyberattacks (in addition to automatic reporting) should be provided. That information should be regularly updated and made available on a website providing information on European cybersecurity certification schemes.

(94) With a view to achieving the objectives of this Regulation and avoiding the fragmentation of the internal market, national cybersecurity certification schemes or procedures for ICT products, ICT services or ICT processes covered by a European cybersecurity certification scheme should cease to be effective from a date established by the Commission by means of implementing acts. Moreover, Member States should not introduce new national cybersecurity certification schemes for ICT products, ICT services or ICT processes already covered by an existing European cybersecurity certification scheme. However, Member States should not be prevented from adopting or maintaining national cybersecurity certification schemes for national security purposes. Member States should inform the Commission and the ECCG of any intention to draw up new national cybersecurity certification schemes. The Commission and the ECCG should evaluate the impact of the new national cybersecurity certification schemes on the proper functioning of the internal market and in light of any strategic interest in requesting a European cybersecurity certification scheme instead.

(95) European cybersecurity certification schemes are intended to help harmonise cybersecurity practices within the Union. They need to contribute to increasing the level of cybersecurity within the Union. The design of the European cybersecurity certification schemes should take into account and allow for the development of innovations in the field of cybersecurity.

([20]) Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

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

(96) European cybersecurity certification schemes should take into account current software and hardware development methods and, in particular, the impact of frequent software or firmware updates on individual European cybersecurity certificates. European cybersecurity certification schemes should specify the conditions under which an update may require that an ICT product, ICT service or ICT process be recertified or that the scope of a specific European cybersecurity certificate be reduced, taking into account any possible adverse effects of the update on compliance with the security requirements of that certificate.

(97) Once a European cybersecurity certification scheme is adopted, manufacturers or providers of ICT products, ICT services or ICT processes should be able to submit applications for certification of their ICT products or ICT services to the conformity assessment body of their choice anywhere in the Union. Conformity assessment bodies should be accredited by a national accreditation body if they comply with certain specified requirements set out in this Regulation. Accreditation should be issued for a maximum of five years and should be renewable on the same conditions provided that the conformity assessment body still meets the requirements. National accreditation bodies should restrict, suspend or revoke the accreditation of a conformity assessment body where the conditions for the accreditation have not been met or are no longer met, or where the conformity assessment body infringes this Regulation.

(98) References in national legislation to national standards which have ceased to be effective due to the entry into force of a European cybersecurity certification scheme can be a source of confusion. Therefore, Member States should reflect the adoption of a European cybersecurity certification scheme in their national legislation.

(99) In order to achieve equivalent standards throughout the Union, to facilitate mutual recognition and to promote the overall acceptance of European cybersecurity certificates and EU statements of conformity, it is necessary to put in place a system of peer review between national cybersecurity certification authorities. Peer review should cover procedures for supervising the compliance of ICT products, ICT services and ICT processes with European cybersecurity certificates, for monitoring the obligations of manufacturers or providers of ICT products, ICT services or ICT processes who carry out the conformity self-assessment, for monitoring conformity assessment bodies, as well as the appropriateness of the expertise of the staff of bodies issuing certificates for assurance level 'high'. The Commission should be able, by means of implementing acts, to establish at least a five-year plan for peer reviews, as well as lay down criteria and methodologies for the operation of the peer review system.

(100) Without prejudice to the general peer review system to be put in place across all national cybersecurity certification authorities within the European cybersecurity certification framework, certain European cybersecurity certification schemes may include a peer-assessment mechanism for the bodies that issue European cybersecurity certificates for ICT products, ICT services and ICT processes with an assurance level 'high' under such schemes. The ECCG should support the implementation of such peer-assessment mechanisms. The peer assessments should assess in particular whether the bodies concerned carry out their tasks in a harmonised way, and may include appeal mechanisms. The results of the peer assessments should be made publicly available. The bodies concerned may adopt appropriate measures to adapt their practices and expertise accordingly.

(101) Member States should designate one or more national cybersecurity certification authorities to supervise compliance with obligations arising from this Regulation. A national cybersecurity certification authority may be an existing or new authority. A Member State should also be able to designate, after agreeing with another Member State, one or more national cybersecurity certification authorities in the territory of that other Member State.

(102) National cybersecurity certification authorities should in particular monitor and enforce the obligations of manufacturers or providers of ICT products, ICT services or ICT processes established in its respective territory in relation to the EU statement of conformity, should assist the national accreditation bodies in the monitoring and supervision of the activities of conformity assessment bodies by providing them with expertise and relevant information, should authorise conformity assessment bodies to carry out their tasks where such bodies meet additional requirements set out in a European cybersecurity certification scheme, and should monitor relevant developments in the field of cybersecurity certification. National cybersecurity certification authorities should also handle complaints lodged by natural or legal persons in relation to European cybersecurity certificates issued by those authorities or in relation to European cybersecurity certificates issued by conformity assessment bodies,

where such certificates indicate assurance level 'high', should investigate, to the extent appropriate, the subject matter of the complaint and should inform the complainant of the progress and the outcome of the investigation within a reasonable period. Moreover, national cybersecurity certification authorities should cooperate with other national cybersecurity certification authorities or other public authorities, including by the sharing of information on the possible non-compliance of ICT products, ICT services and ICT processes with the requirements of this Regulation or with specific European cybersecurity certification schemes. The Commission should facilitate that sharing of information by making available a general electronic information support system, for example the Information and Communication System on Market Surveillance (ICSMS) and the Rapid Alert System for dangerous non-food products (RAPEX), already used by market surveillance authorities pursuant to Regulation (EC) No 765/2008.

(103) With a view to ensuring the consistent application of the European cybersecurity certification framework, an ECCG that consists of representatives of national cybersecurity certification authorities or other relevant national authorities should be established. The main tasks of the ECCG should be to advise and assist the Commission in its work towards ensuring the consistent implementation and application of the European cybersecurity certification framework, to assist and closely cooperate with ENISA in the preparation of candidate cybersecurity certification schemes, in duly justified cases to request ENISA to prepare a candidate scheme, to adopt opinions addressed to ENISA on candidate schemes and to adopt opinions addressed to the Commission on the maintenance and review of existing European cybersecurity certifications schemes. The ECCG should facilitate the exchange of good practices and expertise between the various national cybersecurity certification authorities that are responsible for the authorisation of conformity assessment bodies and the issuance of European cybersecurity certificates.

(104) In order to raise awareness and to facilitate the acceptance of future European cybersecurity certification schemes, the Commission may issue general or sector-specific cybersecurity guidelines, for example on good cybersecurity practices or responsible cybersecurity behaviour highlighting the positive effect of the use of certified ICT products, ICT services and ICT processes.

(105) In order to further facilitate trade, and recognising that ICT supply chains are global, mutual recognition agreements concerning European cybersecurity certificates may be concluded by the Union in accordance with Article 218 of the Treaty on the Functioning of the European Union (TFEU). The Commission, taking into account the advice from ENISA and the European Cybersecurity Certification Group, may recommend the opening of relevant negotiations. Each European cybersecurity certification scheme should provide specific conditions for such mutual recognition agreements with third countries.

(106) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council ([22]).

(107) The examination procedure should be used for the adoption of implementing acts on European cybersecurity certification schemes for ICT products, ICT services or ICT processes, for the adoption of implementing acts on arrangements for carrying out inquiries by ENISA, for the adoption of implementing acts on a plan for the peer review of national cybersecurity certification authorities, as well as for the adoption of implementing acts on the circumstances, formats and procedures of notifications of accredited conformity assessment bodies by the national cybersecurity certification authorities to the Commission.

(108) ENISA's operations should be subject to regular and independent evaluation. That evaluation should have regard to ENISA's objectives, its working practices and the relevance of its tasks, in particular its tasks relating to the operational cooperation at Union level. That evaluation should also assess the impact, effectiveness and efficiency of the European cybersecurity certification framework. In the event of a review, the Commission should evaluate how ENISA's role as a reference point for advice and expertise can be reinforced and should also evaluate the possibility of a role for ENISA in supporting the assessment of third country ICT products, ICT services and ICT processes that do not comply with Union rules, where such products, services and processes enter the Union.

([22]) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(109) Since the objectives of this Regulation cannot be sufficiently achieved by the Member States but can rather, by reason of its scale and effects, 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 (TEU). In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.

(110) Regulation (EU) No 526/2013 should be repealed,

HAVE ADOPTED THIS REGULATION:

TITLE I

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. With a view to ensuring the proper functioning of the internal market while aiming to achieve a high level of cybersecurity, cyber resilience and trust within the Union, this Regulation lays down:

(a) objectives, tasks and organisational matters relating to ENISA (the European Union Agency for Cybersecurity); and

(b) a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.

The framework referred to in point (b) of the first subparagraph applies without prejudice to specific provisions in other Union legal acts regarding voluntary or mandatory certification.

2. This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security and the activities of the State in areas of criminal law.

Article 2

Definitions

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

(1) 'cybersecurity' means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats;

(2) 'network and information system' means a network and information system as defined in point (1) of Article 4 of Directive (EU) 2016/1148;

(3) 'national strategy on the security of network and information systems' means a national strategy on the security of network and information systems as defined in point (3) of Article 4 of Directive (EU) 2016/1148;

(4) 'operator of essential services' means an operator of essential services as defined in point (4) of Article 4 of Directive (EU) 2016/1148;

(5) 'digital service provider' means a digital service provider as defined in point (6) of Article 4 of Directive (EU) 2016/1148;

(6) 'incident' means an incident as defined in point (7) of Article 4 of Directive (EU) 2016/1148;

(7) 'incident handling' means incident handling as defined in point (8) of Article 4 of Directive (EU) 2016/1148;

(8) 'cyber threat' means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons;

(9) 'European cybersecurity certification scheme' means a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes;

(10) 'national cybersecurity certification scheme' means a comprehensive set of rules, technical requirements, standards and procedures developed and adopted by a national public authority and that apply to the certification or conformity assessment of ICT products, ICT services and ICT processes falling under the scope of the specific scheme;

(11) 'European cybersecurity certificate' means a document issued by a relevant body, attesting that a given ICT product, ICT service or ICT process has been evaluated for compliance with specific security requirements laid down in a European cybersecurity certification scheme;

(12) 'ICT product' means an element or a group of elements of a network or information system;

(13) 'ICT service' means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems;

(14) 'ICT process' means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service;

(15) 'accreditation' means accreditation as defined in point (10) of Article 2 of Regulation (EC) No 765/2008;

(16) 'national accreditation body' means a national accreditation body as defined in point (11) of Article 2 of Regulation (EC) No 765/2008;

(17) 'conformity assessment' means a conformity assessment as defined in point (12) of Article 2 of Regulation (EC) No 765/2008;

(18) 'conformity assessment body' means a conformity assessment body as defined in point (13) of Article 2 of Regulation (EC) No 765/2008;

(19) 'standard' means a standard as defined in point (1) of Article 2 of Regulation (EU) No 1025/2012;

(20) 'technical specification' means a document that prescribes the technical requirements to be met by, or conformity assessment procedures relating to, an ICT product, ICT service or ICT process;

(21) 'assurance level' means a basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme, indicates the level at which an ICT product, ICT service or ICT process has been evaluated but as such does not measure the security of the ICT product, ICT service or ICT process concerned;

(22) 'conformity self-assessment' means an action carried out by a manufacturer or provider of ICT products, ICT services or ICT processes, which evaluates whether those ICT products, ICT services or ICT processes meet the requirements of a specific European cybersecurity certification scheme.

TITLE II

ENISA (THE EUROPEAN UNION AGENCY FOR CYBERSECURITY)

CHAPTER I

Mandate and objectives

Article 3

Mandate

1. ENISA shall carry out the tasks assigned to it under this Regulation for the purpose of achieving a high common level of cybersecurity across the Union, including by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. ENISA shall act as a reference point for advice and expertise on cybersecurity for Union institutions, bodies, offices and agencies as well as for other relevant Union stakeholders.

ENISA shall contribute to reducing the fragmentation of the internal market by carrying out the tasks assigned to it under this Regulation.

2. ENISA shall carry out the tasks assigned to it by Union legal acts that set out measures for approximating Member State laws, regulations and administrative provisions which are related to cybersecurity.

3. When carrying out its tasks, ENISA shall act independently while avoiding the duplication of Member State activities and taking into consideration existing Member State expertise.

4. ENISA shall develop its own resources, including technical and human capabilities and skills, necessary to perform the tasks assigned to it under this Regulation.

Article 4

Objectives

1. ENISA shall be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks.

2. ENISA shall assist the Union institutions, bodies, offices and agencies, as well as Member States, in developing and implementing Union policies related to cybersecurity, including sectoral policies on cybersecurity.

3. ENISA shall support capacity-building and preparedness across the Union by assisting the Union institutions, bodies, offices and agencies, as well as Member States and public and private stakeholders, to increase the protection of their network and information systems, to develop and improve cyber resilience and response capacities, and to develop skills and competencies in the field of cybersecurity.

4. ENISA shall promote cooperation, including information sharing and coordination at Union level, among Member States, Union institutions, bodies, offices and agencies, and relevant private and public stakeholders on matters related to cybersecurity.

5. ENISA shall contribute to increasing cybersecurity capabilities at Union level in order to support the actions of Member States in preventing and responding to cyber threats, in particular in the event of cross-border incidents.

6. ENISA shall promote the use of European cybersecurity certification, with a view to avoiding the fragmentation of the internal market. ENISA shall contribute to the establishment and maintenance of a European cybersecurity certification framework in accordance with Title III of this Regulation, with a view to increasing the transparency of the cybersecurity of ICT products, ICT services and ICT processes, thereby strengthening trust in the digital internal market and its competitiveness.

7. ENISA shall promote a high level of cybersecurity awareness, including cyber-hygiene and cyber-literacy among citizens, organisations and businesses.

CHAPTER II

Tasks

Article 5

Development and implementation of Union policy and law

ENISA shall contribute to the development and implementation of Union policy and law, by:

(1) assisting and advising on the development and review of Union policy and law in the field of cybersecurity and on sector-specific policy and law initiatives where matters related to cybersecurity are involved, in particular by providing its independent opinion and analysis as well as carrying out preparatory work;

(2) assisting Member States to implement the Union policy and law regarding cybersecurity consistently, in particular in relation to Directive (EU) 2016/1148, including by means of issuing opinions, guidelines, providing advice and best practices on topics such as risk management, incident reporting and information sharing, as well as by facilitating the exchange of best practices between competent authorities in that regard;

(3) assisting Member States and Union institutions, bodies, offices and agencies in developing and promoting cybersecurity policies related to sustaining the general availability or integrity of the public core of the open internet;

(4) contributing to the work of the Cooperation Group pursuant to Article 11 of Directive (EU) 2016/1148, by providing its expertise and assistance;

(5) supporting:

(a) the development and implementation of Union policy in the field of electronic identity and trust services, in particular by providing advice and issuing technical guidelines, as well as by facilitating the exchange of best practices between competent authorities;

(b) the promotion of an enhanced level of security of electronic communications, including by providing advice and expertise, as well as by facilitating the exchange of best practices between competent authorities;

(c) Member States in the implementation of specific cybersecurity aspects of Union policy and law relating to data protection and privacy, including by providing advice to the European Data Protection Board upon request;

(6) supporting the regular review of Union policy activities by preparing an annual report on the state of the implementation of the respective legal framework regarding:

(a) information on Member States' incident notifications provided by the single points of contact to the Cooperation Group pursuant to Article 10(3) of Directive (EU) 2016/1148;

(b) summaries of notifications of breach of security or loss of integrity received from trust service providers provided by the supervisory bodies to ENISA, pursuant to Article 19(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council ([23]);

(c) notifications of security incidents transmitted by the providers of public electronic communications networks or of publicly available electronic communications services, provided by the competent authorities to ENISA, pursuant to Article 40 of Directive (EU) 2018/1972.

([23]) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

Article 6

Capacity-building

1. ENISA shall assist:

(a) Member States in their efforts to improve the prevention, detection and analysis of, and the capability to respond to cyber threats and incidents by providing them with knowledge and expertise;

(b) Member States and Union institutions, bodies, offices and agencies in establishing and implementing vulnerability disclosure policies on a voluntary basis;

(c) Union institutions, bodies, offices and agencies in their efforts to improve the prevention, detection and analysis of cyber threats and incidents and to improve their capabilities to respond to such cyber threats and incidents, in particular through appropriate support for the CERT-EU;

(d) Member States in developing national CSIRTs, where requested pursuant to Article 9(5) of Directive (EU) 2016/1148;

(e) Member States in developing national strategies on the security of network and information systems, where requested pursuant to Article 7(2) of Directive (EU) 2016/1148, and promote the dissemination of those strategies and note the progress in their implementation across the Union in order to promote best practices;

(f) Union institutions in developing and reviewing Union strategies regarding cybersecurity, promoting their dissemination and tracking the progress in their implementation;

(g) national and Union CSIRTs in raising the level of their capabilities, including by promoting dialogue and exchanges of information, with a view to ensuring that, with regard to the state of the art, each CSIRT possesses a common set of minimum capabilities and operates according to best practices;

(h) Member States by regularly organising the cybersecurity exercises at Union level referred to in Article 7(5) on at least a biennial basis and by making policy recommendations based on the evaluation process of the exercises and lessons learned from them;

(i) relevant public bodies by offering trainings regarding cybersecurity, where appropriate in cooperation with stakeholders;

(j) the Cooperation Group, in the exchange of best practices, in particular with regard to the identification by Member States of operators of essential services, pursuant to point (l) of Article 11(3) of Directive (EU) 2016/1148, including in relation to cross-border dependencies, regarding risks and incidents.

2. ENISA shall support information sharing in and between sectors, in particular in the sectors listed in Annex II to Directive (EU) 2016/1148, by providing best practices and guidance on available tools, procedures, as well as on how to address regulatory issues related to information-sharing.

Article 7

Operational cooperation at Union level

1. ENISA shall support operational cooperation among Member States, Union institutions, bodies, offices and agencies, and between stakeholders.

2. ENISA shall cooperate at the operational level and establish synergies with Union institutions, bodies, offices and agencies, including the CERT-EU, with the services dealing with cybercrime and with supervisory authorities dealing with the protection of privacy and personal data, with a view to addressing issues of common concern, including by means of:

(a) the exchange of know-how and best practices;

(b) the provision of advice and issuing of guidelines on relevant matters related to cybersecurity;

(c) the establishment of practical arrangements for the execution of specific tasks, after consulting the Commission.

3. ENISA shall provide the secretariat of the CSIRTs network pursuant to Article 12(2) of Directive (EU) 2016/1148, and in that capacity shall actively support the information sharing and the cooperation among its members.

4. ENISA shall support Member States with respect to operational cooperation within the CSIRTs network by:

(a) advising on how to improve their capabilities to prevent, detect and respond to incidents and, at the request of one or more Member States, providing advice in relation to a specific cyber threat;

(b) assisting, at the request of one or more Member States, in the assessment of incidents having a significant or substantial impact through the provision of expertise and facilitating the technical handling of such incidents including in particular by supporting the voluntary sharing of relevant information and technical solutions between Member States;

(c) analysing vulnerabilities and incidents on the basis of publicly available information or information provided voluntarily by Member States for that purpose; and

(d) at the request of one or more Member States, providing support in relation to *ex-post* technical inquiries regarding incidents having a significant or substantial impact within the meaning of Directive (EU) 2016/1148.

In performing those tasks, ENISA and CERT-EU shall engage in structured cooperation to benefit from synergies and to avoid the duplication of activities.

5. ENISA shall regularly organise cybersecurity exercises at Union level, and shall support Member States and Union institutions, bodies, offices and agencies in organising cybersecurity exercises following their requests. Such cybersecurity exercises at Union level may include technical, operational or strategic elements. On a biennial basis, ENISA shall organise a large-scale comprehensive exercise.

Where appropriate, ENISA shall also contribute to and help organise sectoral cybersecurity exercises together with relevant organisations that also participate in cybersecurity exercises at Union level.

6. ENISA, in close cooperation with the Member States, shall prepare a regular in-depth EU Cybersecurity Technical Situation Report on incidents and cyber threats based on publicly available information, its own analysis, and reports shared by, among others, the Member States' CSIRTs or the single points of contact established by Directive (EU) 2016/1148, both on a voluntary basis, EC3 and CERT-EU.

7. ENISA shall contribute to developing a cooperative response at Union and Member States level to large-scale cross-border incidents or crises related to cybersecurity, mainly by:

(a) aggregating and analysing reports from national sources that are in the public domain or shared on a voluntary basis with a view to contributing to the establishment of common situational awareness;

(b) ensuring the efficient flow of information and the provision of escalation mechanisms between the CSIRTs network and the technical and political decision-makers at Union level;

(c) upon request, facilitating the technical handling of such incidents or crises, including, in particular, by supporting the voluntary sharing of technical solutions between Member States;

(d) supporting Union institutions, bodies, offices and agencies and, at their request, Member States, in the public communication relating to such incidents or crises;

(e) testing the cooperation plans for responding to such incidents or crises at Union level and, at their request, supporting Member States in testing such plans at national level.

Article 8

Market, cybersecurity certification, and standardisation

1. ENISA shall support and promote the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services and ICT processes, as established in Title III of this Regulation, by:

(a) monitoring developments, on an ongoing basis, in related areas of standardisation and recommending appropriate technical specifications for use in the development of European cybersecurity certification schemes pursuant to point (c) of Article 54(1) where standards are not available;

(b) preparing candidate European cybersecurity certification schemes ('candidate schemes') for ICT products, ICT services and ICT processes in accordance with Article 49;

(c) evaluating adopted European cybersecurity certification schemes in accordance with Article 49(8);

(d) participating in peer reviews pursuant to Article 59(4);

(e) assisting the Commission in providing the secretariat of the ECCG pursuant to Article 62(5).

2. ENISA shall provide the secretariat of the Stakeholder Cybersecurity Certification Group pursuant to Article 22(4).

3. ENISA shall compile and publish guidelines and develop good practices, concerning the cybersecurity requirements for ICT products, ICT services and ICT processes, in cooperation with national cybersecurity certification authorities and industry in a formal, structured and transparent way.

4. ENISA shall contribute to capacity-building related to evaluation and certification processes by compiling and issuing guidelines as well as by providing support to Member States at their request.

5. ENISA shall facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT products, ICT services and ICT processes.

6. ENISA shall draw up, in collaboration with Member States and industry, advice and guidelines regarding the technical areas related to the security requirements for operators of essential services and digital service providers, as well as regarding already existing standards, including Member States' national standards, pursuant to Article 19(2) of Directive (EU) 2016/1148.

7. ENISA shall perform and disseminate regular analyses of the main trends in the cybersecurity market on both the demand and supply sides, with a view to fostering the cybersecurity market in the Union.

Article 9

Knowledge and information

ENISA shall:

(a) perform analyses of emerging technologies and provide topic-specific assessments on the expected societal, legal, economic and regulatory impact of technological innovations on cybersecurity;

(b) perform long-term strategic analyses of cyber threats and incidents in order to identify emerging trends and help prevent incidents;

(c) in cooperation with experts from Member States authorities and relevant stakeholders, provide advice, guidance and best practices for the security of network and information systems, in particular for the security of the infrastructures supporting the sectors listed in Annex II to Directive (EU) 2016/1148 and those used by the providers of the digital services listed in Annex III to that Directive;

(d) through a dedicated portal, pool, organise and make available to the public information on cybersecurity provided by the Union institutions, bodies, offices and agencies and information on cybersecurity provided on a voluntary basis by Member States and private and public stakeholders;

(e) collect and analyse publicly available information regarding significant incidents and compile reports with a view to providing guidance to citizens, organisations and businesses across the Union.

Article 10

Awareness-raising and education

ENISA shall:

(a) raise public awareness of cybersecurity risks, and provide guidance on good practices for individual users aimed at citizens, organisations and businesses, including cyber-hygiene and cyber-literacy;

(b) in cooperation with the Member States, Union institutions, bodies, offices and agencies and industry, organise regular outreach campaigns to increase cybersecurity and its visibility in the Union and encourage a broad public debate;

(c) assist Member States in their efforts to raise cybersecurity awareness and promote cybersecurity education;

(d) support closer coordination and exchange of best practices among Member States on cybersecurity awareness and education.

Article 11

Research and innovation

In relation to research and innovation, ENISA shall:

(a) advise the Union institutions, bodies, offices and agencies and the Member States on research needs and priorities in the field of cybersecurity, with a view to enabling effective responses to current and emerging risks and cyber threats, including with respect to new and emerging information and communications technologies, and with a view to using risk-prevention technologies effectively;

(b) where the Commission has conferred the relevant powers on it, participate in the implementation phase of research and innovation funding programmes or as a beneficiary;

(c) contribute to the strategic research and innovation agenda at Union level in the field of cybersecurity.

Article 12

International cooperation

ENISA shall contribute to the Union's efforts to cooperate with third countries and international organisations as well as within relevant international cooperation frameworks to promote international cooperation on issues related to cybersecurity, by:

(a) where appropriate, engaging as an observer in the organisation of international exercises, and analysing and reporting to the Management Board on the outcome of such exercises;

(b) at the request of the Commission, facilitating the exchange of best practices;

(c) at the request of the Commission, providing it with expertise;

(d) providing advice and support to the Commission on matters concerning agreements for the mutual recognition of cybersecurity certificates with third countries, in collaboration with the ECCG established under Article 62.

CHAPTER III

Organisation of ENISA

Article 13

Structure of ENISA

The administrative and management structure of ENISA shall be composed of the following:

(a) a Management Board;

(b) an Executive Board;

(c) an Executive Director;

(d) an ENISA Advisory Group;

(e) a National Liaison Officers Network.

Section 1

Management Board

Article 14

Composition of the Management Board

1. The Management Board shall be composed of one member appointed by each Member State, and two members appointed by the Commission. All members shall have the right to vote.

2. Each member of the Management Board shall have an alternate. That alternate shall represent the member in the member's absence.

3. Members of the Management Board and their alternates shall be appointed on the basis of their knowledge in the field of cybersecurity, taking into account their relevant managerial, administrative and budgetary skills. The Commission and the Member States shall make efforts to limit the turnover of their representatives on the Management Board, in order to ensure continuity of the Management Board's work. The Commission and the Member States shall aim to achieve gender balance on the Management Board.

4. The term of office of the members of the Management Board and their alternates shall be four years. That term shall be renewable.

Article 15

Functions of the Management Board

1. The Management Board shall:

(a) establish the general direction of the operation of ENISA and ensure that ENISA operates in accordance with the rules and principles laid down in this Regulation; it shall also ensure the consistency of ENISA's work with activities conducted by the Member States as well as at Union level;

(b) adopt ENISA's draft single programming document referred to in Article 24, before its submission to the Commission for an opinion;

(c) adopt ENISA's single programming document, taking into account the Commission opinion;

(d) supervise the implementation of the multiannual and annual programming included in the single programming document;

(e) adopt the annual budget of ENISA and exercise other functions in respect of ENISA's budget in accordance with Chapter IV;

(f) assess and adopt the consolidated annual report on ENISA's activities, including the accounts and a description of how ENISA has met its performance indicators, submit both the annual report and the assessment thereof by 1 July of the following year, to the European Parliament, to the Council, to the Commission and to the Court of Auditors, and make the annual report public;

(g) adopt the financial rules applicable to ENISA in accordance with Article 32;

(h) adopt an anti-fraud strategy that is proportionate to the fraud risks, having regard to a cost-benefit analysis of the measures to be implemented;

(i) adopt rules for the prevention and management of conflicts of interest in respect of its members;

(j) ensure adequate follow-up to the findings and recommendations resulting from investigations of the European Anti-Fraud Office (OLAF) and the various internal or external audit reports and evaluations;

(k) adopt its rules of procedure, including rules for provisional decisions on the delegation of specific tasks, pursuant to Article 19(7);

(l) with respect to the staff of ENISA, exercise the powers conferred by the Staff Regulations of Officials (the 'Staff Regulations of Officials') and the Conditions of Employment of Other Servants of the European Union (the 'Conditions of Employment of Other Servants'), laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68 ([24]) on the appointing authority and on the Authority Empowered to Conclude a Contract of Employment ('appointing authority powers') in accordance with paragraph 2 of this Article;

(m) adopt rules implementing the Staff Regulations of Officials and the Conditions of Employment of Other Servants in accordance with the procedure provided for in Article 110 of the Staff Regulations of Officials;

(n) appoint the Executive Director and where relevant extend his or her term of office or remove him or her from office in accordance with Article 36;

(o) appoint an accounting officer, who may be the Commission's accounting officer, who shall be wholly independent in the performance of his or her duties;

(p) take all decisions concerning the establishment of ENISA's internal structures and, where necessary, the modification of those internal structures, taking into consideration ENISA's activity needs and having regard to sound budgetary management;

(q) authorise the establishment of working arrangements with regard to Article 7;

(r) authorise the establishment or conclusion of working arrangements in accordance with Article 42.

2. In accordance with Article 110 of the Staff Regulations of Officials, the Management Board shall adopt a decision based on Article 2(1) of the Staff Regulations of Officials and Article 6 of the Conditions of Employment of Other Servants, delegating the relevant appointing authority powers to the Executive Director and determining the conditions under which that delegation of powers can be suspended. The Executive Director may sub-delegate those powers.

([24]) OJ L 56, 4.3.1968, p. 1.

3. Where exceptional circumstances so require, the Management Board may adopt a decision to temporarily suspend the delegation of appointing authority powers to the Executive Director and any appointing authority powers sub-delegated by the Executive Director and instead exercise them itself or delegate them to one of its members or to a staff member other than the Executive Director.

Article 16

Chairperson of the Management Board

The Management Board shall elect a Chairperson and a Deputy Chairperson from among its members, by a majority of two thirds of the members. Their terms of office shall be four years, which shall be renewable once. If, however, their membership of the Management Board ends at any time during their term of office, their term of office shall automatically expire on that date. The Deputy Chair shall replace the Chairperson *ex officio* if the Chairperson is unable to attend to his or her duties.

Article 17

Meetings of the Management Board

1. Meetings of the Management Board shall be convened by its Chairperson.

2. The Management Board shall hold at least two ordinary meetings a year. It shall also hold extraordinary meetings at the request of its Chairperson, at the request of the Commission, or at the request of at least one third of its members.

3. The Executive Director shall take part in the meetings of the Management Board but shall not have the right to vote.

4. Members of the ENISA Advisory Group may take part in the meetings of the Management Board at the invitation of the Chairperson, but shall not have the right to vote.

5. The members of the Management Board and their alternates may be assisted at the meetings of the Management Board by advisers or experts, subject to the rules of procedure of the Management Board.

6. ENISA shall provide the secretariat of the Management Board.

Article 18

Voting rules of the Management Board

1. The Management Board shall take its decisions by a majority of its members.

2. A majority of two-thirds of the members of the Management Board shall be required for the adoption of the single programming document and of the annual budget and for the appointment, extension of the term of office or removal of the Executive Director.

3. Each member shall have one vote. In the absence of a member, their alternate shall be entitled to exercise the member's right to vote.

4. The Chairperson of the Management Board shall take part in the voting.

5. The Executive Director shall not take part in the voting.

6. The Management Board's rules of procedure shall establish more detailed voting arrangements, in particular the circumstances in which a member may act on behalf of another member.

Section 2

Executive Board

Article 19

Executive Board

1. The Management Board shall be assisted by an Executive Board.

2. The Executive Board shall:

(a) prepare decisions to be adopted by the Management Board;

(b) together with the Management Board, ensure the adequate follow-up to the findings and recommendations stemming from investigations of OLAF and the various internal or external audit reports and evaluations;

(c) without prejudice to the responsibilities of the Executive Director set out in Article 20, assist and advise the Executive Director in implementing the decisions of the Management Board on administrative and budgetary matters pursuant to Article 20.

3. The Executive Board shall be composed of five members. The members of the Executive Board shall be appointed from among the members of the Management Board. One of the members shall be the Chairperson of the Management Board, who may also chair the Executive Board, and another shall be one of the representatives of the Commission. The appointments of the members of the Executive Board shall aim to ensure gender balance on the Executive Board. The Executive Director shall take part in the meetings of the Executive Board but shall not have the right to vote.

4. The term of office of the members of the Executive Board shall be four years. That term shall be renewable.

5. The Executive Board shall meet at least once every three months. The Chairperson of the Executive Board shall convene additional meetings at the request of its members.

6. The Management Board shall lay down the rules of procedure of the Executive Board.

7. When necessary because of urgency, the Executive Board may take certain provisional decisions on behalf of the Management Board, in particular on administrative management matters, including the suspension of the delegation of the appointing authority powers and budgetary matters. Any such provisional decisions shall be notified to the Management Board without undue delay. The Management Board shall then decide whether to approve or reject the provisional decision no later than three months after the decision was taken. The Executive Board shall not take decisions on behalf of the Management Board that require the approval of a majority of two-thirds of the members of the Management Board.

Section 3

Executive Director

Article 20

Duties of the Executive Director

1. ENISA shall be managed by its Executive Director, who shall be independent in the performance of his or her duties. The Executive Director shall be accountable to the Management Board.

2. The Executive Director shall report to the European Parliament on the performance of his or her duties when invited to do so. The Council may invite the Executive Director to report on the performance of his or her duties.

3. The Executive Director shall be responsible for:

(a) the day-to-day administration of ENISA;

(b) implementing the decisions adopted by the Management Board;

(c) preparing the draft single programming document and submitting it to the Management Board for approval before its submission to the Commission;

(d) implementing the single programming document and reporting to the Management Board thereon;

(e) preparing the consolidated annual report on ENISA's activities, including the implementation of ENISA's annual work programme, and presenting it to the Management Board for assessment and adoption;

(f) preparing an action plan that follows up on the conclusions of the retrospective evaluations, and reporting on progress every two years to the Commission;

(g) preparing an action plan that follows up on the conclusions of internal or external audit reports, as well as on investigations by OLAF and reporting on progress biannually to the Commission and regularly to the Management Board;

(h) preparing the draft financial rules applicable to ENISA as referred to in Article 32;

(i) preparing ENISA's draft statement of estimates of revenue and expenditure and implementing its budget;

(j) protecting the financial interests of the Union by the application of preventive measures against fraud, corruption and any other illegal activities, by effective checks and, if irregularities are detected, by the recovery of the amounts wrongly paid and, where appropriate, by effective, proportionate and dissuasive administrative and financial penalties;

(k) preparing an anti-fraud strategy for ENISA and presenting it to the Management Board for approval;

(l) developing and maintaining contact with the business community and consumers' organisations to ensure regular dialogue with relevant stakeholders;

(m) exchanging views and information regularly with Union institutions, bodies, offices and agencies regarding their activities relating to cybersecurity to ensure coherence in the development and the implementation of Union policy;

(n) carrying out other tasks assigned to the Executive Director by this Regulation.

4. Where necessary and within ENISA's objectives and tasks, the Executive Director may set up ad hoc working groups composed of experts, including experts from the Member States' competent authorities. The Executive Director shall inform the Management Board in advance thereof. The procedures regarding in particular the composition of the working groups, the appointment of the experts of the working groups by the Executive Director and the operation of the working groups shall be specified in ENISA's internal rules of operation.

5. Where necessary, for the purpose of carrying out ENISA's tasks in an efficient and effective manner and based on an appropriate cost-benefit analysis, the Executive Director may decide to establish one or more local offices in one or more Member States. Before deciding to establish a local office, the Executive Director shall seek the opinion of the Member States concerned, including the Member State in which the seat of ENISA is located, and shall obtain the prior consent of the Commission and the Management Board. In cases of disagreement during the consultation process between the Executive Director and the Member States concerned, the issue shall be brought to the Council for discussion. The aggregate number of staff in all local offices shall be kept to a minimum and shall not exceed 40 % of the total number of ENISA's staff located in the Member State in which the seat of ENISA is located. The number of the staff in each local office shall not exceed 10 % of the total number of ENISA's staff located in the Member State in which the seat of ENISA is located.

The decision establishing a local office shall specify the scope of the activities to be carried out at the local office in a manner that avoids unnecessary costs and duplication of administrative functions of ENISA.

Section 4

ENISA Advisory Group, Stakeholder Cybersecurity Certification Group and National Liaison Officers Network

Article 21

ENISA Advisory Group

1. The Management Board, acting on a proposal from the Executive Director, shall establish in a transparent manner the ENISA Advisory Group composed of recognised experts representing the relevant stakeholders, such as the ICT industry, providers of electronic communications networks or services available to the public, SMEs, operators of essential services, consumer groups, academic experts in the field of cybersecurity, and representatives of competent authorities notified in accordance with Directive (EU) 2018/1972, of European standardisation organisations, as well as of law enforcement and data protection supervisory authorities. The Management Board shall aim to ensure an appropriate gender and geographical balance as well as a balance between the different stakeholder groups.

2. Procedures for the ENISA Advisory Group, in particular regarding its composition, the proposal by the Executive Director referred to in paragraph 1, the number and appointment of its members and the operation of the ENISA Advisory Group, shall be specified in ENISA's internal rules of operation and shall be made public.

3. The ENISA Advisory Group shall be chaired by the Executive Director or by any person whom the Executive Director appoints on a case-by-case basis.

4. The term of office of the members of the ENISA Advisory Group shall be two-and-a-half years. Members of the Management Board shall not be members of the ENISA Advisory Group. Experts from the Commission and the Member States shall be entitled to be present at the meetings of the ENISA Advisory Group and to participate in its work. Representatives of other bodies deemed to be relevant by the Executive Director, who are not members of the ENISA Advisory Group, may be invited to attend the meetings of the ENISA Advisory Group and to participate in its work.

5. The ENISA Advisory Group shall advise ENISA in respect of the performance of ENISA's tasks, except of the application of the provisions of Title III of this Regulation. It shall in particular advise the Executive Director on the drawing up of a proposal for ENISA's annual work programme, and on ensuring communication with the relevant stakeholders on issues related to the annual work programme.

6. The ENISA Advisory Group shall inform the Management Board of its activities on a regular basis.

Article 22

Stakeholder Cybersecurity Certification Group

1. The Stakeholder Cybersecurity Certification Group shall be established.

2. The Stakeholder Cybersecurity Certification Group shall be composed of members selected from among recognised experts representing the relevant stakeholders. The Commission, following a transparent and open call, shall select, on the basis of a proposal from ENISA, members of the Stakeholder Cybersecurity Certification Group ensuring a balance between the different stakeholder groups as well as an appropriate gender and geographical balance.

3. The Stakeholder Cybersecurity Certification Group shall:

(a) advise the Commission on strategic issues regarding the European cybersecurity certification framework;

(b) upon request, advise ENISA on general and strategic matters concerning ENISA's tasks relating to market, cybersecurity certification, and standardisation;

(c) assist the Commission in the preparation of the Union rolling work programme referred to in Article 47;

(d) issue an opinion on the Union rolling work programme pursuant to Article 47(4); and

(e) in urgent cases, provide advice to the Commission and the ECCG on the need for additional certification schemes not included in the Union rolling work programme, as outlined in Articles 47 and 48.

4. The Stakeholder Certification Group shall be co-chaired by the representatives of the Commission and of ENISA, and its secretariat shall be provided by ENISA.

Article 23

National Liaison Officers Network

1. The Management Board, acting on a proposal from the Executive Director, shall set up a National Liaison Officers Network composed of representatives of all Member States (National Liaison Officers). Each Member State shall appoint one representative to the National Liaison Officers Network. The meetings of the National Liaison Officers Network may be held in different expert formations.

2. The National Liaison Officers Network shall in particular facilitate the exchange of information between ENISA and the Member States, and shall support ENISA in disseminating its activities, findings and recommendations to the relevant stakeholders across the Union.

3. National Liaison Officers shall act as a point of contact at national level to facilitate cooperation between ENISA and national experts in the context of the implementation of ENISA's annual work programme.

4. While National Liaison Officers shall cooperate closely with the Management Board representatives of their respective Member States, the National Liaisons Officers Network itself shall not duplicate the work of the Management Board or of other Union forums.

5. The functions and procedures of the National Liaisons Officers Network shall be specified in ENISA's internal rules of operation and shall be made public.

Section 5

Operation

Article 24

Single programming document

1. ENISA shall operate in accordance with a single programming document containing its annual and multiannual programming, which shall include all of its planned activities.

2. Each year, the Executive Director shall draw up a draft single programming document containing its annual and multiannual programming with the corresponding financial and human resources planning in accordance with Article 32 of Commission Delegated Regulation (EU) No 1271/2013 ([25]) and taking into account the guidelines set by the Commission.

3. By 30 November each year, the Management Board shall adopt the single programming document referred to in paragraph 1 and shall transmit it to the European Parliament, to the Council and to the Commission by 31 January of the following year, as well as any subsequently updated versions of that document.

4. The single programming document shall become final after the definitive adoption of the general budget of the Union and shall be adjusted as necessary.

([25]) Commission Delegated Regulation (EU) No 1271/2013 of 30 September 2013 on the framework financial regulation for the bodies referred to in Article 208 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council (OJ L 328, 7.12.2013, p. 42).

5. The annual work programme shall comprise detailed objectives and expected results including performance indicators. It shall also contain a description of the actions to be financed and an indication of the financial and human resources allocated to each action, in accordance with the principles of activity-based budgeting and management. The annual work programme shall be coherent with the multiannual work programme referred to in paragraph 7. It shall clearly indicate tasks that have been added, changed or deleted in comparison with the previous financial year.

6. The Management Board shall amend the adopted annual work programme when a new task is assigned to ENISA. Any substantial amendments to the annual work programme shall be adopted by the same procedure as for the initial annual work programme. The Management Board may delegate the power to make non-substantial amendments to the annual work programme to the Executive Director.

7. The multiannual work programme shall set out the overall strategic programming including objectives, expected results and performance indicators. It shall also set out the resource programming including multi-annual budget and staff.

8. The resource programming shall be updated annually. The strategic programming shall be updated where appropriate and in particular where necessary to address the outcome of the evaluation referred to in Article 67.

Article 25

Declaration of interests

1. Members of the Management Board, the Executive Director, and officials seconded by Member States on a temporary basis, shall each make a declaration of commitments and a declaration indicating the absence or presence of any direct or indirect interest which might be considered to be prejudicial to their independence. The declarations shall be accurate and complete, shall be made annually in writing, and shall be updated whenever necessary.

2. Members of the Management Board, the Executive Director, and external experts participating in ad hoc working groups, shall each accurately and completely declare, at the latest at the start of each meeting, any interest which might be considered to be prejudicial to their independence in relation to the items on the agenda, and shall abstain from participating in the discussion of and voting on such items.

3. ENISA shall lay down, in its internal rules of operation, the practical arrangements for the rules on declarations of interest referred to in paragraphs 1 and 2.

Article 26

Transparency

1. ENISA shall carry out its activities with a high level of transparency and in accordance with Article 28.

2. ENISA shall ensure that the public and any interested parties are provided with appropriate, objective, reliable and easily accessible information, in particular with regard to the results of its work. It shall also make public the declarations of interest made in accordance with Article 25.

3. The Management Board, acting on a proposal from the Executive Director, may authorise interested parties to observe the proceedings of some of ENISA's activities.

4. ENISA shall lay down, in its internal rules of operation, the practical arrangements for implementing the transparency rules referred to in paragraphs 1 and 2.

Article 27

Confidentiality

1. Without prejudice to Article 28, ENISA shall not divulge to third parties information that it processes or receives in relation to which a reasoned request for confidential treatment has been made.

2. Members of the Management Board, the Executive Director, the members of the ENISA Advisory Group, external experts participating in ad hoc working groups, and members of the staff of ENISA, including officials seconded by Member States on a temporary basis, shall comply with the confidentiality requirements of Article 339 TFEU, even after their duties have ceased.

3. ENISA shall lay down, in its internal rules of operation, the practical arrangements for implementing the confidentiality rules referred to in paragraphs 1 and 2.

4. If required for the performance of ENISA's tasks, the Management Board shall decide to allow ENISA to handle classified information. In that case ENISA, in agreement with the Commission services, shall adopt security rules applying the security principles set out in Commission Decisions (EU, Euratom) 2015/443 ([26]) and 2015/444 ([27]). Those security rules shall include provisions for the exchange, processing and storage of classified information.

Article 28

Access to documents

1. Regulation (EC) No 1049/2001 shall apply to documents held by ENISA.

2. The Management Board shall adopt arrangements for implementing Regulation (EC) No 1049/2001 by 28 December 2019.

3. Decisions taken by ENISA pursuant to Article 8 of Regulation (EC) No 1049/2001 may be the subject of a complaint to the European Ombudsman under Article 228 TFEU or of an action before the Court of Justice of the European Union under Article 263 TFEU.

CHAPTER IV

Establishment and structure of ENISA's budget

Article 29

Establishment of ENISA's budget

1. Each year, the Executive Director shall draw up a draft statement of estimates of ENISA's revenue and expenditure for the following financial year, and shall transmit it to the Management Board, together with a draft establishment plan. Revenue and expenditure shall be in balance.

2. Each year the Management Board, on the basis of the draft statement of estimates, shall produce a statement of estimates of ENISA's revenue and expenditure for the following financial year.

3. The Management Board, by 31 January each year, shall send the statement of estimates, which shall be part of the draft single programming document, to the Commission and the third countries with which the Union has concluded agreements as referred to in Article 42(2).

4. On the basis of the statement of estimates, the Commission shall enter in the draft general budget of the Union the estimates it deems to be necessary for the establishment plan and the amount of the contribution to be charged to the general budget of the Union, which it shall submit to the European Parliament and to the Council in accordance with Article 314 TFEU.

5. The European Parliament and the Council shall authorise the appropriations for the contribution from the Union to ENISA.

6. The European Parliament and the Council shall adopt ENISA's establishment plan.

([26]) Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41).
([27]) 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).

7. The Management Board shall adopt ENISA's budget together with the single programming document. ENISA's budget shall become final following the definitive adoption of the general budget of the Union. Where necessary, the Management Board shall adjust ENISA's budget and single programming document in accordance with the general budget of the Union.

Article 30

Structure of ENISA's budget

1. Without prejudice to other resources, ENISA's revenue shall be composed of:

(a) a contribution from the general budget of the Union;

(b) revenue assigned to specific items of expenditure in accordance with its financial rules referred to in Article 32;

(c) Union funding in the form of delegation agreements or ad hoc grants in accordance with its financial rules referred to in Article 32 and with the provisions of the relevant instruments supporting the policies of the Union;

(d) contributions from third countries participating in the work of ENISA as referred to in Article 42;

(e) any voluntary contributions from Member States in money or in kind.

Member States that provide voluntary contributions under point (e) of the first subparagraph shall not claim any specific right or service as a result thereof.

2. The expenditure of ENISA shall include staff, administrative and technical support, infrastructure and operational expenses, and expenses resulting from contracts with third parties.

Article 31

Implementation of ENISA's budget

1. The Executive Director shall be responsible for the implementation of ENISA's budget.

2. The Commission's internal auditor shall exercise the same powers over ENISA as over Commission departments.

3. ENISA's accounting officer shall send the provisional accounts for the financial year (year N) to the Commission's accounting officer and to the Court of Auditors by 1 March of the following financial year (year N + 1).

4. Upon the receipt of the Court of Auditors' observations on ENISA's provisional accounts pursuant to Article 246 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council ([28]), ENISA's accounting officer shall draw up ENISA's final accounts under his or her responsibility and shall submit them to the Management Board for an opinion.

5. The Management Board shall deliver an opinion on ENISA's final accounts.

6. By 31 March of year N + 1, the Executive Director shall transmit the report on the budgetary and financial management to the European Parliament, to the Council, to the Commission and to the Court of Auditors.

7. By 1 July of year N + 1, ENISA's accounting officer shall transmit ENISA's final accounts to the European Parliament, to the Council, to the Commission's accounting officer and to the Court of Auditors, together with the Management Board's opinion.

([28]) 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 (OJ L 193, 30.7.2018, p. 1).

8. At the same date as the transmission of ENISA's final accounts, ENISA's accounting officer shall also send to the Court of Auditors a representation letter covering those final accounts, with a copy to the Commission's accounting officer.

9. By 15 November of year N + 1, the Executive Director shall publish ENISA's final accounts in the *Official Journal of the European Union*.

10. By 30 September of year N + 1, the Executive Director shall send the Court of Auditors a reply to its observations and shall also send a copy of that reply to the Management Board and to the Commission.

11. The Executive Director shall submit to the European Parliament, at the latter's request, any information required for the smooth application of the discharge procedure for the financial year concerned in accordance with Article 261(3) of Regulation (EU, Euratom) 2018/1046.

12. On a recommendation from the Council, the European Parliament shall, before 15 May of year N + 2, give a discharge to the Executive Director in respect of the implementation of the budget for the year N.

Article 32

Financial rules

The financial rules applicable to ENISA shall be adopted by the Management Board after consulting the Commission. They shall not depart from Delegated Regulation (EU) No 1271/2013 unless such a departure is specifically required for the operation of ENISA and the Commission has given its prior consent.

Article 33

Combating fraud

1. In order to facilitate the combating of fraud, corruption and other unlawful activities under Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council ([29]), ENISA shall by 28 December 2019, accede to the Interinstitutional Agreement of 25 May 1999 between the European Parliament, the Council of the European Union and the Commission of the European Communities concerning internal investigations by the European Anti-Fraud Office (OLAF) ([30]). ENISA shall adopt appropriate provisions applicable to all employees of ENISA, using the template set out in the Annex to that Agreement.

2. The Court of Auditors shall have the power of audit, on the basis of documents and of on-the-spot inspections, over all grant beneficiaries, contractors and subcontractors who have received Union funds from ENISA.

3. OLAF may carry out investigations, including on-the-spot checks and inspections, in accordance with the provisions and procedures laid down in Regulation (EU, Euratom) No 883/2013 and Council Regulation (Euratom, EC) No 2185/96 ([31]), with a view to establishing whether there has been fraud, corruption or any other illegal activity affecting the financial interests of the Union in connection with a grant or a contract funded by ENISA.

4. Without prejudice to paragraphs 1, 2 and 3, cooperation agreements with third countries or international organisations, contracts, grant agreements and grant decisions of ENISA shall contain provisions expressly empowering the Court of Auditors and OLAF to conduct such audits and investigations, according to their respective competences.

([29]) Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 (OJ L 248, 18.9.2013, p. 1).

([30]) OJ L 136, 31.5.1999, p. 15.

([31]) Council Regulation (Euratom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities (OJ L 292, 15.11.1996, p. 2).

CHAPTER V

Staff

Article 34

General provisions

The Staff Regulations of Officials and the Conditions of Employment of Other Servants, as well as the rules adopted by agreement between the Union institutions for giving effect to the Staff Regulations of Officials and the Conditions of Employment of Other Servants shall apply to the staff of ENISA.

Article 35

Privileges and immunity

Protocol No 7 on the privileges and immunities of the European Union, annexed to the TEU and to the TFEU, shall apply to ENISA and its staff.

Article 36

Executive Director

1. The Executive Director shall be engaged as a temporary agent of ENISA under point (a) of Article 2 of the Conditions of Employment of Other Servants.

2. The Executive Director shall be appointed by the Management Board from a list of candidates proposed by the Commission, following an open and transparent selection procedure.

3. For the purpose of concluding the employment contract with the Executive Director, ENISA shall be represented by the Chairperson of the Management Board.

4. Before appointment, the candidate selected by the Management Board shall be invited to make a statement before the relevant committee of the European Parliament and to answer Members' questions.

5. The term of office of the Executive Director shall be five years. By the end of that period, the Commission shall carry out an assessment of the performance of the Executive Director and ENISA's future tasks and challenges.

6. The Management Board shall reach decisions on appointment, extension of the term of office or removal from office of the Executive Director in accordance with Article 18(2).

7. The Management Board, acting on a proposal from the Commission which takes into account the assessment referred to in paragraph 5, may extend the term of office of the Executive Director once by five years.

8. The Management Board shall inform the European Parliament about its intention to extend the Executive Director's term of office. Within three months before any such extension, the Executive Director, if invited, shall make a statement before the relevant committee of the European Parliament and answer Members' questions.

9. An Executive Director whose term of office has been extended shall not participate in another selection procedure for the same post.

10. The Executive Director may be removed from office only by decision of the Management Board acting on a proposal from the Commission.

Article 37

Seconded national experts and other staff

1. ENISA may make use of seconded national experts or other staff not employed by ENISA. The Staff Regulations of Officials and the Conditions of Employment of Other Servants shall not apply to such staff.

2. The Management Board shall adopt a decision laying down rules on the secondment of national experts to ENISA.

CHAPTER VI

General provisions concerning ENISA

Article 38

Legal status of ENISA

1. ENISA shall be a body of the Union and shall have legal personality.

2. In each Member State ENISA shall enjoy the most extensive legal capacity accorded to legal persons under national law. It may, in particular, acquire or dispose of movable and immovable property and be a party to legal proceedings.

3. ENISA shall be represented by the Executive Director.

Article 39

Liability of ENISA

1. The contractual liability of ENISA shall be governed by the law applicable to the contract in question.

2. The Court of Justice of the European Union shall have jurisdiction to give judgment pursuant to any arbitration clause contained in a contract concluded by ENISA.

3. In the case of non-contractual liability, ENISA shall make good any damage caused by it or its staff in the performance of their duties, in accordance with the general principles common to the laws of the Member States.

4. The Court of Justice of the European Union shall have jurisdiction in any dispute over compensation for damage as referred to in paragraph 3.

5. The personal liability of ENISA's staff towards ENISA shall be governed by the relevant conditions applying to ENISA's staff.

Article 40

Language arrangements

1. Council Regulation No 1 ([32]) shall apply to ENISA. The Member States and the other bodies appointed by the Member States may address ENISA and receive a reply in the official language of the institutions of the Union that they choose.

2. The translation services required for the functioning of ENISA shall be provided by the Translation Centre for the Bodies of the European Union.

Article 41

Protection of personal data

1. The processing of personal data by ENISA shall be subject to Regulation (EU) 2018/1725.

2. The Management Board shall adopt implementing rules as referred to in Article 45(3) of Regulation (EU) 2018/1725. The Management Board may adopt additional measures necessary for the application of Regulation (EU) 2018/1725 by ENISA.

([32]) Council Regulation No 1 determining the languages to be used by the European Economic Community (OJ 17, 6.10.1958, p. 385/58).

Article 42

Cooperation with third countries and international organisations

1. To the extent necessary in order to achieve the objectives set out in this Regulation, ENISA may cooperate with the competent authorities of third countries or with international organisations or both. To that end, ENISA may establish working arrangements with the authorities of third countries and international organisations, subject to the prior approval of the Commission. Those working arrangements shall not create legal obligations incumbent on the Union and its Member States.

2. ENISA shall be open to the participation of third countries that have concluded agreements with the Union to that effect. Under the relevant provisions of such agreements, working arrangements shall be established specifying in particular the nature, extent and manner in which those third countries are to participate in ENISA's work, and shall include provisions relating to participation in the initiatives undertaken by ENISA, to financial contributions and to staff. As regards staff matters, those working arrangements shall comply with the Staff Regulations of Officials and Conditions of Employment of Other Servants in any event.

3. The Management Board shall adopt a strategy for relations with third countries and international organisations concerning matters for which ENISA is competent. The Commission shall ensure that ENISA operates within its mandate and the existing institutional framework by concluding appropriate working arrangements with the Executive Director.

Article 43

Security rules on the protection of sensitive non-classified information and classified information

After consulting the Commission, ENISA shall adopt security rules applying the security principles contained in the Commission's security rules for protecting sensitive non-classified information and EUCI, as set out in Decisions (EU, Euratom) 2015/443 and 2015/444. ENISA's security rules shall include provisions for the exchange, processing and storage of such information.

Article 44

Headquarters Agreement and operating conditions

1. The necessary arrangements concerning the accommodation to be provided for ENISA in the host Member State and the facilities to be made available by that Member State together with the specific rules applicable in the host Member State to the Executive Director, members of the Management Board, ENISA's staff and members of their families shall be laid down in a headquarters agreement between ENISA and the host Member State, concluded after obtaining the approval of the Management Board.

2. ENISA's host Member State shall provide the best possible conditions for ensuring the proper functioning of ENISA, taking into account the accessibility of the location, the existence of adequate education facilities for the children of staff members, appropriate access to the labour market, social security and medical care for both children and spouses of staff members.

Article 45

Administrative control

The operations of ENISA shall be supervised by the European Ombudsman in accordance with Article 228 TFEU.

TITLE III

CYBERSECURITY CERTIFICATION FRAMEWORK

Article 46

European cybersecurity certification framework

1. The European cybersecurity certification framework shall be established in order to improve the conditions for the functioning of the internal market by increasing the level of cybersecurity within the Union and enabling a harmonised approach at Union level to European cybersecurity certification schemes, with a view to creating a digital single market for ICT products, ICT services and ICT processes.

2. The European cybersecurity certification framework shall provide for a mechanism to establish European cybersecurity certification schemes and to attest that the ICT products, ICT services and ICT processes that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, services and processes throughout their life cycle.

Article 47

The Union rolling work programme for European cybersecurity certification

1. The Commission shall publish a Union rolling work programme for European cybersecurity certification (the 'Union rolling work programme') that shall identify strategic priorities for future European cybersecurity certification schemes.

2. The Union rolling work programme shall in particular include a list of ICT products, ICT services and ICT processes or categories thereof that are capable of benefiting from being included in the scope of a European cybersecurity certification scheme.

3. Inclusion of specific ICT products, ICT services and ICT processes or categories thereof in the Union rolling work programme shall be justified on the basis of one or more of the following grounds:

(a) the availability and the development of national cybersecurity certification schemes covering a specific category of ICT products, ICT services or ICT processes and, in particular, as regards the risk of fragmentation;

(b) relevant Union or Member State law or policy;

(c) market demand;

(d) developments in the cyber threat landscape;

(e) request for the preparation of a specific candidate scheme by the ECCG.

4. The Commission shall take due account of the opinions issued by the ECCG and the Stakeholder Certification Group on the draft Union rolling work programme.

5. The first Union rolling work programme shall be published by 28 June 2020. The Union rolling work programme shall be updated at least once every three years and more often if necessary.

Article 48

Request for a European cybersecurity certification scheme

1. The Commission may request ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme on the basis of the Union rolling work programme.

2. In duly justified cases, the Commission or the ECCG may request ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme which is not included in the Union rolling work programme. The Union rolling work programme shall be updated accordingly.

Article 49

Preparation, adoption and review of a European cybersecurity certification scheme

1. Following a request from the Commission pursuant to Article 48, ENISA shall prepare a candidate scheme which meets the requirements set out in Articles 51, 52 and 54.

2. Following a request from the ECCG pursuant to Article 48(2), ENISA may prepare a candidate scheme which meets the requirements set out in Articles 51, 52 and 54. If ENISA refuses such a request, it shall give reasons for its refusal. Any decision to refuse such a request shall be taken by the Management Board.

3. When preparing a candidate scheme, ENISA shall consult all relevant stakeholders by means of a formal, open, transparent and inclusive consultation process.

4. For each candidate scheme, ENISA shall establish an ad hoc working group in accordance with Article 20(4) for the purpose of providing ENISA with specific advice and expertise.

5. ENISA shall closely cooperate with the ECCG. The ECCG shall provide ENISA with assistance and expert advice in relation to the preparation of the candidate scheme and shall adopt an opinion on the candidate scheme.

6. ENISA shall take utmost account of the opinion of the ECCG before transmitting the candidate scheme prepared in accordance with paragraphs 3, 4 and 5 to the Commission. The opinion of the ECCG shall not bind ENISA, nor shall the absence of such an opinion prevent ENISA from transmitting the candidate scheme to the Commission.

7. The Commission, based on the candidate scheme prepared by ENISA, may adopt implementing acts providing for a European cybersecurity certification scheme for ICT products, ICT services and ICT processes which meets the requirements set out in Articles 51, 52 and 54. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 66(2).

8. At least every five years, ENISA shall evaluate each adopted European cybersecurity certification scheme, taking into account the feedback received from interested parties. If necessary, the Commission or the ECCG may request ENISA to start the process of developing a revised candidate scheme in accordance with Article 48 and this Article.

Article 50

Website on European cybersecurity certification schemes

1. ENISA shall maintain a dedicated website providing information on, and publicising, European cybersecurity certification schemes, European cybersecurity certificates and EU statements of conformity, including information with regard to European cybersecurity certification schemes which are no longer valid, to withdrawn and expired European cybersecurity certificates and EU statements of conformity, and to the repository of links to cybersecurity information provided in accordance with Article 55.

2. Where applicable, the website referred to in paragraph 1 shall also indicate the national cybersecurity certification schemes that have been replaced by a European cybersecurity certification scheme.

Article 51

Security objectives of European cybersecurity certification schemes

A European cybersecurity certification scheme shall be designed to achieve, as applicable, at least the following security objectives:

(a) to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process;

(b) to protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process;

(c) that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;

(d) to identify and document known dependencies and vulnerabilities;

(e) to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;

(f) to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;

(g) to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;

(h) to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;

(i) that ICT products, ICT services and ICT processes are secure by default and by design;

(j) that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.

Article 52

Assurance levels of European cybersecurity certification schemes

1. A European cybersecurity certification scheme may specify one or more of the following assurance levels for ICT products, ICT services and ICT processes: 'basic', 'substantial' or 'high'. The assurance level shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident.

2. European cybersecurity certificates and EU statements of conformity shall refer to any assurance level specified in the European cybersecurity certification scheme under which the European cybersecurity certificate or EU statement of conformity is issued.

3. The security requirements corresponding to each assurance level shall be provided in the relevant European cybersecurity certification scheme, including the corresponding security functionalities and the corresponding rigour and depth of the evaluation that the ICT product, ICT service or ICT process is to undergo.

4. The certificate or the EU statement of conformity shall refer to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of, or to prevent cybersecurity incidents.

5. A European cybersecurity certificate or EU statement of conformity that refers to assurance level 'basic' shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate or that EU statement of conformity is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known basic risks of incidents and cyberattacks. The evaluation activities to be undertaken shall include at least a review of technical documentation. Where such a review is not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.

6. A European cybersecurity certificate that refers to assurance level 'substantial' shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities. Where any such evaluation activities are not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.

7. A European cybersecurity certificate that refers to assurance level 'high' shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities; testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities at the state of the art; and an assessment of their resistance to skilled attackers, using penetration testing. Where any such evaluation activities are not appropriate, substitute activities with equivalent effect shall be undertaken.

8. A European cybersecurity certification scheme may specify several evaluation levels depending on the rigour and depth of the evaluation methodology used. Each of the evaluation levels shall correspond to one of the assurance levels and shall be defined by an appropriate combination of assurance components.

Article 53

Conformity self-assessment

1. A European cybersecurity certification scheme may allow for the conformity self-assessment under the sole responsibility of the manufacturer or provider of ICT products, ICT services or ICT processes. Conformity self-assessment shall be permitted only in relation to ICT products, ICT services and ICT processes that present a low risk corresponding to assurance level 'basic'.

2. The manufacturer or provider of ICT products, ICT services or ICT processes may issue an EU statement of conformity stating that the fulfilment of the requirements set out in the scheme has been demonstrated. By issuing such a statement, the manufacturer or provider of ICT products, ICT services or ICT processes shall assume responsibility for the compliance of the ICT product, ICT service or ICT process with the requirements set out in that scheme.

3. The manufacturer or provider of ICT products, ICT services or ICT processes shall make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity of the ICT products or ICT services with the scheme available to the national cybersecurity certification authority referred to in Article 58 for the period provided for in the corresponding European cybersecurity certification scheme. A copy of the EU statement of conformity shall be submitted to the national cybersecurity certification authority and to ENISA.

4. The issuing of an EU statement of conformity is voluntary, unless otherwise specified in Union law or Member State law.

5. EU statements of conformity shall be recognised in all Member States.

Article 54

Elements of European cybersecurity certification schemes

1. A European cybersecurity certification scheme shall include at least the following elements:

(a) the subject matter and scope of the certification scheme, including the type or categories of ICT products, ICT services and ICT processes covered;

(b) a clear description of the purpose of the scheme and of how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme;

(c) references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme;

(d) where applicable, one or more assurance levels;

(e) an indication of whether conformity self-assessment is permitted under the scheme;

(f) where applicable, specific or additional requirements to which conformity assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements;

(g) the specific evaluation criteria and methods to be used, including types of evaluation, in order to demonstrate that the security objectives referred to in Article 51 are achieved;

(h) where applicable, the information which is necessary for certification and which is to be supplied or otherwise be made available to the conformity assessment bodies by an applicant;

(i) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used;

(j) rules for monitoring compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates or the EU statements of conformity, including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements;

(k) where applicable, the conditions for issuing, maintaining, continuing and renewing the European cybersecurity certificates, as well as the conditions for extending or reducing the scope of certification;

(l) rules concerning the consequences for ICT products, ICT services and ICT processes that have been certified or for which an EU statement of conformity has been issued, but which do not comply with the requirements of the scheme;

(m) rules concerning how previously undetected cybersecurity vulnerabilities in ICT products, ICT services and ICT processes are to be reported and dealt with;

(n) where applicable, rules concerning the retention of records by conformity assessment bodies;

(o) the identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, ICT services and ICT processes, security requirements, evaluation criteria and methods, and assurance levels;

(p) the content and the format of the European cybersecurity certificates and the EU statements of conformity to be issued;

(q) the period of the availability of the EU statement of conformity, technical documentation, and all other relevant information to be made available by the manufacturer or provider of ICT products, ICT services or ICT processes;

(r) maximum period of validity of European cybersecurity certificates issued under the scheme;

(s) disclosure policy for European cybersecurity certificates issued, amended or withdrawn under the scheme;

(t) conditions for the mutual recognition of certification schemes with third countries;

(u) where applicable, rules concerning any peer assessment mechanism established by the scheme for the authorities or bodies issuing European cybersecurity certificates for assurance level 'high' pursuant to Article 56(6). Such mechanism shall be without prejudice to the peer review provided for in Article 59;

(v) format and procedures to be followed by manufacturers or providers of ICT products, ICT services or ICT processes in supplying and updating the supplementary cybersecurity information in accordance with Article 55.

2. The specified requirements of the European cybersecurity certification scheme shall be consistent with any applicable legal requirements, in particular requirements emanating from harmonised Union law.

3. Where a specific Union legal act so provides, a certificate or an EU statement of conformity issued under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that legal act.

4. In the absence of harmonised Union law, Member State law may also provide that a European cybersecurity certification scheme may be used for establishing the presumption of conformity with legal requirements.

Article 55

Supplementary cybersecurity information for certified ICT products, ICT services and ICT processes

1. The manufacturer or provider of certified ICT products, ICT services or ICT processes or of ICT products, ICT services and ICT processes for which an EU statement of conformity has been issued shall make publicly available the following supplementary cybersecurity information:

(a) guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the ICT products or ICT services;

(b) the period during which security support will be offered to end users, in particular as regards the availability of cybersecurity related updates;

(c) contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers;

(d) a reference to online repositories listing publicly disclosed vulnerabilities related to the ICT product, ICT service or ICT process and to any relevant cybersecurity advisories.

2. The information referred to in paragraph 1 shall be available in electronic form and shall remain available and be updated as necessary at least until the expiry of the corresponding European cybersecurity certificate or EU statement of conformity.

Article 56

Cybersecurity certification

1. ICT products, ICT services and ICT processes that have been certified under a European cybersecurity certification scheme adopted pursuant to Article 49 shall be presumed to comply with the requirements of such scheme.

2. The cybersecurity certification shall be voluntary, unless otherwise specified by Union law or Member State law.

3. The Commission shall regularly assess the efficiency and use of the adopted European cybersecurity certification schemes and whether a specific European cybersecurity certification scheme is to be made mandatory through relevant Union law to ensure an adequate level of cybersecurity of ICT products, ICT services and ICT processes in the Union and improve the functioning of the internal market. The first such assessment shall be carried out by 31 December 2023, and subsequent assessments shall be carried out at least every two years thereafter. Based on the outcome of those assessments, the Commission shall identify the ICT products, ICT services and ICT processes covered by an existing certification scheme which are to be covered by a mandatory certification scheme.

As a priority, the Commission shall focus on the sectors listed in Annex II to Directive (EU) 2016/1148, which shall be assessed at the latest two years after the adoption of the first European cybersecurity certification scheme.

When preparing the assessment the Commission shall:

(a) take into account the impact of the measures on the manufacturers or providers of such ICT products, ICT services or ICT processes and on the users in terms of the cost of those measures and the societal or economic benefits stemming from the anticipated enhanced level of security for the targeted ICT products, ICT services or ICT processes;

(b) take into account the existence and implementation of relevant Member State and third country law;

(c) carry out an open, transparent and inclusive consultation process with all relevant stakeholders and Member States;

(d) take into account any implementation deadlines, transitional measures and periods, in particular with regard to the possible impact of the measure on the manufacturers or providers of ICT products, ICT services or ICT processes, including SMEs;

(e) propose the most speedy and efficient way in which the transition from a voluntary to mandatory certification schemes is to be implemented.

4. The conformity assessment bodies referred to in Article 60 shall issue European cybersecurity certificates pursuant to this Article referring to assurance level 'basic' or 'substantial' on the basis of criteria included in the European cybersecurity certification scheme adopted by the Commission pursuant to Article 49.

5. By way of derogation from paragraph 4, in duly justified cases a European cybersecurity certification scheme may provide that European cybersecurity certificates resulting from that scheme are to be issued only by a public body. Such body shall be one of the following:

(a) a national cybersecurity certification authority as referred to in Article 58(1); or

(b) a public body that is accredited as a conformity assessment body pursuant to Article 60(1).

6. Where a European cybersecurity certification scheme adopted pursuant to Article 49 requires an assurance level 'high', the European cybersecurity certificate under that scheme is to be issued only by a national cybersecurity certification authority or, in the following cases, by a conformity assessment body:

(a) upon prior approval by the national cybersecurity certification authority for each individual European cybersecurity certificate issued by a conformity assessment body; or

(b) on the basis of a general delegation of the task of issuing such European cybersecurity certificates to a conformity assessment body by the national cybersecurity certification authority.

7. The natural or legal person who submits ICT products, ICT services or ICT processes for certification shall make available to the national cybersecurity certification authority referred to in Article 58, where that authority is the body issuing the European cybersecurity certificate, or to the conformity assessment body referred to in Article 60 all information necessary to conduct the certification.

8. The holder of a European cybersecurity certificate shall inform the authority or body referred to in paragraph 7 of any subsequently detected vulnerabilities or irregularities concerning the security of the certified ICT product, ICT service or ICT process that may have an impact on its compliance with the requirements related to the certification. That authority or body shall forward that information without undue delay to the national cybersecurity certification authority concerned.

9. A European cybersecurity certificate shall be issued for the period provided for in the European cybersecurity certification scheme and may be renewed, provided that the relevant requirements continue to be met.

10. A European cybersecurity certificate issued pursuant to this Article shall be recognised in all Member States.

Article 57

National cybersecurity certification schemes and certificates

1. Without prejudice to paragraph 3 of this Article, national cybersecurity certification schemes, and the related procedures for the ICT products, ICT services and ICT processes that are covered by a European cybersecurity certification scheme shall cease to produce effects from the date established in the implementing act adopted pursuant to Article 49(7). National cybersecurity certification schemes and the related procedures for the ICT products, ICT services and ICT processes that are not covered by a European cybersecurity certification scheme shall continue to exist.

2. Member States shall not introduce new national cybersecurity certification schemes for ICT products, ICT services and ICT processes already covered by a European cybersecurity certification scheme that is in force.

3. Existing certificates that were issued under national cybersecurity certification schemes and are covered by a European cybersecurity certification scheme shall remain valid until their expiry date.

4. With a view to avoiding the fragmentation of the internal market, Member States shall inform the Commission and the ECCG of any intention to draw up new national cybersecurity certification schemes.

Article 58

National cybersecurity certification authorities

1. Each Member State shall designate one or more national cybersecurity certification authorities in its territory or, with the agreement of another Member State, shall designate one or more national cybersecurity certification authorities established in that other Member State to be responsible for the supervisory tasks in the designating Member State.

2. Each Member State shall inform the Commission of the identity of the designated national cybersecurity certification authorities. Where a Member State designates more than one authority, it shall also inform the Commission about the tasks assigned to each of those authorities.

3. Without prejudice to point (a) of Article 56(5) and Article 56(6), each national cybersecurity certification authority shall be independent of the entities it supervises in its organisation, funding decisions, legal structure and decision-making.

4. Member States shall ensure that the activities of the national cybersecurity certification authorities that relate to the issuance of European cybersecurity certificates referred to in point (a) of Article 56(5) and in Article 56(6) are strictly separated from their supervisory activities set out in this Article and that those activities are carried out independently from each other.

5. Member States shall ensure that national cybersecurity certification authorities have adequate resources to exercise their powers and to carry out their tasks in an effective and efficient manner.

6. For the effective implementation of this Regulation, it is appropriate that national cybersecurity certification authorities participate in the ECCG in an active, effective, efficient and secure manner.

7. National cybersecurity certification authorities shall:

(a) supervise and enforce rules included in European cybersecurity certification schemes pursuant to point (j) of Article 54(1) for the monitoring of the compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates that have been issued in their respective territories, in cooperation with other relevant market surveillance authorities;

(b) monitor compliance with and enforce the obligations of the manufacturers or providers of ICT products, ICT services or ICT processes that are established in their respective territories and that carry out conformity self-assessment, and shall, in particular, monitor compliance with and enforce the obligations of such manufacturers or providers set out in Article 53(2) and (3) and in the corresponding European cybersecurity certification scheme;

(c) without prejudice to Article 60(3), actively assist and support the national accreditation bodies in the monitoring and supervision of the activities of conformity assessment bodies, for the purposes of this Regulation;

(d) monitor and supervise the activities of the public bodies referred to in Article 56(5);

(e) where applicable, authorise conformity assessment bodies in accordance with Article 60(3) and restrict, suspend or withdraw existing authorisation where conformity assessment bodies infringe the requirements of this Regulation;

(f) handle complaints by natural or legal persons in relation to European cybersecurity certificates issued by national cybersecurity certification authorities or to European cybersecurity certificates issued by conformity assessment bodies in accordance with Article 56(6) or in relation to EU statements of conformity issued under Article 53, and shall investigate the subject matter of such complaints to the extent appropriate, and shall inform the complainant of the progress and the outcome of the investigation within a reasonable period;

(g) provide an annual summary report on the activities conducted under points (b), (c) and (d) of this paragraph or under paragraph 8 to ENISA and the ECCG;

(h) cooperate with other national cybersecurity certification authorities or other public authorities, including by sharing information on the possible non-compliance of ICT products, ICT services and ICT processes with the requirements of this Regulation or with the requirements of specific European cybersecurity certification schemes; and

(i) monitor relevant developments in the field of cybersecurity certification.

8. Each national cybersecurity certification authority shall have at least the following powers:

(a) to request conformity assessment bodies, European cybersecurity certificates' holders and issuers of EU statements of conformity to provide any information it requires for the performance of its tasks;

(b) to carry out investigations, in the form of audits, of conformity assessment bodies, European cybersecurity certificates' holders and issuers of EU statements of conformity, for the purpose of verifying their compliance with this Title;

(c) to take appropriate measures, in accordance with national law, to ensure that conformity assessment bodies, European cybersecurity certificates' holders and issuers of EU statements of conformity comply with this Regulation or with a European cybersecurity certification scheme;

(d) to obtain access to the premises of any conformity assessment bodies or holders of European cybersecurity certificates, for the purpose of carrying out investigations in accordance with Union or Member State procedural law;

(e) to withdraw, in accordance with national law, European cybersecurity certificates issued by the national cybersecurity certification authorities or European cybersecurity certificates issued by conformity assessment bodies in accordance with Article 56(6), where such certificates do not comply with this Regulation or with a European cybersecurity certification scheme;

(f) to impose penalties in accordance with national law, as provided for in Article 65, and to require the immediate cessation of infringements of the obligations set out in this Regulation.

9. National cybersecurity certification authorities shall cooperate with each other and with the Commission, in particular, by exchanging information, experience and good practices as regards cybersecurity certification and technical issues concerning the cybersecurity of ICT products, ICT services and ICT processes.

Article 59

Peer review

1. With a view to achieving equivalent standards throughout the Union in respect of European cybersecurity certificates and EU statements of conformity, national cybersecurity certification authorities shall be subject to peer review.

2. Peer review shall be carried out on the basis of sound and transparent evaluation criteria and procedures, in particular concerning structural, human resource and process requirements, confidentiality and complaints.

3. Peer review shall assess:

(a) where applicable, whether the activities of the national cybersecurity certification authorities that relate to the issuance of European cybersecurity certificates referred to in point (a) of Article 56(5) and in Article 56(6) are strictly separated from their supervisory activities set out in Article 58 and whether those activities are carried out independently from each other;

(b) the procedures for supervising and enforcing the rules for monitoring the compliance of ICT products, ICT services and ICT processes with European cybersecurity certificates pursuant to point (a) of Article 58(7);

(c) the procedures for monitoring and enforcing the obligations of manufacturers or providers of ICT products, ICT services or ICT processes pursuant to point (b) of Article 58(7);

(d) the procedures for monitoring, authorising and supervising the activities of the conformity assessment bodies;

(e) where applicable, whether the staff of authorities or bodies that issue certificates for assurance level 'high' pursuant to Article 56(6) have the appropriate expertise.

4. Peer review shall be carried out by at least two national cybersecurity certification authorities of other Member States and the Commission and shall be carried out at least once every five years. ENISA may participate in the peer review.

5. The Commission may adopt implementing acts establishing a plan for peer review which covers a period of at least five years, laying down the criteria concerning the composition of the peer review team, the methodology to be used in peer review, and the schedule, the frequency and other tasks related to it. In adopting those implementing acts, the Commission shall take due account of the views of the ECCG. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 66(2).

6. The outcomes of peer reviews shall be examined by the ECCG, which shall draw up summaries that may be made publicly available and which shall, where necessary, issue guidelines or recommendations on actions or measures to be taken by the entities concerned.

Article 60

Conformity assessment bodies

1. The conformity assessment bodies shall be accredited by national accreditation bodies appointed pursuant to Regulation (EC) No 765/2008. Such accreditation shall be issued only where the conformity assessment body meets the requirements set out in the Annex to this Regulation.

2. Where a European cybersecurity certificate is issued by a national cybersecurity certification authority pursuant to point (a) of Article 56(5) and Article 56(6), the certification body of the national cybersecurity certification authority shall be accredited as a conformity assessment body pursuant to paragraph 1 of this Article.

3. Where European cybersecurity certification schemes set out specific or additional requirements pursuant to point (f) of Article 54(1), only conformity assessment bodies that meet those requirements shall be authorised by the national cybersecurity certification authority to carry out tasks under such schemes.

4. The accreditation referred to in paragraph 1 shall be issued to the conformity assessment bodies for a maximum of five years and may be renewed on the same conditions, provided that the conformity assessment body still meets the requirements set out in this Article. National accreditation bodies shall take all appropriate measures within a reasonable timeframe to restrict, suspend or revoke the accreditation of a conformity assessment body issued pursuant to paragraph 1 where the conditions for the accreditation have not been met or are no longer met, or where the conformity assessment body infringes this Regulation.

Article 61

Notification

1. For each European cybersecurity certification scheme, the national cybersecurity certification authorities shall notify the Commission of the conformity assessment bodies that have been accredited and, where applicable, authorised pursuant to Article 60(3) to issue European cybersecurity certificates at specified assurance levels as referred to in Article 52. The national cybersecurity certification authorities shall notify the Commission of any subsequent changes thereto without undue delay.

2. One year after the entry into force of a European cybersecurity certification scheme, the Commission shall publish a list of the conformity assessment bodies notified under that scheme in the *Official Journal of the European Union*.

3. If the Commission receives a notification after the expiry of the period referred to in paragraph 2, it shall publish the amendments to the list of notified conformity assessment bodies in the *Official Journal of the European Union* within two months of the date of receipt of that notification.

4. A national cybersecurity certification authority may submit to the Commission a request to remove a conformity assessment body notified by that authority from the list referred to in paragraph 2. The Commission shall publish the corresponding amendments to that list in the *Official Journal of the European Union* within one month of the date of receipt of the national cybersecurity certification authority's request.

5. The Commission may adopt implementing acts to establish the circumstances, formats and procedures for notifications referred to in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 66(2).

Article 62

European Cybersecurity Certification Group

1. The European Cybersecurity Certification Group (the 'ECCG') shall be established.

2. The ECCG shall be composed of representatives of national cybersecurity certification authorities or representatives of other relevant national authorities. A member of the ECCG shall not represent more than two Member States.

3. Stakeholders and relevant third parties may be invited to attend meetings of the ECCG and to participate in its work.

4. The ECCG shall have the following tasks:

(a) to advise and assist the Commission in its work to ensure the consistent implementation and application of this Title, in particular regarding the Union rolling work programme, cybersecurity certification policy issues, the coordination of policy approaches, and the preparation of European cybersecurity certification schemes;

(b) to assist, advise and cooperate with ENISA in relation to the preparation of a candidate scheme pursuant to Article 49;

(c) to adopt an opinion on candidate schemes prepared by ENISA pursuant to Article 49;

(d) to request ENISA to prepare candidate schemes pursuant to Article 48(2);

(e) to adopt opinions addressed to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes;

(f) to examine relevant developments in the field of cybersecurity certification and to exchange information and good practices on cybersecurity certification schemes;

(g) to facilitate the cooperation between national cybersecurity certification authorities under this Title through capacity-building and the exchange of information, in particular by establishing methods for the efficient exchange of information relating to issues concerning cybersecurity certification;

(h) to support the implementation of peer assessment mechanisms in accordance with the rules established in a European cybersecurity certification scheme pursuant to point (u) of Article 54(1);

(i) to facilitate the alignment of European cybersecurity certification schemes with internationally recognised standards, including by reviewing existing European cybersecurity certification schemes and, where appropriate, making recommendations to ENISA to engage with relevant international standardisation organisations to address insufficiencies or gaps in available internationally recognised standards.

5. With the assistance of ENISA, the Commission shall chair the ECCG, and the Commission shall provide the ECCG with a secretariat in accordance with point (e) of Article 8(1).

Article 63

Right to lodge a complaint

1. Natural and legal persons shall have the right to lodge a complaint with the issuer of a European cybersecurity certificate or, where the complaint relates to a European cybersecurity certificate issued by a conformity assessment body when acting in accordance with Article 56(6), with the relevant national cybersecurity certification authority.

2. The authority or body with which the complaint has been lodged shall inform the complainant of the progress of the proceedings and of the decision taken, and shall inform the complainant of the right to an effective judicial remedy referred to in Article 64.

Article 64

Right to an effective judicial remedy

1. Notwithstanding any administrative or other non-judicial remedies, natural and legal persons shall have the right to an effective judicial remedy with regard to:

(a) decisions taken by the authority or body referred to in Article 63(1) including, where applicable, in relation to the improper issuing, failure to issue or recognition of a European cybersecurity certificate held by those natural and legal persons;

(b) a failure to act on a complaint lodged with the authority or body referred to in Article 63(1).

2. Proceedings pursuant to this Article shall be brought before the courts of the Member State in which the authority or body against which the judicial remedy is sought is located.

Article 65

Penalties

Member States shall lay down the rules on penalties applicable to infringements of this Title and to infringements of European cybersecurity certification schemes, and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall without delay notify the Commission of those rules and of those measures and shall notify it of any subsequent amendment affecting them.

TITLE IV

FINAL PROVISIONS

Article 66

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, point (b) of Article 5(4) of Regulation (EU) No 182/2011 shall apply.

Article 67

Evaluation and review

1. By 28 June 2024, and every five years thereafter, the Commission shall evaluate the impact, effectiveness and efficiency of ENISA and of its working practices, the possible need to modify ENISA's mandate and the financial implications of any such modification. The evaluation shall take into account any feedback provided to ENISA in response to its activities. Where the Commission considers that the continued operation of ENISA is no longer justified in light of the objectives, mandate and tasks assigned to it, the Commission may propose that this Regulation be amended with regard to the provisions related to ENISA.

2. The evaluation shall also assess the impact, effectiveness and efficiency of the provisions of Title III of this Regulation with regard to the objectives of ensuring an adequate level of cybersecurity of ICT products, ICT services and ICT processes in the Union and improving the functioning of the internal market.

3. The evaluation shall assess whether essential cybersecurity requirements for access to the internal market are necessary in order to prevent ICT products, ICT services and ICT processes which do not meet basic cybersecurity requirements from entering the Union market.

4. By 28 June 2024, and every five years thereafter, the Commission shall transmit a report on the evaluation together with its conclusions to the European Parliament, to the Council and to the Management Board. The findings of that report shall be made public.

Article 68

Repeal and succession

1. Regulation (EU) No 526/2013 is repealed with effect from 27 June 2019.

2. References to Regulation (EU) No 526/2013 and to the ENISA as established by that Regulation shall be construed as references to this Regulation and to ENISA as established by this Regulation.

3. ENISA as established by this Regulation shall succeed ENISA as established by Regulation (EU) No 526/2013 as regards all ownership, agreements, legal obligations, employment contracts, financial commitments and liabilities. All decisions of the Management Board and the Executive Board adopted in accordance with Regulation (EU) No 526/2013 shall remain valid, provided that they comply with this Regulation.

4. ENISA shall be established for an indefinite period as of 27 June 2019.

5. The Executive Director appointed pursuant to Article 24(4) of Regulation (EU) No 526/2013 shall remain in office and exercise the duties of the Executive Director as referred to in Article 20 of this Regulation for the remaining part of the Executive Director's term of office. The other conditions of his or her contract shall remain unchanged.

6. The members of the Management Board and their alternates appointed pursuant to Article 6 of Regulation (EU) No 526/2013 shall remain in office and exercise the functions of the Management Board as referred to in Article 15 of this Regulation for the remaining part of their term of office.

Article 69

Entry into force

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

2. Articles 58, 60, 61, 63, 64 and 65 shall apply from 28 June 2021.

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

Done at Strasbourg, 17 April 2019.

For the European Parliament	*For the Council*
The President	*The President*
A. TAJANI	G. CIAMBA

ANNEX

REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES

Conformity assessment bodies that wish to be accredited shall meet the following requirements:

1. A conformity assessment body shall be established under national law and shall have legal personality.

2. A conformity assessment body shall be a third-party body that is independent of the organisation or the ICT products, ICT services or ICT processes that it assesses.

3. A body that belongs to a business association or professional federation representing undertakings involved in the design, manufacturing, provision, assembly, use or maintenance of ICT products, ICT services or ICT processes which it assesses may be considered to be a conformity assessment body, provided that its independence and the absence of any conflict of interest are demonstrated.

4. The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not be the designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the ICT product, ICT service or ICT process which is assessed, or the authorised representative of any of those parties. That prohibition shall not preclude the use of the ICT products assessed that are necessary for the operations of the conformity assessment body or the use of such ICT products for personal purposes.

5. The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not be directly involved in the design, manufacture or construction, the marketing, installation, use or maintenance of the ICT products, ICT services or ICT processes which are assessed, or represent parties engaged in those activities. The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not engage in any activity that may conflict with their independence of judgement or integrity in relation to their conformity assessment activities. That prohibition shall apply, in particular, to consultancy services.

6. If a conformity assessment body is owned or operated by a public entity or institution, the independence and absence of any conflict of interest shall be ensured between the national cybersecurity certification authority and the conformity assessment body, and shall be documented.

7. Conformity assessment bodies shall ensure that the activities of their subsidiaries and subcontractors do not affect the confidentiality, objectivity or impartiality of their conformity assessment activities.

8. Conformity assessment bodies and their staff shall carry out conformity assessment activities with the highest degree of professional integrity and the requisite technical competence in the specific field, and shall be free from all pressures and inducements which might influence their judgement or the results of their conformity assessment activities, including pressures and inducements of a financial nature, especially as regards persons or groups of persons with an interest in the results of those activities.

9. A conformity assessment body shall be capable of carrying out all the conformity assessment tasks assigned to it under this Regulation, regardless of whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility. Any subcontracting to, or consultation of, external staff shall be properly documented, shall not involve any intermediaries and shall be subject to a written agreement covering, among other things, confidentiality and conflicts of interest. The conformity assessment body in question shall take full responsibility for the tasks performed.

10. At all times and for each conformity assessment procedure and each type, category or sub-category of ICT products, ICT services or ICT processes, a conformity assessment body shall have at its disposal the necessary:

    (a) staff with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks;

    (b) descriptions of procedures in accordance with which conformity assessment is to be carried out, to ensure the transparency of those procedures and the possibility of reproducing them. It shall have in place appropriate policies and procedures that distinguish between tasks that it carries out as a body notified pursuant to Article 61 and its other activities;

(c) procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the technology of the ICT product, ICT service or ICT process in question and the mass or serial nature of the production process.

11. A conformity assessment body shall have the means necessary to perform the technical and administrative tasks connected with the conformity assessment activities in an appropriate manner, and shall have access to all necessary equipment and facilities.

12. The persons responsible for carrying out conformity assessment activities shall have the following:

(a) sound technical and vocational training covering all conformity assessment activities;

(b) satisfactory knowledge of the requirements of the conformity assessments they carry out and adequate authority to carry out those assessments;

(c) appropriate knowledge and understanding of the applicable requirements and testing standards;

(d) the ability to draw up certificates, records and reports demonstrating that conformity assessments have been carried out.

13. The impartiality of the conformity assessment bodies, of their top-level management, of the persons responsible for carrying out conformity assessment activities, and of any subcontractors shall be guaranteed.

14. The remuneration of the top-level management and of the persons responsible for carrying out conformity assessment activities shall not depend on the number of conformity assessments carried out or on the results of those assessments.

15. Conformity assessment bodies shall take out liability insurance unless liability is assumed by the Member State in accordance with its national law, or the Member State itself is directly responsible for the conformity assessment.

16. The conformity assessment body and its staff, its committees, its subsidiaries, its subcontractors, and any associated body or the staff of external bodies of a conformity assessment body shall maintain confidentiality and observe professional secrecy with regard to all information obtained in carrying out their conformity assessment tasks under this Regulation or pursuant to any provision of national law giving effect to this Regulation, except where disclosure is required by Union or Member State law to which such persons are subject, and except in relation to the competent authorities of the Member States in which its activities are carried out. Intellectual property rights shall be protected. The conformity assessment body shall have documented procedures in place in respect of the requirements of this point.

17. With the exception of point 16, the requirements of this Annex shall not preclude exchanges of technical information and regulatory guidance between a conformity assessment body and a person who applies for certification or who is considering whether to apply for certification.

18. Conformity assessment bodies shall operate in accordance with a set of consistent, fair and reasonable terms and conditions, taking into account the interests of SMEs in relation to fees.

19. Conformity assessment bodies shall meet the requirements of the relevant standard that is harmonised under Regulation (EC) No 765/2008 for the accreditation of conformity assessment bodies performing certification of ICT products, ICT services or ICT processes.

20. Conformity assessment bodies shall ensure that testing laboratories used for conformity assessment purposes meet the requirements of the relevant standard that is harmonised under Regulation (EC) No 765/2008 for the accreditation of laboratories performing testing.

DIRECTIVES

DIRECTIVE (EU) 2019/882 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 17 April 2019

on the accessibility requirements for products and services

(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 114 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],

Acting in accordance with the ordinary legislative procedure [2],

Whereas:

(1) The purpose of this Directive is to contribute to the proper functioning of the internal market by approximating laws, regulations and administrative provisions of the Member States as regards accessibility requirements for certain products and services by, in particular, eliminating and preventing barriers to the free movement of certain accessible products and services arising from divergent accessibility requirements in the Member States. This would increase the availability of accessible products and services in the internal market and improve the accessibility of relevant information.

(2) The demand for accessible products and services is high and the number of persons with disabilities is projected to increase significantly. An environment where products and services are more accessible allows for a more inclusive society and facilitates independent living for persons with disabilities. In this context, it should be borne in mind that the prevalence of disability in the Union is higher among women than among men.

(3) This Directive defines persons with disabilities in line with the United Nations Convention on the Rights of Persons with Disabilities, adopted on 13 December 2006 (UN CRPD), to which the Union has been a Party since 21 January 2011 and which all Member States have ratified. The UN CRPD states that persons with disabilities 'include those who have long-term physical, mental, intellectual or sensory impairments which in interaction with various barriers may hinder their full and effective participation in society on an equal basis with others'. This Directive promotes full and effective equal participation by improving access to mainstream products and services that, through their initial design or subsequent adaptation, address the particular needs of persons with disabilities.

(4) Other persons who experience functional limitations, such as elderly persons, pregnant women or persons travelling with luggage, would also benefit from this Directive. The concept of 'persons with functional limitations', as referred to in this Directive, includes persons who have any physical, mental, intellectual or sensory impairments, age related impairments, or other human body performance related causes, permanent or temporary, which, in interaction with various barriers, result in their reduced access to products and services, leading to a situation that requires those products and services to be adapted to their particular needs.

(5) The disparities between the laws, regulations and administrative provisions of Member States concerning the accessibility of products and services for persons with disabilities, create barriers to the free movement of products and services and distort effective competition in the internal market. For some products and services, those disparities are likely to increase in the Union after the entry into force of the UN CRPD. Economic operators, in particular small and medium-sized enterprises (SMEs), are particularly affected by those barriers.

[1] OJ C 303, 19.8.2016, p. 103.

[2] Position of the European Parliament of 13 March 2019 (not yet published in the Official Journal) and decision of the Council of 9 April 2019.

(6) Due to the differences in national accessibility requirements, individual professionals, SMEs and microenterprises in particular are discouraged from entering into business ventures outside their own domestic markets. The national, or even regional or local, accessibility requirements that Member States have put in place currently differ as regards both coverage and level of detail. Those differences negatively affect competitiveness and growth, due to the additional costs incurred in the development and marketing of accessible products and services for each national market.

(7) Consumers of accessible products and services and of assistive technologies, are faced with high prices due to limited competition among suppliers. Fragmentation among national regulations reduces potential benefits derived from sharing with national and international peers experiences concerning responding to societal and technological developments.

(8) The approximation of national measures at Union level is therefore necessary for the proper functioning of the internal market in order to put an end to fragmentation in the market of accessible products and services, to create economies of scale, to facilitate cross-border trade and mobility, as well as to help economic operators to concentrate resources on innovation instead of using those resources to cover expenses arising from fragmented legislation across the Union.

(9) The benefits of harmonising accessibility requirements for the internal market have been demonstrated by the application of Directive 2014/33/EU of the European Parliament and of the Council [3] regarding lifts and Regulation (EC) No 661/2009 of the European Parliament and of the Council [4] in the area of transport.

(10) In Declaration No 22, regarding persons with a disability, annexed to the Treaty of Amsterdam, the Conference of the Representatives of the Governments of the Member States agreed that, in drawing up measures under Article 114 of the Treaty on the Functioning of the European Union (TFEU), the institutions of the Union are to take account of the needs of persons with disabilities.

(11) The overall aim of the communication of the Commission of 6 May 2015 'A Digital Single Market Strategy for Europe', is to deliver sustainable economic and social benefits from a connected digital single market, thereby facilitating trade and promoting employment within the Union. Union consumers still do not enjoy the full benefits of prices and choice that the single market can offer, because cross-border online transactions are still very limited. Fragmentation also limits demand for cross-border e-commerce transactions. There is also a need for concerted action to ensure that electronic content, electronic communications services and access to audiovisual media services are fully available to persons with disabilities. It is therefore necessary to harmonise accessibility requirements across the digital single market and to ensure that all Union citizens, regardless of their abilities, can enjoy its benefits.

(12) Since the Union became a Party to the UN CRPD, its provisions have become an integral part of the Union legal order and are binding upon the institutions of the Union and on its Member States.

(13) The UN CRPD requires its Parties to take appropriate measures to ensure that persons with disabilities have access, on an equal basis with others, to the physical environment, to transportation, to information and communications, including information and communications technologies and systems, and to other facilities and services open or provided to the public, both in urban and in rural areas. The United Nations Committee on the Rights of Persons with Disabilities has identified the need to create a legislative framework with concrete, enforceable and time-bound benchmarks for monitoring the gradual implementation of accessibility.

(14) The UN CRPD calls on its Parties to undertake or promote research and development of, and to promote the availability and use of, new technologies, including information and communications technologies, mobility aids, devices and assistive technologies, suitable for persons with disabilities. The UN CRPD also calls for priority to be given to affordable technologies.

---

[3] Directive 2014/33/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to lifts and safety components for lifts (OJ L 96, 29.3.2014, p. 251).

[4] Regulation (EC) No 661/2009 of the European Parliament and of the Council of 13 July 2009 concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended therefor (OJ L 200, 31.7.2009, p. 1).

(15) The entry into force of the UN CRPD in the Member States' legal orders entails the need to adopt additional national provisions on accessibility of products and services. Without Union action, those provisions would further increase disparities between the laws, regulations and administrative provisions of the Member States.

(16) It is therefore necessary to facilitate the implementation in the Union of the UN CRPD by providing common Union rules. This Directive also supports Member States in their efforts to fulfil their national commitments, as well as their obligations under the UN CRPD regarding accessibility in a harmonised manner.

(17) The communication of the Commission of 15 November 2010 'European Disability Strategy 2010-2020 – A Renewed Commitment to a Barrier-Free Europe' – in line with the UN CRPD, identifies accessibility as one of the eight areas of action, indicates that it is a basic precondition for participation in society, and aims to ensure the accessibility of products and services.

(18) The determination of the products and services falling within the scope of this Directive is based on a screening exercise which was carried out during the preparation of the Impact Assessment that identified relevant products and services for persons with disabilities, and for which Member States have adopted or are likely to adopt diverging national accessibility requirements disruptive to the functioning of the internal market.

(19) In order to ensure the accessibility of the services falling within the scope of this Directive, products used in the provision of those services with which the consumer interacts should also be required to comply with the applicable accessibility requirements of this Directive.

(20) Even if a service, or part of a service, is subcontracted to a third party, the accessibility of that service should not be compromised and the service providers should comply with the obligations of this Directive. Service providers should also ensure proper and continuous training of their personnel in order to ensure that they are knowledgeable about how to use accessible products and services. That training should cover issues such as information provision, advice and advertising.

(21) Accessibility requirements should be introduced in the manner that is least burdensome for the economic operators and the Member States.

(22) It is necessary to specify accessibility requirements for the placing on the market of products and services which fall within the scope of this Directive, in order to ensure their free movement in the internal market.

(23) This Directive should make functional accessibility requirements compulsory and they should be formulated in terms of general objectives. Those requirements should be precise enough to create legally binding obligations and sufficiently detailed so as to make it possible to assess conformity in order to ensure the good functioning of the internal market for the products and services covered by this Directive, as well as leave a certain degree of flexibility in order to allow for innovation.

(24) This Directive contains a number of functional performance criteria related to modes of operations of products and services. Those criteria are not meant as a general alternative to the accessibility requirements of this Directive but should be used in very specific circumstances only. Those criteria should apply to specific functions or features of the products or services, to make them accessible, when the accessibility requirements of this Directive do not address one or more of those specific functions or features. In addition, in the event that an accessibility requirement contains specific technical requirements, and an alternative technical solution for those technical requirements is provided in the product or service, this alternative technical solution should still comply with the related accessibility requirements, and should result in equivalent or increased accessibility, by applying the relevant functional performance criteria.

(25) This Directive should cover consumer general purpose computer hardware systems. For those systems to perform in an accessible manner, their operating systems should also be accessible. Such computer hardware systems are characterised by their multipurpose nature and their ability to perform, with the appropriate software, the most common computing tasks requested by consumers and are intended to be operated by consumers. Personal computers, including desktops, notebooks, smartphones and tablets are examples of such computer hardware

systems. Specialised computers embedded in consumer electronics products do not constitute consumer general purpose computer hardware systems. This Directive should not cover, on an individual basis, single components with specific functions, such as a mainboard or a memory chip, that are used or that might be used in such a system.

(26) This Directive should also cover payment terminals, including both their hardware and software, and certain interactive self-service terminals, including both their hardware and software, dedicated to be used for the provision of services covered by this Directive: for example automated teller machines; ticketing machines issuing physical tickets granting access to services such as travel ticket dispensers; bank office queuing ticket machines; check-in machines; and interactive self-service terminals providing information, including interactive information screens.

(27) However, certain interactive self-service terminals providing information installed as integrated parts of vehicles, aircrafts, ships or rolling stock should be excluded from the scope of this Directive, since these form part of those vehicles, aircrafts, ships or rolling stock which are not covered by this Directive.

(28) This Directive should also cover electronic communications services including emergency communications as defined in Directive (EU) 2018/1972 of the European Parliament and of the Council [5]. At present, the measures taken by Member States to provide access to persons with disabilities are divergent and are not harmonised throughout the internal market. Ensuring that the same accessibility requirements apply throughout the Union will lead to economies of scale for economic operators active in more than one Member State and facilitate the effective access for persons with disabilities, both in their own Member State and when travelling between Member States. For electronic communications services including emergency communications to be accessible, providers should, in addition to voice, provide real time text, and total conversation services where video is provided by them, ensuring the synchronisation of all those communication means. Member States should, in addition to the requirements of this Directive, in accordance with Directive (EU) 2018/1972, be able to determine a relay service provider that could be used by persons with disabilities.

(29) This Directive harmonises accessibility requirements for electronic communications services and related products and complements Directive (EU) 2018/1972 which sets requirements on equivalent access and choice for end-users with disabilities. Directive (EU) 2018/1972 also sets requirements under universal service obligations on the affordability of internet access and voice communications and on the affordability and availability of related terminal equipment, specific equipment and services for consumers with disabilities.

(30) This Directive should also cover consumer terminal equipment with interactive computing capability foreseeably to be primarily used to access electronic communications services. For the purposes of this Directive that equipment should be deemed to include equipment used as part of the setup in accessing electronic communications services such as a router or a modem.

(31) For the purposes of this Directive, access to audiovisual media services should mean that the access to audiovisual content is accessible, as well as mechanisms that allow users with disabilities to use their assistive technologies. Services providing access to audiovisual media services could include websites, online applications, set-top box-based applications, downloadable applications, mobile device-based services including mobile applications and related media players as well as connected television services. Accessibility of audiovisual media services is regulated in Directive 2010/13/EU of the European Parliament and of the Council [6], with the exception of the accessibility of electronic programme guides (EPGs) which are included in the definition of services providing access to audiovisual media services to which this Directive applies.

(32) In the context of air, bus, rail and waterborne passenger transport services this Directive should cover, inter alia, the delivery of transport service information including real-time travel information through websites, mobile device-based services, interactive information screens and interactive self-service terminals, required by passengers

[5] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).

[6] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (OJ L 95, 15.4.2010, p. 1).

with disabilities in order to travel. This could include information about the service provider's passenger transport products and services, pre-journey information, information during the journey and information provided when a service is cancelled or its departure is delayed. Other elements of information could also include information on prices and promotions.

(33) This Directive should also cover websites, mobile device-based services including mobile applications developed or made available by operators of passenger transport services within the scope of this Directive or on their behalf, electronic ticketing services, electronic tickets and interactive self-service terminals.

(34) The determination of the scope of this Directive with regard to air, bus, rail and waterborne passenger transport services should be based on the existing sectorial legislation relating to passenger rights. Where this Directive does not apply to certain types of transport services, Member States should encourage service providers to apply the relevant accessibility requirements of this Directive.

(35) Directive (EU) 2016/2102 of the European Parliament and of the Council ([7]) already lays down obligations for public sector bodies providing transport services, including urban and suburban transport services and regional transport services, to make their websites accessible. This Directive contains exemptions for microenterprises providing services, including urban and suburban transport services and regional transport services. In addition, this Directive includes obligations to ensure that e-commerce websites are accessible. Since this Directive contains obligations for the large majority of private transport service providers to make their websites accessible, when selling tickets online, it is not necessary to introduce in this Directive further requirements for the websites of urban and suburban transport service providers and regional transport service providers.

(36) Certain elements of the accessibility requirements, in particular in relation to the provision of information as set out in this Directive, are already covered by existing Union law in the field of passenger transport. This includes elements of Regulation (EC) No 261/2004 of the European Parliament and of the Council ([8]), Regulation (EC) No 1107/2006 of the European Parliament and of the Council ([9]), Regulation (EC) No 1371/2007 of the European Parliament and of the Council ([10]), Regulation (EU) No 1177/2010 of the European Parliament and of the Council ([11]) and Regulation (EU) No 181/2011 of the European Parliament and of the Council ([12]). This includes also relevant acts adopted on the basis of Directive 2008/57/EC of the European Parliament and of the Council ([13]). To ensure regulatory consistency, the accessibility requirements set out in those Regulations and those acts should continue to apply as before. However, additional requirements of this Directive would supplement the existing requirements, improving the functioning of the internal market in the area of transport and benefiting persons with disabilities.

(37) Certain elements of transport services should not be covered by this Directive when provided outside the territory of the Member States even where the service has been directed towards the Union market. With regard to those elements, a passenger transport service operator should only be obliged to ensure that the requirements of this Directive are met with regard to the part of the service offered within the territory of the Union. However, in the case of air transport, Union air carriers should ensure that the applicable requirements of this Directive are also satisfied on flights departing from an airport situated in a third country and flying to an airport situated within the

([7]) Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies (OJ L 327, 2.12.2016, p. 1).

([8]) Regulation (EC) No 261/2004 of the European Parliament and of the Council of 11 February 2004 establishing common rules on compensation and assistance to passengers in the event of denied boarding and of cancellation or long delay of flights, and repealing Regulation (EEC) No 295/91 (OJ L 46, 17.2.2004, p. 1).

([9]) Regulation (EC) No 1107/2006 of the European Parliament and of the Council of 5 July 2006 concerning the rights of disabled persons and persons with reduced mobility when travelling by air (OJ L 204, 26.7.2006, p. 1).

([10]) Regulation (EC) No 1371/2007 of the European Parliament and of the Council of 23 October 2007 on rail passengers' rights and obligations (OJ L 315, 3.12.2007, p. 14).

([11]) Regulation (EU) No 1177/2010 of the European Parliament and of the Council of 24 November 2010 concerning the rights of passengers when travelling by sea and inland waterway and amending Regulation (EC) No 2006/2004 (OJ L 334, 17.12.2010, p. 1).

([12]) Regulation (EU) No 181/2011 of the European Parliament and of the Council of 16 February 2011 concerning the rights of passengers in bus and coach transport and amending Regulation (EC) No 2006/2004 (OJ L 55, 28.2.2011, p. 1).

([13]) Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the interoperability of the rail system within the Community (OJ L 191, 18.7.2008, p. 1).

territory of a Member State. Furthermore, all air carriers, including those which are not licenced in the Union, should ensure that the applicable requirements of this Directive are satisfied in cases where the flights depart from a Union territory to a third country territory.

(38) Urban authorities should be encouraged to integrate barrier-free accessibility to urban transport services in their Sustainable Urban Mobility Plans (SUMPs), as well as to regularly publish lists of best practices regarding barrier-free accessibility to urban public transport and mobility.

(39) Union law on banking and financial services aims to protect and provide information to consumers of those services across the Union but does not include accessibility requirements. With a view to enabling persons with disabilities to use those services throughout the Union, including where provided through websites and mobile device-based services including mobile applications, to make well-informed decisions, and to feel confident that they are adequately protected on an equal basis with other consumers, as well as ensure a level playing field for service providers, this Directive should establish common accessibility requirements for certain banking and financial services provided to consumers.

(40) The appropriate accessibility requirements should also apply to identification methods, electronic signature and payment services, since they are necessary for concluding consumer banking transactions.

(41) E-book files are based on a electronic computer coding that enables the circulation and consultation of a mostly textual and graphical intellectual work. The degree of precision of this coding determines the accessibility of e-book files, in particular regarding the qualification of the different constitutive elements of the work and the standardised description of its structure. The interoperability in terms of accessibility should optimise the compatibility of those files with the user agents and with current and future assistive technologies. Specific features of special volumes like comics, children's books and art books should be considered in the light of all applicable accessibility requirements. Divergent accessibility requirements in Member States would make it difficult for publishers and other economic operators to benefit from the advantages of the internal market, could create interoperability problems with e-readers and would limit the access for consumers with disabilities. In the context of e-books, the concept of a service provider could include publishers and other economic operators involved in their distribution.

It is recognised that persons with disabilities continue to face barriers to accessing content which is protected by copyright and related rights, and that certain measures have already been taken to address this situation for example through the adoption of Directive (EU) 2017/1564 of the European Parliament and of the Council ([14]) and Regulation (EU) 2017/1563 of the European Parliament and of the Council ([15]), and that further Union measures could be taken in this respect in the future.

(42) This Directive defines e-commerce services as a service provided at a distance, through websites and mobile device-based services, by electronic means and at the individual request of a consumer, with a view to concluding a consumer contract. For the purposes of that definition 'at a distance' means that the service is provided without the parties being simultaneously present; 'by electronic means' means that the service is initially sent and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and transmitted, conveyed and received in its entirety by wire, by radio, by optical means or by other electromagnetic means; 'at the individual request of a consumer' means that the service is provided on individual request. Given the increased relevance of e-commerce services and their high technological nature, it is important to have harmonised requirements for their accessibility.

([14]) Directive (EU) 2017/1564 of the European Parliament and of the Council of 13 September 2017 on certain permitted uses of certain works and other subject matter protected by copyright and related rights for the benefit of persons who are blind, visually impaired or otherwise print-disabled and amending Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society (OJ L 242, 20.9.2017, p. 6).

([15]) Regulation (EU) 2017/1563 of the European Parliament and of the Council of 13 September 2017 on the cross-border exchange between the Union and third countries of accessible format copies of certain works and other subject matter protected by copyright and related rights for the benefit of persons who are blind, visually impaired or otherwise print-disabled (OJ L 242, 20.9.2017, p. 1).

(43) The e-commerce services accessibility obligations of this Directive should apply to the online sale of any product or service and should therefore also apply to the sale of a product or service covered in its own right under this Directive.

(44) The measures related to the accessibility of the answering of emergency communications should be adopted without prejudice to, and should have no impact on, the organisation of emergency services, which remains in the exclusive competence of Member States.

(45) In accordance with Directive (EU) 2018/1972, Member States are to ensure that access for end-users with disabilities to emergency services is available through emergency communications and is equivalent to that enjoyed by other end-users, in accordance with Union law harmonising accessibility requirements for products and services. The Commission and the national regulatory or other competent authorities are to take appropriate measures to ensure that, whilst travelling in another Member State, end-users with disabilities can access emergency services on an equivalent basis with other end-users, where feasible without any pre-registration. Those measures seek to ensure interoperability across Member States and are to be based, to the greatest extent possible, on European standards or specifications laid down in accordance with Article 39 of Directive (EU) 2018/1972. Such measures do not prevent Member States from adopting additional requirements in order to pursue the objectives set out in that Directive. As an alternative to fulfilling the accessibility requirements with regard to the answering of emergency communications for users with disabilities set out in this Directive, Member States should be able to determine a third party relay service provider to be used by persons with disabilities to communicate with the public safety answering point, until those public safety answering points are capable of using electronic communications services through internet protocols for ensuring accessibility of answering the emergency communications. In any case, obligations of this Directive should not be understood to restrict or lower any obligations for the benefit of end-users with disabilities, including equivalent access to electronic communications services and emergency services as well as accessibility obligations as set out in Directive (EU) 2018/1972.

(46) Directive (EU) 2016/2102 defines accessibility requirements for websites and mobile applications of public sector bodies and other related aspects, in particular requirements relating to the compliance of the relevant websites and mobile applications. However, that Directive contains a specific list of exceptions. Similar exceptions are relevant for this Directive. Some activities that take place via websites and mobile applications of public sector bodies, such as passenger transport services or e-commerce services, which fall within the scope of this Directive, should in addition comply with the applicable accessibility requirements of this Directive in order to ensure that the online sale of products and services is accessible for persons with disabilities irrespective whether the seller is a public or private economic operator. The accessibility requirements of this Directive should be aligned to the requirements of Directive (EU) 2016/2102, despite differences, for example, in monitoring, reporting and enforcement.

(47) The four principles of accessibility of websites and mobile applications, as used in Directive (EU) 2016/2102, are: perceivability, meaning that information and user interface components must be presentable to users in ways they can perceive; operability, meaning that user interface components and navigation must be operable; understandability, meaning that information and the operation of the user interface must be understandable; and robustness, meaning that content must be robust enough to be interpreted reliably by a wide variety of user agents, including assistive technologies. Those principles are also relevant for this Directive.

(48) Member States should take all appropriate measures to ensure that, where the products and services covered by this Directive comply with the applicable accessibility requirements, their free movement within the Union is not impeded for reasons related to accessibility requirements.

(49) In some situations, common accessibility requirements of the built environment would facilitate the free movement of the related services and of persons with disabilities. Therefore, this Directive should enable Member States to include the built environment used in the provision of the services under the scope of this Directive, ensuring compliance with the accessibility requirements set out in Annex III.

(50) Accessibility should be achieved by the systematic removal and prevention of barriers, preferably through a universal design or 'design for all' approach, which contributes to ensuring access for persons with disabilities

on an equal basis with others. According to the UN CRPD, that approach 'means the design of products, environments, programmes and services to be usable by all people, to the greatest extent possible, without the need for adaptation or specialized design'. In line with the UN CRPD, "universal design' shall not exclude assistive devices for particular groups of persons with disabilities where this is needed'. Furthermore, accessibility should not exclude the provision of reasonable accommodation when required by Union law or national law. Accessibility and universal design should be interpreted in line with General Comment No 2(2014) – Article 9: Accessibility as written by the Committee on the Rights of Persons with Disabilities.

(51) Products and services falling within the scope of this Directive do not automatically fall within the scope of Council Directive 93/42/EEC ([16]). However, some assistive technologies which are medical devices, might fall within the scope of that Directive.

(52) Most jobs in the Union are provided by SMEs and microenterprises. They have a crucial importance for future growth, but very often face hurdles and obstacles in developing their products or services, in particular in the cross-border context. It is therefore necessary to facilitate the work of the SMEs and microenterprises by harmonising the national provisions on accessibility while maintaining the necessary safeguards.

(53) For microenterprises and SMEs to benefit from this Directive they must genuinely fulfil the requirements of Commission Recommendation 2003/361/EC ([17]), and the relevant case law, aimed at preventing the circumvention of its rules.

(54) In order to ensure the consistency of Union law, this Directive should be based on Decision No 768/2008/EC of the European Parliament and of the Council ([18]), since it concerns products already subject to other Union acts, while recognising the specific features of the accessibility requirements of this Directive.

(55) All economic operators falling within the scope of this Directive and intervening in the supply and distribution chain should ensure that they make available on the market only products which are in conformity with this Directive. The same should apply to economic operators providing services. It is necessary to provide for a clear and proportionate distribution of obligations which correspond to the role of each economic operator in the supply and distribution process.

(56) Economic operators should be responsible for the compliance of products and services, in relation to their respective roles in the supply chain, so as to ensure a high level of protection of accessibility and to guarantee fair competition on the Union market.

(57) The obligations of this Directive should apply equally to economic operators from the public and private sectors.

(58) The manufacturer having detailed knowledge of the design and production process is best placed to carry out the complete conformity assessment. While the responsibility for the conformity of products rests with the manufacturer, market surveillance authorities should play a crucial role in checking whether products made available in the Union are manufactured in accordance with Union law.

(59) Importers and distributors and should be involved in market surveillance tasks carried out by national authorities, and should participate actively, providing the competent authorities with all necessary information relating to the product concerned.

(60) Importers should ensure that products from third countries entering the Union market comply with this Directive and in particular that appropriate conformity assessment procedures have been carried out by manufacturers with regard to those products.

(61) When placing a product on the market, importers should indicate, on the product, their name, registered trade name or registered trade mark and the address at which they can be contacted.

([16]) Council Directive 93/42/EEC of 14 June 1993 concerning medical devices (OJ L 169, 12.7.1993, p. 1).
([17]) Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).
([18]) Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC (OJ L 218, 13.8.2008, p. 82).

(62) Distributors should ensure that their handling of the product does not adversely affect the compliance of the product with the accessibility requirements of this Directive.

(63) Any economic operator that either places a product on the market under its name or trademark or modifies a product already placed on the market in such a way that compliance with applicable requirements might be affected should be considered to be the manufacturer and should assume the obligations of the manufacturer.

(64) For reasons of proportionality, accessibility requirements should only apply to the extent that they do not impose a disproportionate burden on the economic operator concerned, or to the extent that they do not require a significant change in the products and services which would result in their fundamental alteration in the light of this Directive. Control mechanisms should nevertheless be in place in order to verify entitlement to exceptions to the applicability of accessibility requirements.

(65) This Directive should follow the principle of 'think small first' and should take account of the administrative burdens that SMEs are faced with. It should set light rules in terms of conformity assessment and should establish safeguard clauses for economic operators, rather than providing for general exceptions and derogations for those enterprises. Consequently, when setting up the rules for the selection and implementation of the most appropriate conformity assessment procedures, the situation of SMEs should be taken into account and the obligations to assess conformity of accessibility requirements should be limited to the extent that they do not impose a disproportionate burden on SMEs. In addition, market surveillance authorities should operate in a proportionate manner in relation to the size of undertakings and to the small serial or non-serial nature of the production concerned, without creating unnecessary obstacles for SMEs and without compromising the protection of public interest.

(66) In exceptional cases, where the compliance with accessibility requirements of this Directive would impose a disproportionate burden on economic operators, economic operators should only be required to comply with those requirements to the extent that they do not impose a disproportionate burden. In such duly justified cases, it would not be reasonably possible for an economic operator to fully apply one or more of the accessibility requirements of this Directive. However, the economic operator should make a service or a product that falls within the scope of this Directive as accessible as possible by applying those requirements to the extent that they do not impose a disproportionate burden. Those accessibility requirements which were not considered by the economic operator to impose a disproportionate burden should apply fully. Exceptions to compliance with one or more accessibility requirements due to the disproportionate burden that they impose should not go beyond what is strictly necessary in order to limit that burden with respect to the particular product or service concerned in each individual case. Measures that would impose a disproportionate burden should be understood as measures that would impose an additional excessive organisational or financial burden on the economic operator, while taking into account the likely resulting benefit for persons with disabilities in line with the criteria set out in this Directive. Criteria based on these considerations should be defined in order to enable both economic operators and relevant authorities to compare different situations and to assess in a systematic way whether a disproportionate burden exists. Only legitimate reasons should be taken into account in any assessment of the extent to which the accessibility requirements cannot be met because they would impose a disproportionate burden. Lack of priority, time or knowledge should not be considered to be legitimate reasons.

(67) The overall assessment of a disproportionate burden should be done using the criteria set out in Annex VI. The assessment of disproportionate burden should be documented by the economic operator taking into account the relevant criteria. Service providers should renew their assessment of a disproportionate burden at least every five years.

(68) The economic operator should inform the relevant authorities that it has relied on the provisions of this Directive related to fundamental alteration and/or disproportionate burden. Only upon a request from the relevant authorities should the economic operator provide a copy of the assessment explaining why its product or service is not fully accessible and providing evidence of the disproportionate burden or fundamental alteration, or both.

(69) If on the basis of the required assessment, a service provider concludes that it would constitute a disproportionate burden to require that all self-service terminals, used in the provision of services covered by this Directive, comply with the accessibility requirements of this Directive, the service provider should still apply those requirements to the extent that those requirements do not impose such a disproportionate burden on it. Consequently, the service providers should assess the extent to which a limited level of accessibility in all self-service terminals or a limited number of fully accessible self-service terminals would enable them to avoid a disproportionate burden that would otherwise be imposed on them, and should be required to comply with the accessibility requirements of this Directive only to that extent.

(70) Microenterprises are distinguished from all other undertakings by their limited human resources, annual turnover or annual balance sheet. The burden of complying with the accessibility requirements for microenterprises therefore, in general, takes a greater share of their financial and human resources than for other undertakings and is more likely to represent a disproportionate share of the costs. A significant proportion of cost for microenterprises comes from completing or keeping paperwork and records to demonstrate compliance with the different requirements set out in Union law. While all economic operators covered by this Directive should be able to assess the proportionality of complying with the accessibility requirements of this Directive and should only comply with them to the extent they are not disproportionate, demanding such an assessment from microenterprises providing services would in itself constitute a disproportionate burden. The requirements and obligations of this Directive should therefore not apply to microenterprises providing services within the scope of this Directive.

(71) For microenterprises dealing with products falling within the scope of this Directive the requirements and obligations of this Directive should be lighter in order to reduce the administrative burden.

(72) While some microenterprises are exempted from the obligations of this Directive, all microenterprises should be encouraged to manufacture, import or distribute products and to provide services that comply with the accessibility requirements of this Directive, in order to increase their competitiveness as well as their growth potential in the internal market. Member States should, therefore, provide guidelines and tools to microenterprises to facilitate the application of national measures transposing this Directive.

(73) All economic operators should act responsibly and in full accordance with the legal requirements applicable when placing or making products available on the market or providing services on the market.

(74) In order to facilitate the assessment of conformity with the applicable accessibility requirements it is necessary to provide for a presumption of conformity for products and services which are in conformity with voluntary harmonised standards that are adopted in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council ([19]) for the purpose of drawing up detailed technical specifications of those requirements. The Commission has already issued a number of standardisation requests to the European standardisation organisations on accessibility, such as standardisation mandates M/376, M/473 and M/420, which would be relevant for the preparation of harmonised standards.

(75) Regulation (EU) No 1025/2012 provides for a procedure for formal objections to harmonised standards that are considered not to comply with the requirements of this Directive.

(76) European standards should be market-driven, take into account the public interest, as well as the policy objectives clearly stated in the Commission's request to one or more European standardisation organisations to draft harmonised standards, and be based on consensus. In the absence of harmonised standards and where needed for internal market harmonisation purposes, the Commission should be able to adopt in certain cases implementing acts establishing technical specifications for the accessibility requirements of this Directive. Recourse to technical specifications should be limited to such cases. The Commission should be able to adopt technical specifications for instance when the standardisation process is blocked due to a lack of consensus between stakeholders or there are undue delays in the establishment of a harmonised standard, for example because the required quality is not reached. The Commission should leave enough time between the adoption of a request to one or more European standardisation organisations to draft harmonised standards and the adoption of a technical specification related to the same accessibility requirement. The Commission should not be allowed to adopt a technical specification if it has not previously tried to have the accessibility requirements covered through the European standardisation system, except where the Commission can demonstrate that the technical specifications respect the requirements laid down in Annex II of Regulation (EU) No 1025/2012.

(77) With a view to establishing, in the most efficient way, harmonised standards and technical specifications that meet the accessibility requirements of this Directive for products and services, the Commission should, where this is feasible, involve European umbrella organisations of persons with disabilities and all other relevant stakeholders in the process.

([19]) Regulation (EU) No 1025/2012 of 25 October 2012 of the European Parliament and of the Council on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

(78) To ensure effective access to information for market surveillance purposes, the information required to declare compliance with all applicable Union acts should be made available in a single EU declaration of conformity. In order to reduce the administrative burden on economic operators, they should be able to include in the single EU declaration of conformity all relevant individual declarations of conformity.

(79) For conformity assessment of products, this Directive should use the Internal production control of 'Module A', set out in Annex II to Decision No 768/2008/EC, as it enables economic operators to demonstrate, and the competent authorities to ensure, that products made available on the market conform to the accessibility requirements while not imposing an undue burden.

(80) When carrying out market surveillance of products and checking compliance of services, authorities should also check the conformity assessments, including whether the relevant assessment of fundamental alteration or disproportionate burden was properly carried out. When carrying out their duties authorities should also do so in cooperation with persons with disabilities and the organisations that represent them and their interests.

(81) For services, the information necessary to assess conformity with the accessibility requirements of this Directive should be provided in the general terms and conditions, or in an equivalent document, without prejudice to Directive 2011/83/EU of the European Parliament and of the Council ([20]).

(82) The CE marking, indicating the conformity of a product with the accessibility requirements of this Directive, is the visible consequence of a whole process comprising conformity assessment in a broad sense. This Directive should follow the general principles governing the CE marking of Regulation (EC) No 765/2008 of the European Parliament and of the Council ([21]) setting out the requirements for accreditation and market surveillance relating to the marketing of products. In addition to making the EU declaration of conformity, the manufacturer should inform consumers in a cost-effective manner about the accessibility of their products.

(83) In accordance with Regulation (EC) No 765/2008, by affixing the CE marking to a product, the manufacturer declares that the product is in conformity with all applicable accessibility requirements and that the manufacturer takes full responsibility therefor.

(84) In accordance with Decision No 768/2008/EC, Member States are responsible for ensuring strong and efficient market surveillance of products in their territories and should allocate sufficient powers and resources to their market surveillance authorities.

(85) Member States should check the compliance of services with the obligations of this Directive and should follow up complaints or reports related to non-compliance in order to ensure that corrective action has been taken.

(86) Where appropriate the Commission, in consultation with stakeholders, could adopt non-binding guidelines to support coordination among market surveillance authorities and authorities responsible for checking compliance of services. The Commission and Member States should be able to set up initiatives for the purpose of sharing the resources and expertise of authorities.

(87) Member States should ensure that market surveillance authorities and authorities responsible for checking compliance of services check the compliance of the economic operators with the criteria set out in Annex VI in accordance with Chapters VIII and IX. Member States should be able to designate a specialised body for carrying out the obligations of market surveillance authorities or authorities responsible for checking compliance of services under this Directive. Member States should be able to decide that the competences of such a specialised body should be limited to the scope of this Directive or certain parts thereof, without prejudice to the Member States' obligations under Regulation (EC) No 765/2008.

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

([21]) Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

(88) A safeguard procedure should be set up to apply in the event of disagreement between Member States over measures taken by a Member State under which interested parties are informed of measures intended to be taken with regard to products not complying with the accessibility requirements of this Directive. The safeguard procedure should allow market surveillance authorities, in cooperation with the relevant economic operators, to act at an earlier stage in respect of such products.

(89) Where the Member States and the Commission agree that a measure taken by a Member State is justified, no further involvement of the Commission should be required, except where non-compliance can be attributed to shortcomings in the harmonised standards or in the technical specifications.

(90) Directives 2014/24/EU ([22]) and 2014/25/EU ([23]) of the European Parliament and of the Council on public procurement, defining procedures for the procurement of public contracts and design contests for certain supplies (products), services and works, establish that, for all procurement which is intended for use by natural persons, whether general public or staff of the contracting authority or entity, the technical specifications are, except in duly justified cases, to be drawn up so as to take into account accessibility criteria for persons with disabilities or design for all users. Furthermore, those Directives require that, where mandatory accessibility requirements are adopted by a legal act of the Union, technical specifications are, as far as accessibility for persons with disabilities or design for all users are concerned, to be established by reference thereto. This Directive should establish mandatory accessibility requirements for products and services covered by it. For products and services not falling under the scope of this Directive, the accessibility requirements of this Directive are not binding. However, the use of those accessibility requirements to fulfil the relevant obligations set out in Union acts other than this Directive would facilitate the implementation of accessibility and contribute to the legal certainty and to the approximation of accessibility requirements across the Union. Authorities should not be prevented from establishing accessibility requirements that go beyond the accessibility requirements set out in Annex I to this Directive.

(91) This Directive should not change the compulsory or voluntary nature of the provisions related to accessibility in other Union acts.

(92) This Directive should only apply to procurement procedures for which the call for competition has been sent or, in cases where a call for competition is not foreseen, where the contracting authority or contracting entity has commenced the procurement procedure after the date of application of this Directive.

(93) In order to ensure the proper application of this Directive, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of: further specifying the accessibility requirements that, by their very nature, cannot produce their intended effect unless they are further specified in binding legal acts of the Union; changing the period during which economic operators are to be able to identify any other economic operator who has supplied them with a product or to whom they have supplied a product; and further specifying the relevant criteria that are to be taken into account by the economic operator for the assessment of whether compliance with the accessibility requirements would impose a disproportionate burden. 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 ([24]). 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.

(94) In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission with regard to the technical specifications. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council ([25]).

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

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

([24]) OJ L 123, 12.5.2016, p. 1.

([25]) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(95) Member States should ensure that adequate and effective means exist to ensure compliance with this Directive and should therefore establish appropriate control mechanisms, such as a posteriori control by the market surveillance authorities, in order to verify that the exemption from the accessibility requirements application is justified. When dealing with complaints related to accessibility, Member States should comply with the general principle of good administration, and in particular with the obligation of officials to ensure that a decision on each complaint is taken within a reasonable time-limit.

(96) In order to facilitate the uniform implementation of this Directive, the Commission should establish a working group consisting of relevant authorities and stakeholders to facilitate exchange of information and of best practices and to provide advice. Cooperation should be fostered between authorities and relevant stakeholders, including persons with disabilities and organisations that represent them, inter alia, to improve coherence in the application of provisions of this Directive concerning accessibility requirements and to monitor implementation of its provisions on fundamental alteration and disproportionate burden.

(97) Given the existing legal framework concerning remedies in the areas covered by Directives 2014/24/EU and 2014/25/EU, the provisions of this Directive relating to enforcement and penalties should not be applicable to the procurement procedures subject to the obligations imposed by this Directive. Such exclusion is without prejudice to the obligations of Member States under the Treaties to take all measures necessary to guarantee the application and effectiveness of Union law.

(98) Penalties should be adequate in relation to the character of the infringements and to the circumstances so as not to serve as an alternative to the fulfilment by economic operators of their obligations to make their products or services accessible.

(99) Member States should ensure that, in accordance with existing Union law, alternative dispute resolutions mechanisms are in place that allow the resolution of any alleged non-compliance with this Directive prior to an action being brought before courts or competent administrative bodies.

(100) In accordance with the Joint Political Declaration of 28 September 2011 of Member States and the Commission on explanatory documents ([26]), Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a Directive and the corresponding parts of national transposition instruments. With regard to this Directive, the legislator considers the transmission of such documents to be justified.

(101) In order to allow service providers sufficient time to adapt to the requirements of this Directive, it is necessary to provide for a transitional period of five years after the date of application of this Directive, during which products used for the provision of a service which were placed on the market before that date do not need to comply with the accessibility requirements of this Directive unless they are replaced by the service providers during the transitional period. Given the cost and long life-cycle of self-service terminals, it is appropriate to provide that, when such terminals are used in the provision of services, they may continue to be used until the end of their economic life, as long as they are not replaced during that period, but not for longer than 20 years.

(102) The accessibility requirements of this Directive should apply to products placed on the market and services provided after the date of application of the national measures transposing this Directive, including used and second-hand products imported from a third country and placed on the market after that date.

(103) This Directive respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union ('the Charter'). In particular, this Directive seeks to ensure full respect for the rights of persons with disabilities to benefit from measures designed to ensure their independence, social and occupational integration and participation in the life of the community and to promote the application of Articles 21, 25 and 26 of the Charter.

(104) Since the objective of this Directive, namely, the elimination of barriers to the free movement of certain accessible products and services, in order to contribute to the proper functioning of the internal market, cannot be sufficiently achieved by the Member States because it requires the harmonisation of different rules currently existing in their respective legal systems, but can rather, by defining common accessibility requirements and rules for the functioning of the internal market, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective,

([26]) OJ C 369, 17.12.2011, p. 14.

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

General provisions

Article 1

Subject matter

The purpose of this Directive is to contribute to the proper functioning of the internal market by approximating the laws, regulations and administrative provisions of the Member States as regards accessibility requirements for certain products and services by, in particular, eliminating and preventing barriers to the free movement of products and services covered by this Directive arising from divergent accessibility requirements in the Member States.

Article 2

Scope

1. This Directive applies to the following products placed on the market after 28 June 2025:

(a) consumer general purpose computer hardware systems and operating systems for those hardware systems;

(b) the following self-service terminals:

(i) payment terminals;

(ii) the following self-service terminals dedicated to the provision of services covered by this Directive:

— automated teller machines;

— ticketing machines;

— check-in machines;

— interactive self-service terminals providing information, excluding terminals installed as integrated parts of vehicles, aircrafts, ships or rolling stock;

(c) consumer terminal equipment with interactive computing capability, used for electronic communications services;

(d) consumer terminal equipment with interactive computing capability, used for accessing audiovisual media services; and

(e) e-readers.

2. Without prejudice to Article 32, this Directive applies to the following services provided to consumers after 28 June 2025:

(a) electronic communications services with the exception of transmission services used for the provision of machine-to-machine services;

(b) services providing access to audiovisual media services;

(c) the following elements of air, bus, rail and waterborne passenger transport services, except for urban, suburban and regional transport services for which only the elements under point (v) apply:

(i) websites;

(ii) mobile device-based services including mobile applications;

(iii) electronic tickets and electronic ticketing services;

(iv) delivery of transport service information, including real-time travel information; this shall, with regard to information screens, be limited to interactive screens located within the territory of the Union; and

(v) interactive self-service terminals located within the territory of the Union, except those installed as integrated parts of vehicles, aircrafts, ships and rolling stock used in the provision of any part of such passenger transport services;

(d) consumer banking services;

(e) e-books and dedicated software; and

(f) e-commerce services.

3. This Directive applies to answering emergency communications to the single European emergency number '112'.

4. This Directive does not apply to the following content of websites and mobile applications:

(a) pre-recorded time-based media published before 28 June 2025;

(b) office file formats published before 28 June 2025;

(c) online maps and mapping services, if essential information is provided in an accessible digital manner for maps intended for navigational use;

(d) third-party content that is neither funded, developed by, or under the control of, the economic operator concerned;

(e) content of websites and mobile applications qualifying as archives, meaning that they only contain content that is not updated or edited after 28 June 2025.

5. This Directive shall be without prejudice to Directive (EU) 2017/1564 and Regulation (EU) 2017/1563.

Article 3

Definitions

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

(1) 'persons with disabilities' means persons who have long-term physical, mental, intellectual or sensory impairments which in interaction with various barriers may hinder their full and effective participation in society on an equal basis with others;

(2) 'product' means a substance, preparation, or good produced through a manufacturing process, other than food, feed, living plants and animals, products of human origin and products of plants and animals relating directly to their future reproduction;

(3) 'service' means a service as defined in point 1 of Article 4 of Directive 2006/123/EC of the European Parliament and of the Council ([27]);

(4) 'service provider' means any natural or legal person who provides a service on the Union market or makes offers to provide such a service to consumers in the Union;

(5) 'audiovisual media services' means services as defined in point (a) of Article 1(1) of Directive 2010/13/EU;

(6) 'services providing access to audiovisual media services' means services transmitted by electronic communications networks which are used to identify, select, receive information on, and view audiovisual media services and any provided features, such as subtitles for the deaf and hard of hearing, audio description, spoken subtitles and sign language interpretation, which result from the implementation of measures to make services accessible as referred to in Article 7 of Directive 2010/13/EU; and includes electronic programme guides (EPGs);

(7) 'consumer terminal equipment with interactive computing capability, used for accessing audiovisual media services' means any equipment the main purpose of which is to provide access to audiovisual media services;

([27]) Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market (OJ L 376, 27.12.2006, p. 36).

(8) 'electronic communications service' means electronic communications service as defined in point 4 of Article 2 of Directive (EU) 2018/1972;

(9) 'total conversation service' means total conversation service as defined in point 35 of Article 2 of Directive (EU) 2018/1972;

(10) 'public safety answering point' or 'PSAP' means public safety answering point or PSAP as defined in point 36 of Article 2 of Directive (EU) 2018/1972;

(11) 'most appropriate PSAP' means most appropriate PSAP as defined in point 37 of Article 2 of Directive (EU) 2018/1972;

(12) 'emergency communication' means emergency communication as defined in point 38 of Article 2 of Directive (EU) 2018/1972;

(13) 'emergency service' means emergency service as defined in point 39 of Article 2 of Directive (EU) 2018/1972;

(14) 'real time text' means a form of text conversation in point to point situations or in multipoint conferencing where the text being entered is sent in such a way that the communication is perceived by the user as being continuous on a character-by-character basis;

(15) 'making available on the market' means any supply of a product for distribution, consumption or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge;

(16) 'placing on the market' means the first making available of a product on the Union market;

(17) 'manufacturer' means any natural or legal person who manufactures a product or has a product designed or manufactured, and markets that product under its name or trademark;

(18) 'authorised representative' means any natural or legal person established within the Union who has received a written mandate from a manufacturer to act on its behalf in relation to specified tasks;

(19) 'importer' means any natural or legal person established within the Union who places a product from a third country on the Union market;

(20) 'distributor' means any natural or legal person in the supply chain, other than the manufacturer or the importer, who makes a product available on the market;

(21) 'economic operator' means the manufacturer, the authorised representative, the importer, the distributor or the service provider;

(22) 'consumer' means any natural person who purchases the relevant product or is a recipient of the relevant service for purposes which are outside his trade, business, craft or profession;

(23) 'microenterprise' means an enterprise which employs fewer than 10 persons and which has an annual turnover not exceeding EUR 2 million or an annual balance sheet total not exceeding EUR 2 million;

(24) 'small and medium-sized enterprises' or 'SMEs' means enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, or an annual balance sheet total not exceeding EUR 43 million, but excludes microenterprises;

(25) 'harmonised standard' means a harmonised standard as defined in point 1(c) of Article 2 of Regulation (EU) No 1025/2012;

(26) 'technical specification' means a technical specification as defined in point 4 of Article 2 of Regulation (EU) No 1025/2012 that provides a means to comply with the accessibility requirements applicable to a product or service;

(27) 'withdrawal' means any measure aimed at preventing a product in the supply chain from being made available on the market;

(28) 'consumer banking services' means the provision to consumers of the following banking and financial services:

(a) credit agreements covered by Directive 2008/48/EC of the European Parliament and of the Council ([28]) or Directive 2014/17/EU of the European Parliament and of the Council ([29]);

(b) services as defined in points 1, 2, 4 and 5 in Section A and points 1, 2, 4 and 5 in Section B of Annex I to Directive 2014/65/EU of the European Parliament and of the Council ([30]);

(c) payment services as defined in point 3 of Article 4 of Directive (EU) 2015/2366 of the European Parliament and of the Council ([31]);

(d) services linked to the payment account as defined in point 6 of Article 2 of Directive 2014/92/EU of the European Parliament and of the Council ([32]); and

(e) electronic money as defined in point 2 of Article 2 of Directive 2009/110/EC of the European Parliament and of the Council ([33]);

(29) 'payment terminal' means a device the main purpose of which is to allow payments to be made by using payment instruments as defined in point 14 of Article 4 of Directive (EU) 2015/2366 at a physical point of sale but not in a virtual environment;

(30) 'e-commerce services' means services provided at a distance, through websites and mobile device-based services by electronic means and at the individual request of a consumer with a view to concluding a consumer contract;

(31) 'air passenger transport services' means commercial passenger air services, as defined in point (l) of Article 2 of Regulation (EC) No 1107/2006, on departure from, on transit through, or on arrival at an airport, when the airport is situated in the territory of a Member State, including flights departing from an airport situated in a third country to an airport situated in the territory of a Member State where the services are operated by Union air carriers;

(32) 'bus passenger transport services' means services covered by Article 2(1) and (2) of Regulation (EU) No 181/2011;

(33) 'rail passenger transport services' means all rail passenger services as referred to in Article 2(1) of Regulation (EC) No 1371/2007, with the exception of services referred to in Article 2(2) thereof;

(34) 'waterborne passenger transport services' means passenger services covered by Article 2(1) of Regulation (EU) No 1177/2010, with the exception of services referred to in Article 2(2) of that Regulation;

(35) 'urban and suburban transport services' means urban and suburban services as defined in point 6 of Article 3 of Directive 2012/34/EU of the European Parliament and of the Council ([34]); but for the purposes of this Directive, it includes only the following modes of transport: rail, bus and coach, metro, tram and trolley bus;

([28]) Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC (OJ L 133, 22.5.2008, p. 66).
([29]) Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010 (OJ L 60, 28.2.2014, p. 34).
([30]) Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).
([31]) Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).
([32]) Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features (OJ L 257, 28.8.2014, p. 214).
([33]) Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (OJ L 267, 10.10.2009, p. 7).
([34]) Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (OJ L 343, 14.12.2012, p. 32).

(36) 'regional transport services' means regional services as defined in point 7 of Article 3 of Directive 2012/34/EU; but for the purposes of this Directive, it includes only the following modes of transport: rail, bus and coach, metro, tram and trolley bus;

(37) 'assistive technology' means any item, piece of equipment, service or product system including software that is used to increase, maintain, substitute or improve functional capabilities of persons with disabilities or for, alleviation and compensation of impairments, activity limitations or participation restrictions;

(38) 'operating system' means software, which, inter alia, handles the interface to peripheral hardware, schedules tasks, allocates storage, and presents a default interface to the user when no application program is running including a graphical user interface, regardless of whether such software is an integral part of consumer general purpose computer hardware, or constitutes free-standing software intended to be run on consumer general purpose computer hardware, but excluding an operating system loader, basic input/output system, or other firmware required at boot time or when installing the operating system;

(39) 'consumer general purpose computer hardware system' means the combination of hardware which forms a complete computer, characterised by its multipurpose nature, its ability to perform, with the appropriate software, most common computing tasks requested by consumers and intended to be operated by consumers, including personal computers, in particular desktops, notebooks, smartphones and tablets;

(40) 'interactive computing capability' means functionality supporting human-device interaction allowing for processing and transmission of data, voice or video or any combination thereof;

(41) 'e-book and dedicated software' means a service, consisting of the provision of digital files that convey an electronic version of a book, that can be accessed, navigated, read and used and the software including mobile device-based services including mobile applications dedicated to the accessing, navigation, reading and use of those digital files, and it excludes software covered under the definition in point (42);

(42) 'e-reader' means dedicated equipment, including both hardware and software, used to access, navigate, read and use e-book files;

(43) 'electronic tickets' means any system in which an entitlement to travel, in the form of single or multiple travel tickets, travel subscriptions or travel credit, is stored electronically on a physical transport pass or other device, instead of being printed on a paper ticket;

(44) 'electronic ticketing services' means any system in which passenger transport tickets are purchased including online using a device with interactive computing capability, and delivered to the purchaser in electronic form, to enable them to be printed in paper form or displayed using a mobile device with interactive computing capability when travelling.

CHAPTER II

Accessibility requirements and free movement

Article 4

Accessibility requirements

1. Member States shall ensure, in accordance with paragraphs 2, 3 and 5 of this Article and subject to Article 14, that economic operators only place on the market products and only provide services that comply with the accessibility requirements set out in Annex I.

2. All products shall comply with the accessibility requirements set out in Section I of Annex I.

All products, except for self-service terminals, shall comply with the accessibility requirements set out in Section II of Annex I.

3. Without prejudice to paragraph 5 of this Article, all services, except for urban and suburban transport services and regional transport services, shall comply with the accessibility requirements set out in Section III of Annex I.

Without prejudice to paragraph 5 of this Article, all services shall comply with the accessibility requirements set out in Section IV of Annex I.

4. Member States may decide, in the light of national conditions, that the built environment used by clients of services covered by this Directive shall comply with the accessibility requirements set out in Annex III, in order to maximise their use by persons with disabilities.

5. Microenterprises providing services shall be exempt from complying with the accessibility requirements referred to in paragraph 3 of this Article and any obligations relating to the compliance with those requirements.

6. Member States shall provide guidelines and tools to microenterprises to facilitate the application of the national measures transposing this Directive. Member States shall develop those tools in consultation with relevant stakeholders.

7. Member States may inform economic operators of the indicative examples, contained in Annex II, of possible solutions that contribute to meeting the accessibility requirements in Annex I.

8. Member States shall ensure that the answering of emergency communications to the single European emergency number '112' by the most appropriate PSAP, shall comply with the specific accessibility requirements set out in Section V of Annex I in the manner best suited to the national organisation of emergency systems.

9. The Commission is empowered to adopt delegated acts in accordance with Article 26 to supplement Annex I by further specifying the accessibility requirements that, by their very nature, cannot produce their intended effect unless they are further specified in binding legal acts of the Union, such as requirements related to interoperability.

Article 5

Existing Union law in the field of passenger transport

Services complying with the requirements on the provision of accessible information and of information on accessibility laid down in Regulations (EC) No 261/2004, (EC) No 1107/2006, (EC) No 1371/2007, (EU) No 1177/2010, and (EU) No 181/2011 and relevant acts adopted on the basis of Directive 2008/57/EC shall be deemed to comply with the corresponding requirements of this Directive. Where this Directive provides for requirements additional to those provided in those Regulations and those acts, the additional requirements shall apply in full.

Article 6

Free movement

Member States shall not impede, for reasons related to accessibility requirements, the making available on the market in their territory of products or the provision of services in their territory that comply with this Directive.

CHAPTER III

Obligations of economic operators dealing with products

Article 7

Obligations of manufacturers

1. When placing their products on the market, manufacturers shall ensure that the products have been designed and manufactured in accordance with the applicable accessibility requirements of this Directive.

2. Manufacturers shall draw up the technical documentation in accordance with Annex IV and carry out the conformity assessment procedure set out in that Annex or have it carried out.

Where compliance of a product with the applicable accessibility requirements has been demonstrated by that procedure, manufacturers shall draw up an EU declaration of conformity and affix the CE marking.

3. Manufacturers shall keep the technical documentation and the EU declaration of conformity for five years after the product has been placed on the market.

4. Manufacturers shall ensure that procedures are in place for series production to remain in conformity with this Directive. Changes in product design or characteristics and changes in the harmonised standards, or in technical specifications, by reference to which conformity of a product is declared shall be adequately taken into account.

5. Manufacturers shall ensure that their products bear a type, batch or serial number or other element allowing their identification, or, where the size or nature of the product does not allow it, that the required information is provided on the packaging or in a document accompanying the product.

6. Manufacturers shall indicate their name, registered trade name or registered trade mark and the address at which they can be contacted on the product or, where that is not possible, on its packaging or in a document accompanying the product. The address must indicate a single point at which the manufacturer can be contacted. The contact details shall be in a language easily understood by end-users and market surveillance authorities.

7. Manufacturers shall ensure that the product is accompanied by instructions and safety information in a language which can be easily understood by consumers and other end-users, as determined by the Member State concerned. Such instructions and information, as well as any labelling, shall be clear, understandable and intelligible.

8. Manufacturers who consider or have reason to believe that a product which they have placed on the market is not in conformity with this Directive shall immediately take the corrective measures necessary to bring that product into conformity, or, if appropriate, to withdraw it. Furthermore, where the product does not comply with the accessibility requirements of this Directive, manufacturers shall immediately inform the competent national authorities of the Member States in which they made the product available to that effect, giving details, in particular, of the non-compliance and of any corrective measures taken. In such cases, manufacturers shall keep a register of products which do not comply with applicable accessibility requirements and of the related complaints.

9. Manufacturers shall, further to a reasoned request from a competent national authority, provide it with all the information and documentation necessary to demonstrate the conformity of the product, in a language which can be easily understood by that authority. They shall cooperate with that authority, at its request, on any action taken to eliminate the non-compliance with the applicable accessibility requirements of products which they have placed on the market, in particular bringing the products into compliance with the applicable accessibility requirements.

Article 8

Authorised representatives

1. A manufacturer may, by a written mandate, appoint an authorised representative.

The obligations laid down in Article 7(1) and the drawing up of technical documentation shall not form part of the authorised representative's mandate.

2. An authorised representative shall perform the tasks specified in the mandate received from the manufacturer. The mandate shall allow the authorised representative to do at least the following:

(a) keep the EU declaration of conformity and the technical documentation at the disposal of market surveillance authorities for five years;

(b) further to a reasoned request from a competent national authority, provide that authority with all the information and documentation necessary to demonstrate the conformity of a product;

(c) cooperate with the competent national authorities, at their request, on any action taken to eliminate the non-compliance with the applicable accessibility requirements of products covered by their mandate.

Article 9

Obligations of importers

1. Importers shall place only compliant products on the market.

2. Before placing a product on the market, importers shall ensure that the conformity assessment procedure set out in Annex IV has been carried out by the manufacturer. They shall ensure that the manufacturer has drawn up the technical documentation required by that Annex, that the product bears the CE marking and is accompanied by the required documents and that the manufacturer has complied with the requirements set out in Article 7(5) and (6).

3. Where an importer considers or has reason to believe that a product is not in conformity with the applicable accessibility requirements of this Directive, the importer shall not place the product on the market until it has been brought into conformity. Furthermore, where the product does not comply with the applicable accessibility requirements, the importer shall inform the manufacturer and the market surveillance authorities to that effect.

4. Importers shall indicate their name, registered trade name or registered trade mark and the address at which they can be contacted on the product or, where that is not possible, on its packaging or in a document accompanying the product. The contact details shall be in a language easily understood by end-users and market surveillance authorities.

5. Importers shall ensure that the product is accompanied by instructions and safety information in a language which can be easily understood by consumers and other end-users, as determined by the Member State concerned.

6. Importers shall ensure that, while a product is under their responsibility, storage or transport conditions do not jeopardise its compliance with the applicable accessibility requirements.

7. Importers shall, for a period of five years keep a copy of the EU declaration of conformity at the disposal of the market surveillance authorities and shall ensure that the technical documentation can be made available to those authorities upon request.

8. Importers who consider or have reason to believe that a product which they have placed on the market is not in conformity with this Directive shall immediately take the corrective measures necessary to bring that product into conformity, or, if appropriate, to withdraw it. Furthermore, where the product does not comply with the applicable accessibility requirements, importers shall immediately inform the competent national authorities of the Member States in which they made the product available to that effect, giving details, in particular, of the non-compliance and of any corrective measures taken. In such cases, importers shall keep a register of products which do not comply with applicable accessibility requirements, and of the related complaints.

9. Importers shall, further to a reasoned request from a competent national authority, provide it with all the information and documentation necessary to demonstrate the conformity of a product in a language which can be easily understood by that authority. They shall cooperate with that authority, at its request, on any action taken to eliminate the non-compliance with the applicable accessibility requirements of products which they have placed on the market.

Article 10

Obligations of distributors

1. When making a product available on the market distributors shall act with due care in relation to the requirements of this Directive.

2. Before making a product available on the market distributors shall verify that the product bears the CE marking, that it is accompanied by the required documents and by instructions and safety information in a language which can be easily understood by consumers and other end-users in the Member State in which the product is to be made available on the market and that the manufacturer and the importer have complied with the requirements set out in Article 7(5) and (6) and Article 9(4) respectively.

3. Where a distributor considers or has reason to believe that a product is not in conformity with the applicable accessibility requirements of this Directive, the distributor shall not make the product available on the market until it has been brought into conformity. Furthermore, where the product does not comply with the applicable accessibility requirements, the distributor shall inform the manufacturer or the importer and the market surveillance authorities to that effect.

4. Distributors shall ensure that, while a product is under their responsibility, storage or transport conditions do not jeopardise its compliance with the applicable accessibility requirements.

5. Distributors who consider or have reason to believe that a product which they have made available on the market is not in conformity with this Directive shall make sure that the corrective measures necessary to bring that product into conformity, or, if appropriate, to withdraw it, are taken. Furthermore, where the product, does not comply with the applicable accessibility requirements, distributors shall immediately inform the competent national authorities of the Member States in which they made the product available to that effect, giving details, in particular, of the non-compliance and of any corrective measures taken.

6. Distributors shall, further to a reasoned request from a competent national authority, provide it with all the information and documentation necessary to demonstrate the conformity of a product. They shall cooperate with that authority, at its request, on any action taken to eliminate the non-compliance with the applicable accessibility requirements of products which they have made available on the market.

Article 11

Cases in which obligations of manufacturers apply to importers and distributors

An importer or distributor shall be considered a manufacturer for the purposes of this Directive and shall be subject to the obligations of the manufacturer under Article 7, where it places a product on the market under its name or trademark or modifies a product already placed on the market in such a way that compliance with the requirements of this Directive may be affected.

Article 12

Identification of economic operators dealing with products

1. Economic operators referred to in Articles 7 to 10 shall, upon request, identify to the market surveillance authorities, the following:

(a) any other economic operator who has supplied them with a product;

(b) any other economic operator to whom they have supplied a product.

2. Economic operators referred to in Articles 7 to 10 shall be able to present the information referred to in paragraph 1 of this Article for a period of five years after they have been supplied with the product and for a period of five years after they have supplied the product.

3. The Commission is empowered to adopt delegated acts in accordance with Article 26 to amend this Directive in order to change the period referred to in paragraph 2 of this Article for specific products. That amended period shall be longer than five years, and shall be in proportion to the economically useful life of the product concerned.

CHAPTER IV

Obligations of service providers

Article 13

Obligations of service providers

1. Service providers shall ensure that they design and provide services in accordance with the accessibility requirements of this Directive.

2. Service providers shall prepare the necessary information in accordance with Annex V and shall explain how the services meet the applicable accessibility requirements. The information shall be made available to the public in written and oral format, including in a manner which is accessible to persons with disabilities. Service providers shall keep that information for as long as the service is in operation.

3. Without prejudice to Article 32, service providers shall ensure that procedures are in place so that the provision of services remains in conformity with the applicable accessibility requirements. Changes in the characteristics of the provision of the service, changes in applicable accessibility requirements and changes in the harmonised standards or in technical specifications by reference to which a service is declared to meet the accessibility requirements shall be adequately taken into account by the service providers.

4. In the case of non-conformity, service providers shall take the corrective measures necessary to bring the service into conformity with the applicable accessibility requirements. Furthermore, where the service is not compliant with applicable accessibility requirements, service providers shall immediately inform the competent national authorities of the Member States in which the service is provided, to that effect, giving details, in particular, of the non-compliance and of any corrective measures taken.

5. Service providers shall, further to a reasoned request from a competent authority, provide it with all information necessary to demonstrate the conformity of the service with the applicable accessibility requirements. They shall cooperate with that authority, at the request of that authority, on any action taken to bring the service into compliance with those requirements.

CHAPTER V

Fundamental alteration of products or services and disproportionate burden to economic operators

Article 14

Fundamental alteration and disproportionate burden

1. The accessibility requirements referred to in Article 4 shall apply only to the extent that compliance:

(a) does not require a significant change in a product or service that results in the fundamental alteration of its basic nature; and

(b) does not result in the imposition of a disproportionate burden on the economic operators concerned.

2. Economic operators shall carry out an assessment of whether compliance with the accessibility requirements referred to in Article 4 would introduce a fundamental alteration or, based on the relevant criteria set out in Annex VI, impose a disproportionate burden, as provided for in paragraph 1 of this Article.

3. Economic operators shall document the assessment referred to in paragraph 2. Economic operators shall keep all relevant results for a period of five years to be calculated from the last making available of a product on the market or after a service was last provided, as applicable. Upon a request from the market surveillance authorities or from the authorities responsible for checking compliance of services, as applicable, the economic operators shall provide the authorities with a copy of the assessment referred to in paragraph 2.

4. By way of derogation from paragraph 3, microenterprises dealing with products shall be exempted from the requirement to document their assessment. However, if a market surveillance authority so requests, microenterprises dealing with products and which have chosen to rely on paragraph 1 shall provide the authority with the facts relevant to the assessment referred to in paragraph 2.

5. Service providers relying on point (b) of paragraph 1 shall, with regard to each category or type of service, renew their assessment of whether the burden is disproportionate:

(a) when the service offered is altered; or

(b) when requested to do so by the authorities responsible for checking compliance of services; and

(c) in any event, at least every five years.

6. Where economic operators receive funding from other sources than the economic operator's own resources, whether public or private, that is provided for the purpose of improving accessibility, they shall not be entitled to rely on point (b) of paragraph 1.

7. The Commission is empowered to adopt delegated acts in accordance with Article 26 to supplement Annex VI by further specifying the relevant criteria that are to be taken into account by the economic operator for the assessment referred to in paragraph 2 of this Article. When further specifying those criteria, the Commission shall take into account not only the potential benefits for persons with disabilities, but also those for persons with functional limitations.

When necessary, the Commission shall adopt the first such delegated act by 28 June 2020. Such act shall start to apply, at the earliest, in 28 June 2025.

8. Where economic operators rely on paragraph 1 for a specific product or service they shall send information to that effect to the relevant market surveillance authorities, or authorities responsible for checking the compliance of services, of the Member State where the specific product is placed on the market or the specific service is provided.

The first subparagraph shall not apply to microenterprises.

CHAPTER VI

Harmonised standards and technical specifications of products and services

Article 15

Presumption of conformity

1. Products and services which are in conformity with harmonised standards or parts thereof the references of which have been published in the *Official Journal of the European Union*, shall be presumed to be in conformity with the accessibility requirements of this Directive in so far as those standards or parts thereof cover those requirements.

2. The Commission shall, in accordance with Article 10 of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards for the product accessibility requirements set out in Annex I. The Commission shall submit the first such draft request to the relevant committee by 28 June 2021.

3. The Commission may adopt implementing acts establishing technical specifications that meet the accessibility requirements of this Directive where the following conditions have been fulfilled:

(a) no reference to harmonised standards is published in the *Official Journal of the European Union* in accordance with Regulation (EU) No 1025/2012; and

(b) either:

(i) the Commission has requested one or more European standardisation organisations to draft a harmonised standard and there are undue delays in the standardisation procedure or the request has not been accepted by any European standardisation organisations; or

(ii) the Commission can demonstrate that a technical specification respects the requirements laid down in Annex II of Regulation (EU) No 1025/2012, except for the requirement that the technical specifications should have been developed by a non-profit making organisation.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 27(2).

4. Products and services which are in conformity with the technical specifications or parts thereof shall be presumed to be in conformity with the accessibility requirements of this Directive in so far as those technical specifications or parts thereof cover those requirements.

CHAPTER VII

Conformity of products and CE marking

Article 16

EU declaration of conformity of products

1. The EU declaration of conformity shall state that the fulfilment of the applicable accessibility requirements has been demonstrated. Where as an exception, Article 14 has been used, the EU declaration of conformity shall state which accessibility requirements are subject to that exception.

2. The EU declaration of conformity shall have the model structure set out in Annex III to Decision No 768/2008/EC. It shall contain the elements specified in Annex IV to this Directive and shall be continuously updated. The requirements concerning the technical documentation shall avoid imposing any undue burden for microenterprises and SMEs. It shall be translated into the language or languages required by the Member State in which the product is placed or made available on the market.

3. Where a product is subject to more than one Union act requiring an EU declaration of conformity, a single EU declaration of conformity shall be drawn up in respect of all such Union acts. That declaration shall contain the identification of the acts concerned including the publication references.

4. By drawing up the EU declaration of conformity, the manufacturer shall assume responsibility for the compliance of the product with the requirements of this Directive.

Article 17

General principles of the CE marking of products

The CE marking shall be subject to the general principles set out in Article 30 of Regulation (EC) No 765/2008.

Article 18

Rules and conditions for affixing the CE marking

1. The CE marking shall be affixed visibly, legibly and indelibly to the product or to its data plate. Where that is not possible, or not warranted, on account of the nature of the product, it shall be affixed to the packaging and to the accompanying documents.

2. The CE marking shall be affixed before the product is placed on the market.

3. Member States shall build upon existing mechanisms to ensure correct application of the regime governing the CE marking and shall take appropriate action in the event of improper use of that marking.

CHAPTER VIII

Market surveillance of products and Union safeguard procedure

Article 19

Market surveillance of products

1. Article 15(3), Articles 16 to 19, Article 21, Articles 23 to 28 and Article 29(2) and (3) of Regulation (EC) No 765/2008 shall apply to products.

2. When carrying out market surveillance of products, the relevant market surveillance authorities shall, when the economic operator has relied on Article 14 of this Directive:

(a) check that the assessment referred to in Article 14 has been conducted by the economic operator;

(b) review that assessment and its results, including the correct use of the criteria set out in Annex VI; and

(c) check compliance with the applicable accessibility requirements.

3. Member States shall ensure that information held by market surveillance authorities concerning the compliance of economic operators with the applicable accessibility requirements of this Directive and the assessment provided for in Article 14, is made available to consumers upon request and in an accessible format, except where that information cannot be provided for reasons of confidentiality as provided for in Article 19(5) of Regulation (EC) No 765/2008.

Article 20

Procedure at national level for dealing with products not complying with the applicable accessibility requirements

1. Where the market surveillance authorities of one Member State have sufficient reason to believe that a product covered by this Directive does not comply with the applicable accessibility requirements, they shall carry out an evaluation in relation to the product concerned covering all requirements laid down in this Directive. The relevant economic operators shall fully cooperate with the market surveillance authorities for that purpose.

Where, in the course of the evaluation referred to in the first subparagraph, the market surveillance authorities find that the product does not comply with the requirements laid down in this Directive, they shall without delay require the relevant economic operator to take all appropriate corrective action to bring the product into compliance with those requirements within a reasonable period, commensurate with the nature of the non-compliance, as they may prescribe.

Market surveillance authorities shall require the relevant economic operator to withdraw the product from the market, within an additional reasonable period, only if the relevant economic operator has failed to take adequate corrective action within the period referred to in the second subparagraph.

Article 21 of Regulation (EC) No 765/2008 shall apply to the measures referred to in the second and third subparagraphs of this paragraph.

2. Where the market surveillance authorities consider that non-compliance is not restricted to their national territory, they shall inform the Commission and the other Member States of the results of the evaluation and of the actions which they have required the economic operator to take.

3. The economic operator shall ensure that all appropriate corrective action is taken in respect of all the products concerned that it has made available on the market throughout the Union.

4. Where the relevant economic operator does not take adequate corrective action within the period referred to in the third subparagraph of paragraph 1, the market surveillance authorities shall take all appropriate provisional measures to prohibit or restrict the product's being made available on their national markets or to withdraw the product from that market.

The market surveillance authorities shall inform the Commission and the other Member States, without delay, of those measures.

5. The information referred to in the second subparagraph of paragraph 4 shall include all available details, in particular the data necessary for the identification of the non-compliant product, the origin of the product, the nature of the non-compliance alleged and the accessibility requirements with which the product does not comply, the nature and duration of the national measures taken and the arguments put forward by the relevant economic operator. In particular, the market surveillance authorities shall indicate whether the non-compliance is due to either:

(a) the failure of the product to meet the applicable accessibility requirements; or

(b) the shortcomings in the harmonised standards or in the technical specifications referred to in Article 15 conferring a presumption of conformity.

6. Member States other than the Member State initiating the procedure under this Article shall without delay inform the Commission and the other Member States of any measures adopted and of any additional information at their disposal relating to the non-compliance of the product concerned, and, in the event of disagreement with the notified national measure, of their objections.

7. Where, within three months of receipt of the information referred to in the second subparagraph of paragraph 4, no objection has been raised by either a Member State or the Commission in respect of a provisional measure taken by a Member State, that measure shall be deemed justified.

8. Member States shall ensure that appropriate restrictive measures, such as withdrawal of the product from their market, are taken in respect of the product concerned without delay.

Article 21

Union safeguard procedure

1. Where, on completion of the procedure set out in Article 20(3) and (4), objections are raised against a measure taken by a Member State, or where the Commission has reasonable evidence to suggest that a national measure is contrary to Union law, the Commission shall without delay enter into consultation with the Member States and the relevant economic operator or operators and shall evaluate the national measure. On the basis of the results of that evaluation, the Commission shall decide whether the national measure is justified or not.

The Commission shall address its decision to all Member States and shall immediately communicate it to them and the relevant economic operator or operators.

2. Where the national measure referred to in paragraph 1 is considered justified, all Member States shall take the measures necessary to ensure that the non-compliant product is withdrawn from their market, and shall inform the Commission accordingly. Where the national measure is considered unjustified, the Member State concerned shall withdraw the measure.

3. Where the national measure referred to in paragraph 1 of this Article is considered justified and the non-compliance of the product is attributed to shortcomings in the harmonised standards referred to in point (b) of Article 20(5), the Commission shall apply the procedure provided for in Article 11 of Regulation (EU) No 1025/2012.

4. Where the national measure referred to in paragraph 1 of this Article is considered justified and the non-compliance of the product is attributed to shortcomings in the technical specifications referred to in point (b) of Article 20(5), the Commission shall, without delay, adopt implementing acts amending or repealing the technical specification concerned. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 27(2).

Article 22

Formal non-compliance

1. Without prejudice to Article 20, where a Member State makes one of the following findings, it shall require the relevant economic operator to put an end to the non-compliance concerned:

(a) the CE marking has been affixed in violation of Article 30 of Regulation (EC) No 765/2008 or of Article 18 of this Directive;

(b) the CE marking has not been affixed;

(c) the EU declaration of conformity has not been drawn up;

(d) the EU declaration of conformity has not been drawn up correctly;

(e) technical documentation is either not available or not complete;

(f) the information referred to in Article 7(6) or Article 9(4) is absent, false or incomplete;

(g) any other administrative requirement provided for in Article 7 or Article 9 is not fulfilled.

2. Where the non-compliance referred to in paragraph 1 persists, the Member State concerned shall take all appropriate measures to restrict or prohibit the product being made available on the market or to ensure that it is withdrawn from the market.

CHAPTER IX

Compliance of services

Article 23

Compliance of services

1. Member States shall establish, implement and periodically update adequate procedures in order to:

(a) check the compliance of services with the requirements of this Directive, including the assessment referred to in Article 14 for which Article 19(2) shall apply mutatis mutandis;

(b) follow up complaints or reports on issues relating to non-compliance of services with the accessibility requirements of this Directive;

(c) verify that the economic operator has taken the necessary corrective action.

2. Member States shall designate the authorities responsible for the implementation of the procedures referred to in paragraph 1 with respect to the compliance of services.

Member States shall ensure that the public is informed of the existence, responsibilities, identity, work and decisions of the authorities referred to in the first subparagraph. Those authorities shall make that information available in accessible formats upon request.

CHAPTER X

Accessibility requirements in other Union acts

Article 24

Accessibility under other Union acts

1. As regards the products and services referred to in Article 2 of this Directive, the accessibility requirements set out in Annex I thereto shall constitute mandatory accessibility requirements within the meaning of Article 42(1) of Directive 2014/24/EU and of Article 60(1) of Directive 2014/25/EU.

2. Any product or service, the features, elements or functions of which comply with the accessibility requirements set out in Annex I to this Directive in accordance with Section VI thereof shall be presumed to fulfil the relevant obligations set out in Union acts other than this Directive, as regards accessibility, for those features, elements or functions, unless otherwise provided in those other acts.

Article 25

Harmonised standards and technical specifications for other Union acts

Conformity with harmonised standards and technical specifications or parts thereof which are adopted in accordance with Article 15, shall create a presumption of compliance with Article 24 in so far as those standards and technical specifications or parts thereof meet the accessibility requirements of this Directive.

CHAPTER XI

Delegated acts, implementing powers and final provisions

Article 26

Exercise of the delegation

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

2. The power to adopt delegated acts referred to in Article 4(9) shall be conferred on the Commission for an indeterminate period of time from 27 June 2019.

The power to adopt delegated acts referred to in Article 12(3) and Article 14(7) shall be conferred on the Commission for a period of five years from 27 June 2019. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

3. The delegation of power referred to in Article 4(9), Article 12(3) and Article 14(7) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect on the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

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

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

6. A delegated act adopted pursuant to Article 4(9), Article 12(3) and Article 14(7) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 27

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 28

Working Group

The Commission shall establish a working group consisting of representatives of market surveillance authorities, authorities responsible for compliance of services and relevant stakeholders, including representatives of persons with disabilities organisations.

The working group shall:

(a) facilitate the exchange of information and best practices among the authorities and relevant stakeholders;

(b) foster cooperation between authorities and relevant stakeholders on matters relating to the implementation of this Directive to improve coherence in the application of the accessibility requirements of this Directive and to monitor closely the implementation of Article 14; and

(c) provide advice, in particular to the Commission, notably on the implementation of Article 4 and Article 14.

Article 29

Enforcement

1. Member States shall ensure that adequate and effective means exist to ensure compliance with this Directive.

2. The means referred to in paragraph 1 shall include:

(a) provisions whereby a consumer may take action under national law before the courts or before the competent administrative bodies to ensure that the national provisions transposing this Directive are complied with;

(b) provisions whereby public bodies or private associations, organisations or other legal entities which have a legitimate interest, in ensuring that this Directive is complied with, may engage under national law before the courts or before the competent administrative bodies either on behalf or in support of the complainant, with his or her approval, in any judicial or administrative procedure provided for the enforcement of obligations under this Directive.

3. This Article shall not apply to procurement procedures which are subject to Directive 2014/24/EU or Directive 2014/25/EU.

Article 30

Penalties

1. Member States shall lay down the rules on penalties applicable to infringements of national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented.

2. The penalties provided for shall be effective, proportionate and dissuasive. Those penalties shall also be accompanied by effective remedial action in case of non-compliance of the economic operator.

3. Member States shall, without delay, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.

4. Penalties shall take into account the extent of the non-compliance, including its seriousness, and the number of units of non-complying products or services concerned, as well as the number of persons affected.

5. This Article shall not apply to procurement procedures which are subject to Directive 2014/24/EU or Directive 2014/25/EU.

Article 31

Transposition

1. Member States shall adopt and publish, by 28 June 2022, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately communicate the text of those measures to the Commission.

2. They shall apply those measures from 28 June 2025.

3. By way of derogation from paragraph 2 of this Article, Member States may decide to apply the measures regarding the obligations set out in Article 4(8) at the latest from 28 June 2027.

4. When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

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

6. Member States using the possibility provided for in Article 4(4) shall communicate to the Commission the text of the main measures of national law which they adopt to that end and shall report to the Commission on the progress made in their implementation.

Article 32

Transitional measures

1. Without prejudice to paragraph 2 of this Article, Member States shall provide for a transitional period ending on 28 June 2030 during which service providers may continue to provide their services using products which were lawfully used by them to provide similar services before that date.

Service contracts agreed before 28 June 2025 may continue without alteration until they expire, but no longer than five years from that date.

2. Member States may provide that self-service terminals lawfully used by service providers for the provision of services before 28 June 2025 may continue to be used in the provision of similar services until the end of their economically useful life, but no longer than 20 years after their entry into use.

Article 33

Report and review

1. By 28 June 2030, and every five years thereafter, the Commission shall submit to the European Parliament, to the Council, to the European Economic and Social Committee and to the Committee of the Regions a report on the application of this Directive.

2. The reports shall, inter alia, address in the light of social, economic and technological developments the evolution of the accessibility of products and services, possible technology lock in or barriers to innovation and the impact of this Directive on economic operators and on persons with disabilities. The reports shall also assess whether the application of Article 4(4) has contributed to approximate diverging accessibility requirements of the built environment of passenger transport services, consumer banking services and customer service centres of shops of electronic communications service providers, where possible, with a view to allowing their progressive alignment to the accessibility requirements set out in Annex III.

The reports shall also assess if the application of this Directive, in particular its voluntary provisions, has contributed to approximate accessibility requirements of the built environment constituting works falling within the scope of Directive 2014/23/EU of the European Parliament and of the Council ([35]), Directive 2014/24/EU and Directive 2014/25/EU.

The reports shall also address the effects to the functioning of the internal market of the application of Article 14 of this Directive, including, where available, on the basis of information received in accordance with Article 14(8), as well as the exemptions for microenterprises. The reports shall conclude whether this Directive has achieved its objectives and whether it would be appropriate to include new products and services, or to exclude certain products or services from the scope of this Directive and they shall identify, where possible, areas for burden reduction with a view to a possible revision of this Directive.

The Commission shall, if necessary, propose appropriate measures which could include legislative measures.

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

3. Member States shall communicate to the Commission in due time all the information necessary for the Commission to draw up such reports.

4. The Commission's reports shall take into account the views of the economic stakeholders and relevant non-governmental organisations, including organisations of persons with disabilities.

Article 34

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

Article 35

This Directive is addressed to the Member States.

Done at Strasbourg, 17 April 2019.

For the European Parliament	*For the Council*
The President	*The President*
A. TAJANI	G. CIAMBA

ANNEX I

ACCESSIBILITY REQUIREMENTS FOR PRODUCTS AND SERVICES

Section I

General accessibility requirements related to all products covered by this directive in accordance with Article 2(1)

Products must be designed and produced in such a way as to maximise their foreseeable use by persons with disabilities and shall be accompanied where possible in or on the product by accessible information on their functioning and on their accessibility features.

1. Requirements on the provision of information:

   (a) the information on the use of the product provided on the product itself (labelling, instructions and warning) shall be:

      (i) made available via more than one sensory channel;

      (ii) presented in an understandable way;

      (iii) presented to users in ways they can perceive;

      (iv) presented in fonts of adequate size and suitable shape, taking into account foreseeable conditions of use, and using sufficient contrast, as well as adjustable spacing between letters, lines and paragraphs;

   (b) the instructions for use of a product, where not provided on the product itself but made available through the use of the product or through other means such as a website, including the accessibility functions of the product, how to activate them and their interoperability with assistive solutions shall be publicly available when the product is placed on the market and shall:

      (i) be made available via more than one sensory channel;

      (ii) be presented in an understandable way;

      (iii) be presented to users in ways they can perceive;

      (iv) be presented in fonts of adequate size and suitable shape, taking into account foreseeable conditions of use and using sufficient contrast, as well as adjustable spacing between letters, lines and paragraphs;

      (v) with regard to content, be made available in text formats that can be used for generating alternative assistive formats to be presented in different ways and via more than one sensory channel;

      (vi) be accompanied by an alternative presentation of any non-textual content;

      (vii) include a description of the user interface of the product (handling, control and feedback, input and output) which is provided in accordance with point 2; the description shall indicate for each of the points in point 2 whether the product provides those features;

      (viii) include a description of the functionality of the product which is provided by functions aiming to address the needs of persons with disabilities in accordance with point 2; the description shall indicate for each of the points in point 2 whether the product provides those features;

      (ix) include a description of the software and hardware interfacing of the product with assistive devices; the description shall include a list of those assistive devices which have been tested together with the product.

2. User interface and functionality design:

   The product, including its user interface, shall contain features, elements and functions, that allow persons with disabilities to access, perceive, operate, understand and control the product by ensuring that:

   (a) when the product provides for communication, including interpersonal communication, operation, information, control and orientation, it shall do so via more than one sensory channel; this shall include providing alternatives to vision, auditory, speech and tactile elements;

   (b) when the product uses speech it shall provide alternatives to speech and vocal input for communication, operation control and orientation;

(c) when the product uses visual elements it shall provide for flexible magnification, brightness and contrast for communication, information and operation, as well as ensure interoperability with programmes and assistive devices to navigate the interface;

(d) when the product uses colour to convey information, indicate an action, require a response or identify elements, it shall provide an alternative to colour;

(e) when the product uses audible signals to convey information, indicate an action, require a response or identify elements, it shall provide an alternative to audible signals;

(f) when the product uses visual elements it shall provide for flexible ways of improving vision clarity;

(g) when the product uses audio it shall provide for user control of volume and speed, and enhanced audio features including the reduction of interfering audio signals from surrounding products and audio clarity;

(h) when the product requires manual operation and control, it shall provide for sequential control and alternatives to fine motor control, avoiding the need for simultaneous controls for manipulation, and shall use tactile discernible parts;

(i) the product shall avoid modes of operation requiring extensive reach and great strength;

(j) the product shall avoid triggering photosensitive seizures;

(k) the product shall protect the user's privacy when he or she uses the accessibility features;

(l) the product shall provide an alternative to biometrics identification and control;

(m) the product shall ensure the consistency of the functionality and shall provide enough, and flexible amounts of, time for interaction;

(n) the product shall provide software and hardware for interfacing with the assistive technologies;

(o) the product shall comply with the following sector-specific requirements:

(i) self-service terminals:

— shall provide for text-to-speech technology;

— shall allow for the use of personal headsets;

— where a timed response is required, shall alert the user via more than one sensory channel;

— shall give the possibility to extend the time given;

— shall have an adequate contrast and tactilely discernible keys and controls when keys and controls are available;

— shall not require an accessibility feature to be activated in order to enable a user who needs the feature to turn it on;

— when the product uses audio or audible signals, it shall be compatible with assistive devices and technologies available at Union level, including hearing technologies such as hearing aids, telecoils, cochlear implants and assistive listening devices;

(ii) e-readers shall provide for text-to-speech technology;

(iii) consumer terminal equipment with interactive computing capability, used for the provision of electronic communications services:

— shall, when such products have text capability in addition to voice, provide for the handling of real time text and support high fidelity audio;

— shall, when they have video capabilities in addition to or in combination with text and voice, provide for the handling of total conversation including synchronised voice, real time text, and video with a resolution enabling sign language communication;

— shall ensure effective wireless coupling to hearing technologies;

— shall avoid interferences with assistive devices;

(iv) consumer terminal equipment with interactive computing capability, used for accessing audio visual media services shall make available to persons with disabilities the accessibility components provided by the audiovisual media service provider, for user access, selection, control, and personalisation and for transmission to assistive devices.

3. Support services:

Where available, support services (help desks, call centres, technical support, relay services and training services) shall provide information on the accessibility of the product and its compatibility with assistive technologies, in accessible modes of communication.

Section II

Accessibility requirements related to products in Article 2(1), except for the self-service terminals referred to in Article 2(1)(b)

In addition to the requirements of Section I, the packaging and instructions of products covered by this Section shall be made accessible, in order to maximise their foreseeable use by persons with disabilities. This means that:

(a) the packaging of the product including the information provided in it (e.g. about opening, closing, use, disposal), including, when provided, information about the accessibility characteristics of the product, shall be made accessible; and, when feasible, that accessible information shall be provided on the package;

(b) the instructions for the installation and maintenance, storage and disposal of the product not provided on the product itself but made available through other means, such as a website, shall be publicly available when the product is placed on the market and shall comply with the following requirements:

(i) be available via more than one sensory channel;

(ii) be presented in an understandable way;

(iii) be presented to users in ways they can perceive;

(iv) be presented in fonts of adequate size and suitable shape, taking into account foreseeable conditions of use, and using sufficient contrast, as well as adjustable spacing between letters, lines and paragraphs;

(v) content of instructions shall be made available in text formats that can be used for generating alternative assistive formats to be presented in different ways and via more than one sensory channel; and

(vi) instructions containing any non-textual content shall be accompanied by an alternative presentation of that content.

Section III

General accessibility requirements related to all services covered by this Directive in accordance with Article 2(2)

The provision of services in order to maximise their foreseeable use by persons with disabilities, shall be achieved by:

(a) ensuring the accessibility of the products used in the provision of the service, in accordance with Section I of this Annex and, where applicable, Section II thereof;

(b) providing information about the functioning of the service, and where products are used in the provision of the service, its link to these products as well as information about their accessibility characteristics and interoperability with assistive devices and facilities:

(i) making the information available via more than one sensory channel;

(ii) presenting the information in an understandable way;

(iii) presenting the information to users in ways they can perceive;

(iv) making the information content available in text formats that can be used to generate alternative assistive formats to be presented in different ways by the users and via more than one sensory channel;

(v) presenting in fonts of adequate size and suitable shape, taking into account foreseeable conditions of use and using sufficient contrast, as well as adjustable spacing between letters, lines and paragraphs;

(vi) supplementing any non-textual content with an alternative presentation of that content; and

(vii) providing electronic information needed in the provision of the service in a consistent and adequate way by making it perceivable, operable, understandable and robust;

(c) making websites, including the related online applications, and mobile device-based services, including mobile applications, accessible in a consistent and adequate way by making them perceivable, operable, understandable and robust;

(d) where available, support services (help desks, call centres, technical support, relay services and training services) providing information on the accessibility of the service and its compatibility with assistive technologies, in accessible modes of communication.

Section IV

Additional accessibility requirements related to specific services

The provision of services in order to maximise their foreseeable use by persons with disabilities, shall be achieved by including functions, practices, policies and procedures and alterations in the operation of the service targeted to address the needs of persons with disabilities and ensure interoperability with assistive technologies:

(a) Electronic communications services, including emergency communications referred to in Article 109(2) of Directive (EU) 2018/1972:

(i) providing real time text in addition to voice communication;

(ii) providing total conversation where video is provided in addition to voice communication;

(iii) ensuring that emergency communications using voice, text (including real time text) is synchronised and where video is provided is also synchronised as total conversation and is transmitted by the electronic communications service providers to the most appropriate PSAP.

(b) Services providing access to audiovisual media services:

(i) providing electronic programme guides (EPGs) which are perceivable, operable, understandable and robust and provide information about the availability of accessibility;

(ii) ensuring that the accessibility components (access services) of the audiovisual media services such as subtitles for the deaf and hard of hearing, audio description, spoken subtitles and sign language interpretation are fully transmitted with adequate quality for accurate display, and synchronised with sound and video, while allowing for user control of their display and use.

(c) Air, bus, rail and waterborne passenger transport services except for urban and suburban transport services and regional transport services:

(i) ensuring the provision of information on the accessibility of vehicles, the surrounding infrastructure and the built environment and on assistance for persons with disabilities;

(ii) ensuring the provision of information about smart ticketing (electronic reservation, booking of tickets, etc.), real-time travel information (timetables, information about traffic disruptions, connecting services, onwards travel with other transport modes, etc.), and additional service information (e.g. staffing of stations, lifts that are out of order or services that are temporarily unavailable).

(d) Urban and suburban transport services and regional transport services: ensuring the accessibility of self-service terminals used in the provision of the service in accordance with Section I of this Annex.

(e) Consumer banking services:

(i) providing identification methods, electronic signatures, security, and payment services which are perceivable, operable, understandable and robust;

(ii) ensuring that the information is understandable, without exceeding a level of complexity superior to level B2 (upper intermediate) of the Council of Europe's Common European Framework of Reference for Languages.

(f) E-books:

(i) ensuring that, when an e-book contains audio in addition to text, it then provides synchronised text and audio;

(ii) ensuring that e-book digital files do not prevent assistive technology from operating properly;

(iii) ensuring access to the content, the navigation of the file content and layout including dynamic layout, the provision of the structure, flexibility and choice in the presentation of the content;

(iv) allowing alternative renditions of the content and its interoperability with a variety of assistive technologies, in such a way that it is perceivable, understandable, operable and robust;

(v) making them discoverable by providing information through metadata about their accessibility features;

(vi) ensuring that digital rights management measures do not block accessibility features.

(g) E-Commerce services:

(i) providing the information concerning accessibility of the products and services being sold when this information is provided by the responsible economic operator;

(ii) ensuring the accessibility of the functionality for identification, security and payment when delivered as part of a service instead of a product by making it perceivable, operable, understandable and robust;

(iii) providing identification methods, electronic signatures, and payment services which are perceivable, operable, understandable and robust.

Section V

Specific accessibility requirements related to the answering of emergency communications to the single European emergency number '112' by the most appropriate PSAP

In order to maximise their foreseeable use by persons with disabilities, the answering of emergency communications to the single European emergency number '112' by the most appropriate PSAP, shall be achieved by including functions, practices, policies and procedures and alterations targeted to address the needs of persons with disabilities.

Emergency communications to the single European emergency number '112' shall be appropriately answered, in the manner best suited to the national organisation of emergency systems, by the most appropriate PSAP using the same communication means as received, namely by using synchronised voice and text (including real time text), or, where video is provided, voice, text (including real time text) and video synchronised as total conversation.

Section VI

Accessibility requirements for features, elements or functions of products and services in accordance with Article 24(2)

The presumption to fulfil the relevant obligations set out in other Union acts concerning features, elements or functions of products and services requires the following:

1. Products:

(a) the accessibility of the information concerning the functioning and accessibility features related to products complies with the corresponding elements set out in point 1 of Section I of this Annex, namely information on the use of the product provided on the product itself and the instructions for use of a product, not provided in the product itself but made available through the use of the product or other means such as a website;

(b) the accessibility of features, elements and functions of the user interface and the functionality design of products complies with the corresponding accessibility requirements of such user interface or functionality design set out in point 2 of Section I of this Annex;

(c) the accessibility of the packaging, including the information provided in it and instructions for the installation and maintenance, storage and disposal of the product not provided in the product itself but made available through other means such as a website, except for self-service terminals complies with the corresponding accessibility requirements set out in Section II of this Annex.

2. Services:

the accessibility of the features, elements and functions of services complies with the corresponding accessibility requirements for those features, elements and functions set out in the services-related Sections of this Annex.

Section VII

Functional performance criteria

In order to maximise the foreseeable use by persons with disabilities, when the accessibility requirements, set out in Sections I to VI of this Annex, do not address one or more functions of the design and production of products or the provision of services those functions or means shall be accessible by complying with the related functional performance criteria.

Those functional performance criteria may only be used as an alternative to one or more specific technical requirements, when these are referred to in the accessibility requirements, if and only if the application of the relevant functional performance criteria complies with the accessibility requirements and it determines that the design and production of products and the provision of services results in equivalent or increased accessibility for the foreseable use by persons with disabilities.

(a) Usage without vision

Where the product or service provides visual modes of operation, it shall provide at least one mode of operation that does not require vision.

(b) Usage with limited vision

Where the product or service provides visual modes of operation, it shall provide at least one mode of operation that enables users to operate the product with limited vision.

(c) Usage without perception of colour

Where the product or service provides visual modes of operation, it shall provide at least one mode of operation that does not require user perception of colour.

(d) Usage without hearing

Where the product or service provides auditory modes of operation, it shall provide at least one mode of operation that does not require hearing.

(e) Usage with limited hearing

Where the product or service provides auditory modes of operation, it shall provide at least one mode of operation with enhanced audio features that enables users with limited hearing to operate the product.

(f) Usage without vocal capability

Where the product or service requires vocal input from users, it shall provide at least one mode of operation that does not require vocal input. Vocal input includes any orally-generated sounds like speech, whistles or clicks.

(g) Usage with limited manipulation or strength

Where the product or service requires manual actions, it shall provide at least one mode of operation that enables users to make use of the product through alternative actions not requiring fine motor control and manipulation, hand strength or operation of more than one control at the same time.

(h) Usage with limited reach

The operational elements of products shall be within reach of all users. Where the product or service provides a manual mode of operation, it shall provide at least one mode of operation that is operable with limited reach and limited strength.

(i) Minimising the risk of triggering photosensitive seizures

Where the product provides visual modes of operation, it shall avoid modes of operation that trigger photosensitive seizures.

(j) Usage with limited cognition

The product or service shall provide at least one mode of operation incorporating features that make it simpler and easier to use.

(k) Privacy

Where the product or service incorporates features that are provided for accessibility, it shall provide at least one mode of operation that maintains privacy when using those features that are provided for accessibility.

ANNEX II

INDICATIVE NON-BINDING EXAMPLES OF POSSIBLE SOLUTIONS THAT CONTRIBUTE TO MEETING THE ACCESSIBILITY REQUIREMENTS IN ANNEX I

SECTION I:

EXAMPLES RELATED TO GENERAL ACCESSIBILITY REQUIREMENTS FOR ALL PRODUCTS COVERED BY THIS DIRECTIVE IN ACCORDANCE WITH ARTICLE 2(1)

REQUIREMENTS IN SECTION I OF ANNEX I	EXAMPLES
1. The provision of information	
(a)	
(i)	Providing visual and tactile information or visual and auditory information indicating the place where to introduce a card in a self-service terminal so that blind persons and deaf persons can use the terminal.
(ii)	Using the same words in a consistent manner, or in a clear and logical structure, so that persons with intellectual disabilities can better understand it.
(iii)	Providing tactile relief format or sound in addition to a text warning so that blind persons can perceive it.
(iv)	Allowing that text can be read by persons who are visually impaired.
(b)	
(i)	Providing electronic files which can be read by a computer using screen readers so that blind persons can use the information.
(ii)	Using the same words in a consistent manner, or in a clear and logical structure, so that persons with intellectual disabilities can better understand them.
(iii)	Providing subtitles when video instructions are provided.
(iv)	Allowing that the text can be read by persons who are visually impaired.
(v)	Printing in Braille, so that a blind person can use them.
(vi)	Accompanying a diagram with a text description identifying the main elements or describing key actions.
(vii)	No example provided
(viii)	No example provided
(ix)	Including a socket and software in automated teller machines which will allow the plugging of a headphone which will receive the text on the screen in the form of sound.

2. User interface and functionality design	
(a)	Providing instructions in the form of voice and text, or by incorporating tactile signs in a keypad, so that persons who are blind or hard of hearing can interact with the product.
(b)	Offering in a self-service terminal in addition to the spoken instructions, for example, instructions in the form of text or images so that deaf persons can also perform the action required
(c)	Allowing users to enlarge a text, to zoom in on a particular pictogram or to increase the contrast, so that persons who are visually impaired can perceive the information.
(d)	In addition of giving a choice to press the green or the red button for selecting an option, providing in written on the buttons what the options are, in order to allow person who are colour blind to make the choice.
(e)	When a computer gives an error signal, providing a written text or an image indicating the error, so as to allow deaf persons to apprehend that an error is occurring.
(f)	Allowing for additional contrast in foreground images so that persons who have low vision can see them.
(g)	Allowing the user of a telephone to select the volume of the sound and reduce the interference with hearing aids so that persons who are hard of hearing can use the telephone.
(h)	Making touch screen buttons bigger and well separated so that persons with tremor can press them.
(i)	Ensuring that buttons to be pressed do not require much force so that persons who have motor impairments can use them.
(j)	Avoiding flickering images so that persons who get seizures are not at risk.
(k)	Allowing the use of headphones when spoken information is provided by automated teller machines.
(l)	As an alternative to fingerprint recognition, allowing users who cannot use their hands to select a password for locking and unlocking a phone.
(m)	Ensuring that the software reacts in a predictable way when a particular action is performed and providing enough time to enter a password so that is easy to use for persons with intellectual disabilities.
(n)	Offering a connection with a refreshable Braille display so that blind persons can use the computer.
(o)	Examples of sector-specific requirements
(i)	No example provided
(ii)	No example provided
(iii) First indent	Providing that a mobile phone should be able to handle real time text conversations so that persons who are hard of hearing can exchange information in an interactive way.
(iii) Fourth indent	Allowing the simultaneous use of video to display sign language and text to write a message, so that two deaf persons can communicate with each other or with a hearing person.

(iv)	Ensuring that subtitles are transmitted through the set top box for their use by deaf persons.

3. Support services: No example provided

SECTION II:

EXAMPLES RELATED TO ACCESSIBILITY REQUIREMENTS FOR PRODUCTS IN ARTICLE 2(1), EXCEPT FOR THE SELF-SERVICE TERMINALS REFERRED TO IN ARTICLE 2(1)(b)

REQUIREMENTS IN SECTION II OF ANNEX I	EXAMPLES
Packaging and instructions of products	
(a)	Indicating in the packaging that the phone contains accessibility features for persons with disabilities.
(b)	
(i)	Providing electronic files which can be read by a computer using screen readers so that blind persons can use the information.
(ii)	Using the same words in a consistent manner, or in a clear and logical structure, so that persons with intellectual disabilities can better understand it.
(iii)	Providing tactile relief format or sound when a text warning is present so that blind persons receive the warning.
(iv)	Providing that the text can be read by persons who are visually impaired.
(v)	Printing in Braille, so that a blind person can read it.
(vi)	Supplementing a diagram with a text description identifying the main elements or describing key actions.

SECTION III:

EXAMPLES RELATED TO GENERAL ACCESSIBILITY REQUIREMENTS FOR ALL SERVICES COVERED BY THIS DIRECTIVE IN ACCORDANCE WITH ARTICLE 2(2)

REQUIREMENTS IN SECTION III OF ANNEX I	EXAMPLES
The provision of services	
(a)	No example provided
(b)	
(i)	Providing electronic files which can be read by a computer using screen readers so that blind persons can use the information.
(ii)	Using the same words in a consistent manner or in a clear and logical structure so that persons with intellectual disabilities can better understand it.
(iii)	Including subtitles when a video with instructions is provided.

(iv)	Providing that a blind person can use a file by printing it in Braille.
(v)	Providing that the text can be read by persons who are visually impaired.
(vi)	Supplementing a diagram with a text description identifying the main elements or describing key actions.
(vii)	When a service provider offers a USB-key containing information about the service, providing that information is accessible.
(c)	Providing text description of pictures, making all functionality available from a keyboard, giving users enough time to read, making content appear and operate in a predictable way, and providing compatibility with assistive technologies, so that persons with diverse disabilities can read and interact with a website.
(d)	No example provided

SECTION IV:

EXAMPLES RELATED TO ADDITIONAL ACCESSIBILITY REQUIREMENTS FOR SPECIFIC SERVICES

REQUIREMENTS IN SECTION IV OF ANNEX I	EXAMPLES
Specific services	
(a)	
(i)	Providing that persons who are hard of hearing could write and receive text in an interactive manner and in real time.
(ii)	Providing that deaf persons can use sign language to communicate among themselves.
(iii)	Providing that a person who has speech and hearing impairments and chooses to use a combination of text, voice and video, knows that the communication is transmitted through the network to an emergency service.
(b)	
(i)	Providing that a blind person can select programmes on the television.
(ii)	Supporting the possibility to select, personalise and display 'access services' such as subtitles for deaf persons or persons who are hard of hearing, audio description, spoken subtitles and sign language interpretation, by providing means for effective wireless coupling to hearing technologies or by providing user controls to activate 'access services' for audiovisual media services at the same level of prominence as the primary media controls.
(c)	
(i)	No example provided
(ii)	No example provided
(d)	No example provided
(e)	
(i)	Making the identification dialogues on a screen readable by screen readers so that blind persons can use them.

(ii)	No example provided
(f)	
(i)	Providing that a person with dyslexia can read and hear the text at the same time.
(ii)	Enabling synchronized text and audio output or by enabling a refreshable Braille transcript.
(iii)	Providing that a blind person can access the index or change chapters.
(iv)	No example provided
(v)	Ensuring that information on their accessibility features is available in the electronic file so that persons with disabilities can be informed.
(vi)	Ensuring that there is no blocking, for example that technical protection measures, rights management information or interoperability issues do not prevent the text from being read aloud by the assistive devices, so that blind users can read the book.
(g)	
(i)	Ensuring that available information on the accessibility features of a product is not deleted.
(ii)	Making the payment service user interface available by voice so that blind persons can make online purchases independently.
(iii)	Making the identification dialogues on a screen readable by screen readers so that blind persons can use them.

ANNEX III

ACCESSIBILITY REQUIREMENTS FOR THE PURPOSE OF ARTICLE 4(4) CONCERNING THE BUILT ENVIRONMENT WHERE THE SERVICES UNDER THE SCOPE OF THIS DIRECTIVE ARE PROVIDED

In order to maximise the foreseeable use in an independent manner by persons with disabilities of the built environment in which a service is provided and which is under the responsibility of the service provider, as referred to in Article 4(4), the accessibility of areas intended for public access shall include the following aspects:

(a) use of related outdoor areas and facilities;

(b) approaches to buildings;

(c) use of entrances;

(d) use of paths in horizontal circulation;

(e) use of paths in vertical circulation;

(f) use of rooms by the public;

(g) use of equipment and facilities used in the provision of the service;

(h) use of toilets and sanitary facilities;

(i) use of exits, evacuation routes and concepts for emergency planning;

(j) communication and orientation via more than one sensory channel;

(k) use of facilities and buildings for their foreseeable purpose;

(l) protection from hazards in the environment indoors and outdoors.

ANNEX IV

CONFORMITY ASSESSMENT PROCEDURE – PRODUCTS

1. Internal production control

Internal production control is the conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2, 3 and 4 of this Annex, and ensures and declares on its sole responsibility that the product concerned satisfy the appropriate requirements of this Directive.

2. Technical documentation

The manufacturer shall establish the technical documentation. The technical documentation shall make it possible to assess the conformity of the product to the relevant accessibility requirements referred to in Article 4 and, in case the manufacturer relied on Article 14, to demonstrate that relevant accessibility requirements would introduce a fundamental alteration or impose a disproportionate burden. The technical documentation shall specify only the applicable requirements and cover, as far as relevant for the assessment, the design, manufacture and operation of the product.

The technical documentation shall, wherever applicable, contain at least the following elements:

(a) a general description of the product;

(b) a list of the harmonised standards and technical specifications the references of which have been published in the *Official Journal of the European Union*, applied in full or in part, and descriptions of the solutions adopted to meet the relevant accessibility requirements referred to in Article 4 where those harmonised standards or technical specifications have not been applied; in the event of partly applied harmonised standards or technical specifications, the technical documentation shall specify the parts which have been applied.

3. Manufacturing

The manufacturer shall take all measures necessary so that the manufacturing process and its monitoring ensure compliance of the products with the technical documentation referred to in point 2 of this Annex and with the accessibility requirements of this Directive.

4. CE marking and EU declaration of conformity

4.1. The manufacturer shall affix the CE marking referred to in this Directive to each individual product that satisfies the applicable requirements of this Directive.

4.2. The manufacturer shall draw up a written EU declaration of conformity for a product model. The EU declaration of conformity shall identify the product for which it has been drawn up.

A copy of the EU declaration of conformity shall be made available to the relevant authorities upon request.

5. Authorised representative

The manufacturer's obligations set out in point 4 may be fulfilled by its authorised representative, on its behalf and under its responsibility, provided that they are specified in the mandate.

ANNEX V

INFORMATION ON SERVICES MEETING ACCESSIBILITY REQUIREMENTS

1. The service provider shall include the information assessing how the service meets the accessibility requirements referred to in Article 4 in the general terms and conditions, or equivalent document. The information shall describe the applicable requirements and cover, as far as relevant for the assessment the design and the operation of the service. In addition to the consumer information requirements of Directive 2011/83/EU, the information shall, where applicable, contain the following elements:

   (a) a general description of the service in accessible formats;

   (b) descriptions and explanations necessary for the understanding of the operation of the service;

   (c) a description of how the relevant accessibility requirements set out in Annex I are met by the service.

2. To comply with point 1 of this Annex the service provider may apply in full or in part the harmonised standards and technical specifications, for which references have been published in the *Official Journal of the European Union*.

3. The service provider shall provide information demonstrating that the service delivery process and its monitoring ensure compliance of the service with point 1 of this Annex and with the applicable requirements of this Directive.

ANNEX VI

CRITERIA FOR ASSESSMENT OF DISPROPORTIONATE BURDEN

Criteria to carry out and document the assessment:

1. Ratio of the net costs of compliance with accessibility requirements to the overall costs (operating and capital expenditures) of manufacturing, distributing or importing the product or providing the service for the economic operators.

   Elements to use to assess the net costs of compliance with accessibility requirements:

   (a) criteria related to one-off organisational costs to take into account in the assessment:

      (i) costs related to additional human resources with accessibility expertise;

      (ii) costs related to training human resources and acquiring competences on accessibility;

      (iii) costs of development of a new process for including accessibility in the product development or service provision;

      (iv) costs related to development of guidance material on accessibility;

      (v) one-off costs of understanding the legislation on accessibility;

   (b) criteria related to on-going production and development costs to take into account in the assessment:

      (i) costs related to the design of the accessibility features of the product or service;

      (ii) costs incurred in the manufacturing processes;

      (iii) costs related to testing the product or service for accessibility;

      (iv) costs related to establishing documentation.

2. The estimated costs and benefits for the economic operators, including production processes and investments, in relation to the estimated benefit for persons with disabilities, taking into account the amount and frequency of use of the specific product or service.

3. Ratio of the net costs of compliance with accessibility requirements to the net turnover of the economic operator.

   Elements to use to assess the net costs of compliance with accessibility requirements:

   (a) criteria related to one-off organisational costs to take into account in the assessment:

      (i) costs related to additional human resources with accessibility expertise;

      (ii) costs related to training human resources and acquiring competences on accessibility;

      (iii) costs of development of a new process for including accessibility in the product development or service provision;

      (iv) costs related to development of guidance material on accessibility;

      (v) one off costs of understanding the legislation on accessibility;

   (b) criteria related to on-going production and development costs to take into account in the assessment:

      (i) costs related to the design of the accessibility features of the product or service;

      (ii) costs incurred in the manufacturing processes;

      (iii) costs related to testing the product or service for accessibility;

      (iv) costs related to establishing documentation.

DIRECTIVE (EU) 2019/883 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 17 April 2019

on port reception facilities for the delivery of waste from ships, amending Directive 2010/65/EU and repealing Directive 2000/59/EC

(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]),

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

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

Whereas:

(1) The Union's maritime policy aims to ensure a high level of safety and environmental protection. This can be achieved through compliance with international conventions, codes and resolutions while maintaining the freedom of navigation as provided for by the United Nations Convention on the Law of the Sea ('UNCLOS').

(2) The United Nations Sustainable Development Goal 14 calls attention to the threats of marine and nutrient pollution, resource depletion and climate change, all of which are caused primarily by human actions. Those threats place further pressure on environmental systems, like biodiversity and natural infrastructure, while creating global socioeconomic problems, including health, safety and financial risks. The Union must work to protect marine species and to support the people who depend on oceans, whether it be for employment, resources or leisure.

(3) The International Convention for the Prevention of Pollution from Ships ('MARPOL Convention') provides for general prohibitions on discharges from ships at sea, but also regulates the conditions under which certain types of waste can be discharged into the marine environment. The MARPOL Convention requires contracting Parties to ensure the provision of adequate reception facilities in ports.

(4) The Union has pursued the implementation of parts of the MARPOL Convention through Directive 2000/59/EC of the European Parliament and the Council ([4]), by following a port-based approach. Directive 2000/59/EC aims to reconcile the interests of smooth operation of maritime transport with the protection of the marine environment.

(5) In the last two decades, the MARPOL Convention and its Annexes have been the object of important amendments, which have put in place stricter norms and prohibitions for the discharges of waste from ships at sea.

(6) Annex VI to the MARPOL Convention introduced discharge norms for new waste categories, in particular the residues from exhaust gas cleaning systems, consisting of both sludge and bleed-off water. Those waste categories should be included in the scope of this Directive.

([1]) OJ C 283, 10.8.2018, p. 61.
([2]) OJ C 461, 21.12.2018, p. 220.
([3]) Position of the European Parliament of 13 March 2019 (not yet published in the Official Journal) and decision of the Council of 9 April 2019.
([4]) Directive 2000/59/EC of the European Parliament and the Council of 27 November 2000 on port reception facilities for ship-generated waste and cargo residues (OJ L 332, 28.12.2000, p. 81).

(7) Member States should continue to work at International Maritime Organization ('IMO') level for a comprehensive consideration of the environmental impacts of wastewater discharges from open loop scrubbers, including for measures to counter possible impacts.

(8) Member States should be encouraged to take appropriate measures in accordance with Directive 2000/60/EC of the European Parliament and of the Council ([5]), including discharge bans for wastewater from open loop scrubbers and certain cargo residues in their territorial waters.

(9) On 1 March 2018, the IMO adopted the revised Consolidated Guidance for port reception facility providers and users (MEPC.1/Circ. 834/Rev.1) ('the IMO Consolidated Guidance'), which includes standard formats for waste notification, for the waste delivery receipt and for reporting alleged inadequacies of port reception facilities, as well as waste reception facility reporting requirements.

(10) Despite those regulatory developments, discharges of waste at sea still occur at substantial environmental, social and economic costs. This is due to a combination of factors, namely adequate port reception facilities not always being available in ports, enforcement often being insufficient and there being a lack of incentives to deliver the waste onshore.

(11) Directive 2000/59/EC has contributed to increasing the volumes of waste being delivered to port reception facilities, inter alia, by ensuring that ships contribute to the costs of those facilities, irrespective of their actual use of those facilities, and as such has been instrumental in reducing waste discharges at sea, as was revealed in the evaluation of that Directive carried out in the framework of the Regulatory Fitness and Performance programme ('REFIT Evaluation').

(12) The REFIT Evaluation has also demonstrated that Directive 2000/59/EC has not been fully effective due to inconsistencies with the MARPOL Convention framework. In addition, Member States have developed different interpretations of the key concepts in that Directive, such as adequacy of the facilities, advance waste notification, the mandatory delivery of waste to port reception facilities and exemptions for ships in scheduled traffic. The REFIT Evaluation called for more harmonisation of those concepts and full alignment with the MARPOL Convention in order to avoid unnecessary administrative burden on both ports and port users.

(13) In order to align Directive 2005/35/EC of the European Parliament and of the Council ([6]) to the relevant MARPOL Convention provisions on discharge norms, the Commission should assess the desirability of a review of that Directive, in particular through an extension of its scope.

(14) Union maritime policy should aim at a high level of protection of the marine environment taking into account the diversity of the maritime areas of the Union. It should be based on the principles that preventive action should be taken and that damage to the marine environment should, as a priority, be rectified at source and that the polluter should pay.

(15) This Directive should be instrumental for the application of the main environmental legislation and principles in the context of ports and the management of waste from ships. In particular, Directives 2008/56/EC ([7]) and 2008/98/EC ([8]) of the European Parliament and the Council are relevant instruments in this regard.

(16) Directive 2008/98/EC lays down the main waste management principles, including the 'polluter pays' principle and the waste hierarchy, which calls for the reuse and recycling of waste over other forms of waste recovery and disposal and requires the establishment of systems for the separate collection of waste. In addition, the extended producer responsibility concept is a guiding principle of Union waste law, on the basis of which producers are responsible for the environmental impacts of their products throughout the life-cycle of those products. Those obligations also apply to the management of waste from ships.

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

([6]) Directive 2005/35/EC of the European Parliament and of the Council of 7 September 2005 on ship-source pollution and on the introduction of penalties, including criminal penalties, for pollution offences (OJ L 255, 30.9.2005, p. 11).

([7]) Directive 2008/56/EC of the European Parliament and of the Council of 17 June 2008 establishing a framework for community action in the field of marine environmental policy (Marine Strategy Framework Directive) (OJ L 164, 25.6.2008, p. 19).

([8]) Directive 2008/98/EC of the European Parliament and of the Council of 19 November 2008 on waste and repealing certain Directives (OJ L 312, 22.11.2008, p. 3).

(17) Separate collection of waste from ships, including derelict fishing gear, is necessary to ensure its further recovery to enable it to be prepared for reuse or recycling in the downstream waste management chain and to prevent it from causing damage to marine wildlife and environments. Waste is often segregated on-board ships in accordance with international norms and standards, and Union law should ensure that these efforts of on-board waste segregation are not undermined by a lack of arrangements for separate collection on shore.

(18) Every year a substantial amount of plastic enters the seas and oceans in the Union. Although, in most sea areas, the majority of marine litter originates from land-based activities, the shipping industry, including the fishing and recreational sectors, is also an important contributor, with discharges of waste, including plastic and derelict fishing gear, going directly into the sea.

(19) Directive 2008/98/EC calls on Member States to halt the generation of marine litter as a contribution towards the United Nations Sustainable Development Goal to prevent and significantly reduce marine pollution of all kinds.

(20) The Commission Communication of 2 December 2015 entitled 'Closing the loop – An EU action plan for the Circular Economy' acknowledged the specific role Directive 2000/59/EC had to play in this respect, by ensuring the availability of adequate facilities for the reception of waste, and providing for both the right level of incentives and the enforcement of the delivery of waste to the on-shore facilities.

(21) Offshore installations are one of the sea-based sources of marine litter. For that reason, Member States should adopt measures as appropriate on waste delivery from offshore installations flying their flag or operating in their waters, or both, and ensure compliance with the stringent discharge norms applicable to offshore installations laid down in the MARPOL Convention.

(22) Waste, in particular plastic waste, from rivers is one of the main contributors to marine litter, which includes discharges from inland waterway vessels. Those vessels should therefore be subject to stringent discharge and delivery norms. Nowadays, those rules are laid down by the relevant River Commission. However, inland ports are covered by Union waste law. To continue the efforts of harmonising the legislative framework for Union inland waterways, the Commission is invited to evaluate a Union regime for discharge and delivery norms of inland waterway vessels, taking into account the Convention on the collection, deposit and reception of waste produced during navigation on the Rhine and inland waterways of 9 September 1996 (CDNI).

(23) Council Regulation (EC) No 1224/2009 ([9]) requires Union fishing vessels to have the equipment on board to retrieve lost gear. In cases where gear is lost, the master of the vessel is to attempt to retrieve it as soon as possible. If the lost gear cannot be retrieved, the master of the fishing vessel is to inform the authorities of its flag Member State within 24 hours. The flag Member State has then to inform the competent authority of the coastal Member State. The information includes the external identification number and the name of the fishing vessel, the type and the position of lost gear as well as the measures that were undertaken to retrieve it. Fishing vessels below 12 metres can be exempted. Under the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 1224/2009, the reporting by the fishing vessel is to be done in an electronic logbook, and Member States are required to collect and record the information concerning lost gear and provide it to the Commission upon request. The information collected and available in the waste delivery receipts on passively fished waste in line with this Directive could also be reported in this way.

(24) In accordance with the International Convention for the Control and Management of Ships' Ballast Water and Sediments, which was adopted on 13 February 2004 by IMO and which entered into force on 8 September 2017, all ships are obliged to carry out ballast water management procedures according to IMO standards, and ports and terminals designated for the cleaning and repair of ballast water tanks are required to provide adequate facilities for the reception of sediments.

([9]) 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 (OJ L 343, 22.12.2009, p. 1).

(25) A port reception facility is considered to be adequate if it is able to meet the needs of the ships normally using the port without causing undue delay, as also specified in the IMO Consolidated Guidance and the IMO Guidelines for ensuring the adequacy of port waste reception facilities (Resolution MEPC.83(44)). Adequacy relates both to the operational conditions of the facility in view of the user needs, as well as to the environmental management of the facilities in accordance with Union waste law. It might, in some cases, be difficult to assess whether a port reception facility located outside the Union meets such standard.

(26) Regulation (EC) No 1069/2009 of the European Parliament and of the Council ([10]) requires international catering waste to be incinerated or disposed of by burial in an authorised landfill, including waste from ships calling at Union ports which has potentially been in contact with animal by-products on board. In order for this requirement not to limit the preparation for reuse and recycling of waste from ships, efforts should be made in accordance with the IMO Consolidated Guidance in order to better segregate the waste so that potential contamination of waste, such as packaging waste, can be avoided.

(27) As established in Regulation (EC) No 1069/2009, in conjunction with Commission Regulation (EU) No 142/2011 ([11]), intra-Union voyages are not considered transport operating internationally and the catering waste from those voyages does not need to be incinerated. However, such intra-Union voyages are considered international voyages under international maritime legislation (the MARPOL Convention and the International Convention for the Safety of Life at Sea (SOLAS)). In order to ensure the coherence of Union law, the definitions from Regulation (EC) No 1069/2009 should be followed when defining the scope and treatment of international catering waste under this Directive, in conjunction with Regulation (EU) No 142/2011.

(28) To ensure the adequacy of port reception facilities, the development, implementation and re-assessment of the waste reception and handling plan is essential, based on the consultation of all relevant parties. For practical and organisational reasons, neighbouring ports in the same geographical region might want to develop a joint plan, covering the availability of port reception facilities in each of the ports covered by that plan while providing a common administrative framework.

(29) It can be challenging to adopt and monitor waste reception and handling plans for small non-commercial ports, such as mooring areas and marinas, which receive low traffic, consisting of recreational craft only, or which are only in use during part of the year. The waste from those small ports is normally handled by the municipal waste management system in accordance with the principles set out in Directive 2008/98/EC. In order not to overburden the local authorities and facilitate the waste management in such small ports, it should be sufficient that waste from such ports is included in the municipal waste stream and managed accordingly, that the port makes information regarding waste reception available to port users, and that the exempted ports are reported in an electronic system to allow for a minimum level of monitoring.

(30) To address the problem of marine litter effectively, it is fundamental to provide the right level of incentives for the delivery of waste to port reception facilities, in particular waste as defined in Annex V to the MARPOL Convention ('MARPOL Annex V waste'). This can be achieved through a cost recovery system which requires the application of an indirect fee. That indirect fee should be due irrespective of the delivery of waste and should give the right of delivery of the waste without any additional direct charges. The fishing and recreational sector, given their contribution to the occurrence of marine litter, should also be subject to the indirect fee. However, where a ship delivers an exceptional amount of MARPOL Annex V waste, especially operational waste, which exceeds the maximum dedicated storage capacity as mentioned in the advance notification form for waste delivery, it should be possible for an additional direct fee to be charged in order to ensure that the costs related to receiving this exceptional amount of waste do not cause a disproportionate burden on a port's cost recovery system. This might also be the case where declared dedicated storage capacity is excessive or unreasonable.

([10]) Regulation (EC) No 1069/2009 of the European Parliament and the Council of 21 October 2009 laying down health rules as regards animal by-products and derived products not intended for human consumption and repealing Regulation (EC) No 1774/2002 (Animal by-products Regulation) (OJ L 300, 14.11.2009, p. 1).

([11]) Commission Regulation (EU) No 142/2011 of 25 February 2011 implementing Regulation (EC) No 1069/2009 of the European Parliament and of the Council laying down health rules as regards animal by-products and derived products not intended for human consumption and implementing Council Directive 97/78/EC as regards certain samples and items exempt from veterinary checks at the border under that Directive (OJ L 54, 26.2.2011, p. 1).

(31) In certain Member States, schemes have been set up to provide alternative financing of the costs of collecting and managing fishing gear waste or passively fished waste ashore, including 'fishing for litter schemes'. Such initiatives should be welcomed, and Member States should be encouraged to complement the cost recovery systems set up in accordance with this Directive with the fishing for litter schemes to cover the costs of passively fished waste. As such, those cost recovery systems, which are based on the application of a 100 % indirect fee for MARPOL Annex V waste, excluding cargo residues, should not create a disincentive for fishing port communities to participate in existing delivery schemes for passively fished waste.

(32) A ship's fee should be reduced for those vessels designed, equipped or operated to minimise waste, following certain criteria to be developed by implementing powers conferred on the Commission, in line with the IMO guidelines for the implementation of MARPOL Annex V and with standards developed by the International Organization for Standardization. Reduction and efficient recycling of waste can be primarily achieved through effective on-board waste segregation in line with those guidelines and standards.

(33) Due to its type of trade, which is characterised by frequent port calls, short sea shipping faces significant costs within the current regime for the delivery of waste to port reception facilities, having to pay a fee at each and every port call. At the same time, the traffic is not sufficiently scheduled and regular to qualify for an exemption from payment and delivery of waste on those grounds. To limit the financial burden on the sector, a reduced fee should be charged to vessels based on the type of traffic in which they are engaged.

(34) Cargo residues remain the property of the cargo owner after unloading the cargo to the terminal, and may have an economic value. For this reason, cargo residues should not be included in the cost recovery systems and the application of the indirect fee. The charges for the delivery of cargo residues should be paid by the user of the port reception facility, as specified in the contractual arrangements between the parties involved or in other local arrangements. Cargo residues also include the remnants of oily or noxious liquid cargo after cleaning operations, to which the discharge norms of Annexes I and II to MARPOL Convention apply, and which under certain conditions, as set out in those Annexes, do not need to be delivered in port to avoid unnecessary operational costs for ships and congestion in ports.

(35) Member States should encourage the delivery of residues from tank washings containing high-viscosity persistent floating substances, possibly by way of appropriate financial incentives.

(36) Regulation (EU) 2017/352 of the European Parliament and of the Council ([12]) includes the provision of port reception facilities as a service in its scope. It provides rules on the transparency of the charging structures applied for the use of port services, consultation of port users and handling of complaint procedures. This Directive goes beyond the framework provided by that Regulation by providing more detailed requirements for the design and operation of the cost recovery systems for port reception facilities for waste from ships and the transparency of the cost structure.

(37) In addition to providing incentives for delivery of waste, effective enforcement of the delivery obligation is paramount and should follow a risk-based approach, for which a Union risk-based targeting mechanism should be established.

(38) One of the main obstacles for the effective enforcement of the mandatory delivery obligation has been the different interpretation and implementation by Member States of the exception based on sufficient storage capacity. To avoid the application of this exception undermining the main objective of this Directive, it should be specified further, in particular with regard to the next port of call, and sufficient storage capacity should be determined in a harmonised way, based on common methodology and criteria. In cases where it is difficult to establish whether adequate port reception facilities in ports outside the Union are available, it is essential that the competent authority carefully considers the application of the exception.

([12]) Regulation (EU) 2017/352 of the European Parliament and of the Council of 15 February 2017 establishing a framework for the provision of port services and common rules on the financial transparency of ports (OJ L 57, 3.3.2017, p. 1).

(39) There is a need for further harmonisation of the regime of exemptions for ships engaged in scheduled traffic with frequent and regular port calls, in particular clarification of the terms used and the conditions governing those exemptions. The REFIT Evaluation and the impact assessment have revealed that the lack of harmonisation of the conditions and application of exemptions has resulted in an unnecessary administrative burden for ships and ports.

(40) Monitoring and enforcement should be facilitated through a system based on electronic reporting and exchange of information. To this end, the existing information and monitoring system set up under Directive 2000/59/EC should be further developed and should continue to be operated on basis of existing electronic data systems, in particular the Union Maritime Information and Exchange system (SafeSeaNet) established by Directive 2002/59/EC of the European Parliament and of the Council ([13]) and the Inspection Database set up by Directive 2009/16/EC of the European Parliament and of the Council ([14]) (THETIS). Such a system should also include the information on port reception facilities available in the different ports.

(41) Directive 2010/65/EU of the European Parliament and of the Council ([15]) simplifies and harmonises administrative procedures applied to maritime transport by making the electronic transmission of information more general and streamlining reporting formalities. The Valletta Declaration on the priorities for the EU's maritime transport policy until 2020, endorsed by the Council in its conclusions of 8 June 2017, invited the Commission to propose appropriate follow-up to the revision of that Directive. A public consultation on the reporting formalities for ships was carried out by the Commission from 25 October 2017 to 18 January 2018. On 17 May 2018, the Commission transmitted to the European Parliament and to the Council a proposal for a Regulation establishing a European Maritime Single Window environment and repealing Directive 2010/65/EU.

(42) The MARPOL Convention requires the contracting Parties to maintain up-to-date information on their port reception facilities and to communicate this information to the IMO. To this end, the IMO has established a port reception facilities database within its Global Integrated Shipping Information System ('GISIS').

(43) In the IMO Consolidated Guidance, the IMO provides for the reporting of alleged inadequacies of port reception facilities. Under that procedure, a ship should report such inadequacies to the administration of the flag State, which in turn is to notify the IMO and the port State of the occurrence. The port State should examine the report and respond appropriately, informing the IMO and the reporting flag State. Reporting of this information on alleged inadequacies directly into the information, monitoring and enforcement system provided for in this Directive would allow for the subsequent transmission of this information into GISIS, relieving Member States as flag and port States from their reporting duty to the IMO.

(44) The Sub-group on Port Reception Facilities, which was set up under the European Sustainable Shipping Forum, and which brought together a wide range of experts in the field of ship-source pollution and the management of waste from ships, was adjourned in December 2017 in view of the start of interinstitutional negotiations. Since that Sub-group provided valuable guidance and expertise to the Commission, it would be desirable to create a similar expert group with a mandate of exchanging experience on the implementation of this Directive.

(45) It is important that any penalties laid down by Member States be properly implemented and be effective, proportionate and dissuasive.

(46) Good working conditions for port personnel working in port reception facilities are of paramount importance to creating a safe, efficient and socially accountable maritime sector, which is able to attract qualified workers and ensure a wide-level playing field across Europe. Initial and periodic training of staff is essential to ensure the quality of services and the protection of workers. Port authorities and port reception facility authorities should ensure that all personnel receive the necessary training to acquire the knowledge which is essential for their work, with specific attention for health and safety aspects pertaining to dealing with hazardous materials, and that training requirements are regularly updated to meet the challenges of technological innovation.

([13]) Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p. 10).

([14]) Directive 2009/16/EC of the European Parliament and of the Council of 23 April 2009 on port State control (OJ L 131, 28.5.2009, p. 57).

([15]) Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC (OJ L 283, 29.10.2010, p. 1).

(47) The powers conferred on the Commission to implement Directive 2000/59/EC should be updated in accordance with the Treaty on the Functioning of the European Union (TFEU).

(48) The power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of amending the Annexes to this Directive and the references to international instruments to the extent necessary to bring them into line with Union law or in order to take account of developments at international level, in particular at IMO level; amending the Annexes to this Directive when this is necessary in order to improve the implementation and monitoring arrangements established by it, in particular in relation to the effective notification and delivery of waste, and the proper application of exemptions; as well as, in exceptional circumstances, where duly justified by an appropriate analysis by the Commission and in order to avoid a serious and unacceptable threat to the marine environment, amending this Directive to the extent necessary to avoid such a threat, in order to prevent, if necessary, changes to those international instruments from applying for the purposes of this Directive. 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 ([16]). 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.

(49) In order to provide for the methods for the calculation of the sufficient dedicated storage capacity; to develop common criteria for recognising, for the purpose of granting a reduced waste fee to ships, that a ship's design, equipment and operation demonstrate that it produces reduced quantities of waste, and manages its waste in a sustainable and environmentally sound manner; to define methodologies for monitoring data on the volume and quantity of passively fished waste and the format for reporting; to define the detailed elements of a Union risk-based targeting mechanism, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and the Council ([17]).

(50) Since the objective of this Directive, namely the protection of the marine environment from discharges of waste at sea, cannot be sufficiently achieved by the Member States but can rather, by reason of the scale of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

(51) The Union is characterised by regional differences at port level, as also demonstrated in the territorial impact assessment carried out by the Commission. Ports differ based on geographic location, size, administrative set-up and ownership, and are characterised by the type of ships that normally visit. In addition, waste management systems reflect the differences at municipal level and downstream waste management infrastructure.

(52) Article 349 TFEU requires consideration to be given to the special characteristics of the outermost regions of the Union, namely Guadeloupe, French Guiana, Martinique, Mayotte, Réunion, Saint-Martin, the Azores, Madeira and the Canary Islands. To ensure the adequacy and availability of port reception facilities, it might be appropriate for Member States to make regional operating aid available to port reception facility operators or port authorities in those regions of the Union in order to address the effects of the permanent handicaps referred to in that Article. Regional operating aid made available by Member States in that context is exempt from the notification obligation laid down in Article 108(3) TFEU if, at the time it is granted, it fulfils the conditions laid down by Commission Regulation (EU) No 651/2014 ([18]), adopted pursuant to Council Regulation (EC) No 994/98 ([19]).

(53) Directive 2000/59/EC should therefore be repealed,

([16]) OJ L 123, 12.5.2016, p. 1.
([17]) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).
([18]) Commission Regulation (EU) No 651/2014 of 17 June 2014 declaring certain categories of aid compatible with the internal market in application of Article s 107 and 108 of the Treaty (OJ L 187, 26.6.2014, p. 1).
([19]) Council Regulation (EC) No 994/98 of 7 May 1998 on the application of Article s 107 and 108 of the Treaty on the Functioning of the European Union to certain categories of horizontal State aid (OJ L 142, 14.5.1998, p. 1).

HAVE ADOPTED THIS DIRECTIVE:

Section 1

General provisions

Article 1

Subject matter

This Directive aims to protect the marine environment against the negative effects from discharges of waste from ships using ports located in the Union, while ensuring the smooth operation of maritime traffic, by improving the availability and use of adequate port reception facilities and the delivery of waste to those facilities.

Article 2

Definitions

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

(1) 'ship' means a seagoing vessel of any type operating in the marine environment, including fishing vessels, recreational craft, hydrofoil boats, air-cushion vehicles, submersibles and floating craft;

(2) 'MARPOL Convention' means the International Convention for the Prevention of Pollution from Ships, in its up-to-date version;

(3) 'waste from ships' means all waste, including cargo residues, which is generated during the service of a ship or during loading, unloading and cleaning operations and which falls within the scope of Annexes I, II, IV, V and VI to MARPOL Convention, as well as passively fished waste;

(4) 'passively fished waste' means waste collected in nets during fishing operations;

(5) 'cargo residues' means the remnants of any cargo material on board which remain on the deck or in holds or tanks following loading and unloading, including loading and unloading excess or spillage, whether in wet or dry condition or entrained in wash-water, excluding cargo dust remaining on the deck after sweeping or dust of the external surfaces of the ship;

(6) 'port reception facility' means any facility which is fixed, floating or mobile and capable of providing the service of receiving the waste from ships;

(7) 'fishing vessel' means any ship equipped or used commercially for catching fish or other living resources from the sea;

(8) 'recreational craft' means a ship of any type, with a hull length of 2,5 metres or more, regardless of the means of propulsion, intended for sports or leisure purposes, and not engaged in trade;

(9) 'port' means a place or a geographical area made up of such improvement works and equipment designed principally to permit the reception of ships, including the anchorage area within the jurisdiction of the port;

(10) 'sufficient storage capacity' means enough capacity to store the waste on board from the moment of departure until the next port of call, including the waste that is likely to be generated during the voyage;

(11) 'scheduled traffic' means traffic based on a published or planned list of times of departures and arrivals between identified ports or recurrent crossings that constitute a recognised schedule;

(12) 'regular port calls' means repeated voyages of the same ship forming a constant pattern between identified ports or a series of voyages from and to the same port without intermediate calls;

(13) 'frequent port calls' means visits by a ship to the same port taking place at least once a fortnight;

(14) 'GISIS' means the Global Integrated Shipping Information System set up by the IMO;

(15) 'treatment' means recovery or disposal operations, including preparation prior to recovery or disposal;

(16) 'indirect fee' means a fee paid for the provision of port reception facility services, irrespective of the actual delivery of waste from ships.

'Waste from ships' referred to in point (3) shall be considered to be waste within the meaning of point 1 of Article 3 of Directive 2008/98/EC.

Article 3

Scope

1. This Directive applies to:

(a) all ships, irrespective of their flag, calling at, or operating within, a port of a Member State, with the exception of ships engaged in port services within the meaning of Article 1(2) of Regulation (EU) 2017/352, and with the exception of any warship, naval auxiliary or other ship owned or operated by a State and used, for the time being, only on a government non-commercial basis;

(b) all ports of the Member States normally visited by ships falling within the scope of point (a).

For the purpose of this Directive, and to avoid undue delay to ships, Member States may decide to exclude the anchorage area from their ports for the purposes of the application of Article s 6, 7 and 8.

2. Member States shall take measures to ensure that, where reasonably possible, ships which do not fall within the scope of this Directive deliver their waste in a manner consistent with this Directive.

3. Member States which have neither ports nor ships flying their flag that fall within the scope of this Directive may, with the exception of the obligation set out in the third subparagraph of this paragraph, derogate from the provisions of this Directive.

Member States which do not have ports that fall within the scope of this Directive may derogate from the provisions of this Directive which are addressed solely to ports.

Those Member States which intend to avail themselves of the derogations set out in this paragraph shall communicate to the Commission by 28 June 2021 whether the relevant conditions have been met and shall inform the Commission annually thereafter of any subsequent change. Until such Member States have transposed and implemented this Directive, they may not have any ports falling within the scope of this Directive and they may not allow ships, including craft, that fall within the scope of this Directive to fly their flag.

Section 2

Provision of adequate port reception facilities

Article 4

Port reception facilities

1. Member States shall ensure the availability of port reception facilities adequate to meet the need of the ships normally using the port without causing undue delay to ships.

2. Member States shall ensure that:

(a) the port reception facilities have the capacity to receive the types and quantities of waste from ships normally using that port, taking into account:

(i) the operational needs of the port users;

(ii) the size and geographical location of that port;

(iii) the type of ships calling at that port; and

(iv) the exemptions provided for under Article 9;

(b) the formalities and practical arrangements relating to the use of the port reception facilities are simple and expeditious to avoid undue delays to ships;

(c) the fees charged for delivery do not create a disincentive for ships to use the port reception facilities; and

(d) the port reception facilities allow for the management of the waste from ships in an environmentally sound manner in accordance with Directive 2008/98/EC and other relevant Union and national waste law.

For the purposes of point (d) of the first subparagraph, the Member States shall ensure separate collection to facilitate reuse and recycling of waste from ships in ports as required under Union waste law, in particular Directive 2006/66/EC of the European Parliament and the Council ([20]), Directive 2008/98/EC and Directive 2012/19/EU of the European Parliament and of the Council ([21]). In order to facilitate this process, port reception facilities may collect the separate waste fractions in accordance with waste categories defined in the MARPOL Convention, taking into account the guidelines thereof.

Point (d) of the first subparagraph shall apply without prejudice to the more stringent requirements imposed by Regulation (EC) No 1069/2009 for the management of catering waste from international transport.

3. Member States, in their capacity as flag States, shall use the IMO forms and procedures to notify the IMO as well as the authorities of the port State of alleged inadequacies of port reception facilities.

Member States, in their capacity as port States, shall investigate all reported cases of alleged inadequacies and use the IMO forms and procedures to notify the IMO and the reporting flag State of the outcome of the investigation.

4. The port authorities concerned or, failing them, the relevant authorities shall ensure that waste delivery or reception operations are carried out with sufficient safety measures to avert risks to persons and the environment at ports covered by this Directive.

5. Member States shall ensure that any party involved in the delivery or reception of waste from ships can claim compensation for damage caused by undue delay.

([20]) Directive 2006/66/EC of the European Parliament and of the Council of 6 September 2006 on batteries and accumulators and waste batteries and accumulators and repealing Directive 91/157/EEC (OJ L 266, 26.9.2006, p. 1).

([21]) Directive 2012/19/EU of the European Parliament and of the Council of 4 July 2012 on waste electrical and electronic equipment (WEEE) (OJ L 197, 24.7.2012, p. 38).

Article 5

Waste reception and handling plans

1. Member States shall ensure that an appropriate waste reception and handling plan is in place and has been implemented for each port following ongoing consultations with the relevant parties, including in particular with port users or their representatives, and, where appropriate, local competent authorities, port reception facility operators, organisations implementing extended producer responsibility obligations and representatives of civil society. Those consultations should be held both during the initial drafting of the waste reception and handling plan and after its adoption, in particular when significant changes have taken place, with regard to the requirements in Article s 4, 6 and 7.

The detailed requirements for the development of the waste reception and handling plan are set out in Annex 1.

2. Member States shall ensure that the following information from the waste reception and handling plan on the availability of adequate port reception facilities in their ports and the structure of the costs is clearly communicated to the ship operators, is made publicly available and is easily accessible, in an official language of the Member State where the port is located and, where relevant, in a language that is internationally used:

(a) location of port reception facilities applicable to each berth, and, where relevant, their opening hours;

(b) list of waste from ships normally managed by the port;

(c) list of contact points, the port reception facility operators and the services offered;

(d) description of the procedures for delivery of the waste;

(e) description of the cost recovery system, including waste management schemes and funds as referred to in Annex 4, where applicable.

The information referred to in the first subparagraph of this paragraph shall also be made available electronically and kept up-to-date in that part of the information, monitoring and enforcement system referred to in Article 13.

3. Where required for reasons of efficiency, the waste reception and handling plans may be developed jointly by two or more neighbouring ports in the same geographical region, with the appropriate involvement of each port, provided that the need for and availability of port reception facilities are specified for each port.

4. Member States shall evaluate and approve the waste reception and handling plan and ensure its re-approval at least every five years after it has been approved or re-approved, and after significant changes in the operation of the port have taken place. Those changes may include structural changes in traffic to the port, development of new infrastructure, changes in the demand and provision of port reception facilities, and new on-board treatment techniques.

Member States shall monitor the port's implementation of the waste reception and handling plan. Where, during the five-year period referred to in the first subparagraph, no significant changes have taken place, the re-approval may consist of a validation of existing plans.

5. Small non-commercial ports which are characterised by rare or low traffic from recreational craft only may be exempted from paragraphs 1 to 4 if their port reception facilities are integrated in the waste handling system managed by or on behalf of the relevant municipality and the Member States where those ports are located ensure that the information regarding the waste management system is made available to the users of those ports.

The Member States where such ports are located shall notify the name and location of those ports electronically in that part of the information, monitoring and enforcement system referred to in Article 13.

Section 3

Delivery of waste from ships

Article 6

Advance waste notification

1. The operator, agent or master of a ship which falls within the scope of Directive 2002/59/EC bound for a Union port shall complete truly and accurately the form set out in Annex 2 to this Directive ('advance waste notification') and notify all the information contained therein to the authority or body designated for this purpose by the Member State in which that port is located:

(a) at least 24 hours prior to arrival, if the port of call is known;

(b) as soon as the port of call is known, if this information is available less than 24 hours prior to arrival; or

(c) at the latest upon departure from the previous port, if the duration of the voyage is less than 24 hours.

2. The information from the advance waste notification shall be reported electronically in that part of the information, monitoring and enforcement system referred to in Article 13 of this Directive, in accordance with Directives 2002/59/EC and 2010/65/EU.

3. The information from the advance waste notification shall be available on board, preferably in electronic form, at least until the next port of call and shall be made available upon request to the relevant Member States' authorities.

4. Member States shall ensure that the information that is notified pursuant to this Article is examined and shared with the relevant enforcement authorities without delay.

Article 7

Delivery of waste from ships

1. The master of a ship calling at a Union port shall, before leaving that port, deliver all its waste carried on board to a port reception facility in accordance with the relevant discharge norms laid down in the MARPOL Convention.

2. Upon delivery, the port reception facility operator or the authority of the port where the waste was delivered shall truly and accurately complete the form set out in Annex 3 ('waste delivery receipt') and issue and provide, without undue delay, the waste delivery receipt to the master of the ship.

The requirements set out in the first subparagraph shall not apply in small ports with unmanned facilities or that are remotely located, provided that the Member State where such ports are located has notified the name and location of those ports electronically in that part of the information, monitoring and enforcement system referred to in Article 13.

3. The operator, agent or master of a ship which falls within the scope of Directive 2002/59/EC shall before departure, or as soon as the waste delivery receipt has been received, electronically report the information contained therein in that part of the information, monitoring and enforcement system referred to in Article 13 of this Directive, in accordance with Directives 2002/59/EC and 2010/65/EU.

The information from the waste delivery receipt shall be available on board for at least two years, where relevant with the appropriate Oil Record Book, Cargo Record Book, Garbage Record Book or the Garbage Management Plan, and shall be made available upon request to the Member States' authorities.

4. Without prejudice to paragraph 1, a ship may proceed to the next port of call without delivering the waste, if:

(a) the information provided in accordance with Annexes 2 and 3 shows that there is sufficient dedicated storage capacity for all waste that has been accumulated and will be accumulated during the intended voyage of the ship until the next port of call;

(b) the information available on board ships falling outside the scope of Directive 2002/59/EC shows that there is sufficient dedicated storage capacity for all waste that has been accumulated and will be accumulated during the intended voyage of the ship until the next port of call; or

(c) the ship only calls at anchorage for less than 24 hours or under adverse weather conditions, unless such an area has been excluded in accordance with the second subparagraph of Article 3(1).

In order to ensure uniform conditions for the implementation of the exception referred to in points (a) and (b) of the first subparagraph, the Commission shall adopt implementing acts to define the methods to be used for the calculation of the sufficient dedicated storage capacity. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 20(2).

5. A Member State shall require the ship to deliver, before departure, all its waste if:

(a) it cannot be established, based on the available information, including information electronically available in that part of the information, monitoring and enforcement system referred to in Article 13 or in GISIS, that adequate port reception facilities are available in the next port of call; or

(b) the next port of call is unknown.

6. Paragraph 4 shall apply without prejudice to more stringent requirements for ships adopted in accordance with international law.

Article 8

Cost recovery systems

1. Member States shall ensure that the costs of operating port reception facilities for the reception and treatment of waste from ships, other than cargo residues, are covered through the collection of a fee from ships. Those costs include the elements listed in Annex 4.

2. The cost recovery systems shall provide no incentive for ships to discharge their waste at sea. To this end, the Member States shall apply all of the following principles in the design and operation of the cost recovery systems:

(a) ships shall pay an indirect fee, irrespective of delivery of waste to a port reception facility;

(b) the indirect fee shall cover:

(i) the indirect administrative costs;

(ii) a significant part of the direct operational costs, as determined in Annex 4, which shall represent at least 30 % of the total direct costs for actual delivery of the waste during the previous year, with the possibility of also taking into account costs related to the traffic volume expected for the coming year;

(c) in order to provide for a maximum incentive for the delivery of MARPOL Annex V waste other than cargo residues, no direct fee shall be charged for such waste, in order to ensure a right of delivery without any additional charges based on the volume of waste delivered, except where the volume of waste delivered exceeds the maximum dedicated storage capacity mentioned in the form set out in Annex 2 to this Directive; passively fished waste shall be covered by this regime, including the right of delivery;

(d) in order to avoid that the costs of collection and treatment of passively fished waste are borne exclusively by port users, Member States shall cover, where appropriate, those costs from the revenues generated by alternative financing systems, including by waste management schemes and by Union, national or regional funding available;

(e) in order to encourage the delivery of residues from tank washing containing high-viscosity persistent floating substances, Member States may provide for appropriate financial incentives for their delivery;

(f) the indirect fee shall not include the waste from exhaust gas cleaning systems, the costs of which shall be covered on the basis of the types and quantities of waste delivered.

3. The part of the costs which is not covered by the indirect fee, if any, shall be covered on the basis of the types and quantities of waste actually delivered by the ship.

4. The fees may be differentiated on the following basis:

(a) the category, type and size of the ship;

(b) the provision of services to ships outside normal operating hours in the port; or

(c) the hazardous nature of the waste.

5. The fees shall be reduced on the following basis:

(a) the type of trade the ship is engaged in, in particular when a ship is engaged in short sea shipping trade;

(b) the ship's design, equipment and operation demonstrate that the ship produces reduced quantities of waste, and manages its waste in a sustainable and environmentally sound manner.

By 28 June 2020, the Commission shall adopt implementing acts to define the criteria for determining that a ship meets the requirements stated in point (b) of the first subparagraph in relation to the ship's on-board waste management. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 20(2).

6. In order to ensure that the fees are fair, transparent, easily identifiable, non-discriminatory, and that they reflect the costs of the facilities and services made available, and, where appropriate, used, the amount of the fees and the basis on which they have been calculated shall be made available in an official language of the Member State where the port is located and, where relevant, in a language that is internationally used to the port users in the waste reception and handling plan.

7. Member States shall ensure that monitoring data on the volume and quantity of passively fished waste are collected, and shall report such monitoring data to the Commission. The Commission shall, on the basis of those monitoring data, publish a report by 31 December 2022 and every two years thereafter.

The Commission shall adopt implementing acts to define monitoring data methodologies and the format for reporting. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 20(2).

Article 9

Exemptions

1. Member States may exempt a ship calling at their ports from the obligations in Article 6, Article 7(1) and Article 8 ('the exemption'), where there is sufficient evidence that the following conditions are met:

(a) the ship is engaged in scheduled traffic with frequent and regular port calls;

(b) there is an arrangement to ensure the delivery of the waste and payment of the fees in a port along the ship's route which:

  (i) is evidenced by a signed contract with a port or waste contractor and by waste delivery receipts;

  (ii) has been notified to all ports on the ship's route; and

  (iii) has been accepted by the port where the delivery and payment take place, which can be a Union port or another port in which, as established on the basis of the information reported electronically into that part of the information, monitoring and enforcement system referred to in Article 13 and in GISIS, adequate facilities are available;

(c) the exemption does not pose a negative impact on maritime safety, health, shipboard living or working conditions or on the marine environment.

2. If the exemption is granted, the Member State where the port is located shall issue an exemption certificate, based on the format set out in Annex 5, confirming that the ship meets the necessary conditions and requirements for the application of the exemption and stating the duration of the exemption.

3. Member States shall report the information from the exemption certificate electronically in that part of the information, monitoring and enforcement system referred to in Article 13.

4. Member States shall ensure effective monitoring and enforcement of the arrangements for the delivery and payment in place for the exempted ships visiting their ports.

5. Notwithstanding the exemption granted, a ship shall not proceed to the next port of call if there is insufficient dedicated storage capacity for all waste that has been accumulated and that will be accumulated during the intended voyage of the ship until the next port of call.

Section 4

Enforcement

Article 10

Inspections

Member States shall ensure that any ship may be subject to inspections, including random ones, in order to verify that it complies with this Directive.

Article 11

Inspection commitments

1. Each Member State shall carry out inspections of ships calling in its ports corresponding to at least 15 % of the total number of individual ships calling in its ports annually.

The total number of individual ships calling in a Member State shall be calculated as the average number of individual ships over the previous three years, as reported through that part of the information, monitoring and enforcement system referred to in Article 13.

2. Member States shall comply with paragraph 1 of this Article by selecting ships on the basis of a Union risk-based targeting mechanism.

In order to ensure harmonisation of inspections and to provide for uniform conditions for selection of ships for inspection, the Commission shall adopt implementing acts to define the detailed elements of the Union risk-based targeting mechanism. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 20(2).

3. Member States shall establish procedures for inspections of ships that fall outside the scope of Directive 2002/59/EC in order to ensure, as far as practicable, compliance with this Directive.

When establishing those procedures, Member States may take into account the Union risk-based targeting mechanism referred to in paragraph 2.

4. If the relevant authority of the Member State is not satisfied with the results of the inspection, it shall, without prejudice to the application of the penalties referred to in Article 16, ensure that the ship does not leave port until it has delivered its waste to a port reception facility in accordance with Article 7.

Article 12

Information, monitoring and enforcement system

The implementation and enforcement of this Directive shall be facilitated by the electronic reporting and exchange of information between Member States in accordance with Article s 13 and 14.

Article 13

Reporting and exchange of information

1. The reporting and exchange of information shall be based on the Union Maritime Information and Exchange System ('SafeSeaNet') referred to in Article 22a(3) of and Annex III to Directive 2002/59/EC.

2. Member States shall ensure that the following information is reported electronically and within reasonable time in accordance with Directive 2010/65/EU:

(a) the information on the actual time of arrival and time of departure of every ship falling within the scope of Directive 2002/59/EC which calls at a Union port, together with an identifier of the port concerned;

(b) the information from the advance waste notification, as set out in Annex 2;

(c) the information from the waste delivery receipt, as set out in Annex 3;

(d) the information from the exemption certificate, as set out in Annex 5.

3. Member States shall ensure that the information listed in Article 5(2) is made electronically available through SafeSeaNet.

Article 14

Recording of inspections

1. The Commission shall develop, maintain and update an inspection database to which all Member States shall be connected and which shall contain all the information required for the implementation of the inspection system provided for by this Directive ('the inspection database'). The inspection database shall be based on the inspection database referred to in Article 24 of Directive 2009/16/EC and shall have similar functionalities to that database.

2. Member States shall ensure that the information related to inspections under this Directive, including information regarding non-compliance and prohibition of departure orders issued, is transferred without delay to the inspection database, as soon as:

(a) the inspection report has been completed;

(b) the prohibition of departure order has been lifted; or

(c) an exemption has been granted.

3. The Commission shall ensure that the inspection database makes it possible to retrieve any relevant data reported by the Member States for the purpose of monitoring the implementation of this Directive.

The Commission shall ensure that the inspection database provides information for the Union risk-based targeting mechanism referred to in Article 11(2).

The Commission shall regularly review the inspection database to monitor the implementation of this Directive and call attention to any doubts regarding comprehensive implementation with the aim of instigating corrective action.

4. Member States shall at all times have access to the information recorded in the inspection database.

Article 15

Training of personnel

Port authorities and port reception facility authorities shall ensure that all personnel receive the necessary training to acquire the knowledge which is essential for their work on dealing with waste, with specific attention to health and safety aspects pertaining to dealing with hazardous materials, and that training requirements are regularly updated to meet the challenges of technological innovation.

Article 16

Penalties

Member States shall lay down the rules on penalties applicable to infringements of national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.

Section 5

Final provisions

Article 17

Exchange of experience

The Commission shall provide for the organisation of exchanges of experience between the Member States' national authorities and experts, including those from the private sector, civil society and trade unions, on the application of this Directive in Union ports.

Article 18

Amendment procedure

1. The Commission is empowered to adopt delegated acts in accordance with Article 19 to amend the Annexes to this Directive and the references to IMO instruments in this Directive to the extent necessary to bring them into line with Union law or in order to take account of developments at international level, in particular at IMO level.

2. The Commission is also empowered to adopt delegated acts in accordance with Article 19 to amend the Annexes when this is necessary in order to improve the implementation and monitoring arrangements established by this Directive, in particular those provided for in Article s 6, 7 and 9, in order to ensure the effective notification and delivery of waste, and the proper application of exemptions.

3. In exceptional circumstances, where duly justified by an appropriate analysis by the Commission and in order to avoid a serious and unacceptable threat to the marine environment, the Commission is empowered to adopt delegated acts in accordance with Article 19 to amend this Directive to the extent necessary to avoid such a threat, in order not to apply, for the purposes of this Directive, an amendment to the MARPOL Convention.

4. The delegated acts provided for in this Article shall be adopted at least three months before the expiration of the period established internationally for the tacit acceptance of the amendment to the MARPOL Convention or the envisaged date for the entry into force of that amendment.

In the period preceding the entry into force of such delegated acts, Member States shall refrain from any initiative intended to integrate that amendment in national law or to apply the amendment to the international instrument concerned.

Article 19

Exercise of the delegation

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

2. The power to adopt delegated acts referred to in Article 18(1), (2) and (3) shall be conferred on the Commission for a period of five years from 27 June 2019. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

3. The delegation of power referred to in Article 18(1), (2) and (3) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

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

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

6. A delegated act adopted pursuant to Article 18(1), (2) and (3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 20

Committee procedure

1. The Commission shall be assisted by the Committee on Safe Seas and the Prevention of Pollution from Ships (COSS) established by Regulation (EC) No 2099/2002 of the European Parliament and of the Council [22]. That Committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 21

Amendment to Directive 2010/65/EU

In point A of the Annex to Directive 2010/65/EU, point 4 is replaced by the following:

'4. Notification of waste from ships, including residues

Articles 6, 7 and 9 of Directive (EU) 2019/883 of the European Parliament and the Council of 17 April 2019 on port reception facilities for the delivery of waste from ships, amending Directive 2010/65/EU and repealing Directive 2000/59/EC (OJ L 151, 7.6.2019, p. 116)'.

Article 22

Repeal

Directive 2000/59/EC is repealed.

References to the repealed Directive shall be construed as references to this Directive.

Article 23

Review

1. The Commission shall evaluate this Directive and submit the results of the evaluation to the European Parliament and the Council by 28 June 2026. The evaluation shall also include a report detailing best waste prevention and management practices on board ships.

2. In the context of Regulation (EU) 2016/1625 of the European Parliament and of the Council [23], when the next review of the European Maritime Safety Agency (EMSA) mandate is due, the Commission shall also evaluate whether EMSA should be granted additional competences for the enforcement of this Directive.

[22] Regulation (EC) No 2099/2002 of the European Parliament and of the Council of 5 November 2002 establishing a Committee on Safe Seas and the Prevention of Pollution from Ships (COSS) and amending the Regulations on maritime safety and the prevention of pollution from ships (OJ L 324, 29.11.2002, p. 1).

[23] Regulation (EU) 2016/1625 of the European Parliament and of the Council of 14 September 2016 amending Regulation (EC) No 1406/2002 establishing a European Maritime Safety Agency (OJ L 251, 16.9.2016, p. 77).

Article 24

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 28 June 2021. They shall immediately inform the Commission thereof.

When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

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

Article 25

Entry into force

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

Article 26

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 17 April 2019.

For the European Parliament	*For the Council*
The President	*The President*
A. TAJANI	G. CIAMBA

ANNEX 1

REQUIREMENTS FOR WASTE RECEPTION AND HANDLING PLANS

The waste reception and handling plans shall cover all types of waste from ships normally visiting the port and shall be developed according to the size of the port and the types of ships calling at that port.

The waste reception and handling plans shall include the following elements:

(a) an assessment of the need for port reception facilities, in light of the needs of ships normally visiting the port;

(b) a description of the type and capacity of port reception facilities;

(c) a description of the procedures for the reception and collection of waste from ships;

(d) a description of the cost recovery system;

(e) a description of the procedure for reporting alleged inadequacies of port reception facilities;

(f) a description of the procedure for ongoing consultations with port users, waste contractors, terminal operators and other interested parties; and

(g) an overview of the type and quantities of waste received from ships and handled in the facilities.

The waste reception and handling plans may include:

(a) a summary of relevant national law and the procedure and formalities for the delivery of the waste to port reception facilities;

(b) an identification of a point of contact in the port;

(c) a description of the pre-treatment equipment and processes for specific waste streams in the port, if any;

(d) a description of methods for recording the actual use of the port reception facilities;

(e) a description of methods for recording the amounts of the waste delivered by ships;

(f) a description of methods for managing the different waste streams in the port.

The procedures for reception, collection, storage, treatment and disposal should conform in all respects to an environmental management scheme suitable for the progressive reduction of the environmental impact of these activities. Such conformity is presumed if the procedures are in compliance with Regulation (EC) No 1221/2009 of the European Parliament and the Council ([1]).

(1) Regulation (EC) No 1221/2009 of the European Parliament and the Council of 25 November 2009 on the voluntary participation by organisations in a Community eco-management and audit scheme (EMAS), repealing Regulation (EC) No 761/2001 and Commission Decisions 2001/681/EC and 2006/193/EC (OJ L 342, 22.12.2009, p. 1).

ANNEX 2

STANDARD FORMAT OF THE ADVANCE NOTIFICATION FORM FOR WASTE DELIVERY TO PORT RECEPTION FACILITIES

Notification of the delivery of waste to: *(enter name of port of call, as referred to in Article 6 of Directive (EU) 2019/883)*

This form should be retained on board the ship along with the appropriate Oil Record Book, Cargo Record Book, Garbage Record Book or Garbage Management Plan as required by the MARPOL Convention.

1. SHIP PARTICULARS

1.1 Name of ship:	1.5 Owner or operator:
1.2 IMO number:	1.6 Distinctive number or letters:
	MMSI (Maritime Mobile Service Identity) number:
1.3 Gross tonnage:	1.7 Flag State:
1.4 Type of ship: ☐ Oil tanker ☐ Chemical tanker ☐ Bulk carrier ☐ Container ☐ Other cargo ship ☐ Passenger ship ☐ Ro-ro ☐ Other (specify)	

2. PORT AND VOYAGE PARTICULARS

2.1 Location/terminal name:	2.6 Last port where waste was delivered:
2.2 Arrival date and time:	2.7 Date of last delivery:
2.3 Departure date and time:	2.8 Next port of delivery:
2.4 Last port and country:	2.9 Person submitting this form (if other than the master):
2.5 Next port and country (if known):	

3. TYPE AND AMOUNT OF WASTE AND STORAGE CAPACITY

Type	Waste to be delivered (m^3)	Maximum dedicated storage capacity (m^3)	Amount of waste retained on board (m^3)	Port at which remaining waste will be delivered	Estimated amount of waste to be generated between notification and next port of call (m^3)
MARPOL Annex I – Oil					
Oily bilge water					
Oily residues (sludge)					
Oily tank washings					
Dirty ballast water					

Type	Waste to be delivered (m^3)	Maximum dedicated storage capacity (m^3)	Amount of waste retained on board (m^3)	Port at which remaining waste will be delivered	Estimated amount of waste to be generated between notification and next port of call (m^3)
Scale and sludge from tank cleaning					
Other (please specify)					
MARPOL Annex II – NOXIOUS LIQUID SUBSTANCES (NLS) (1)					
Category X substance					
Category Y substance					
Category Z substance					
OS – other substances					
MARPOL Annex IV – Sewage					
MARPOL Annex V – Garbage					
A. Plastics					
B. Food Waste					
C. Domestic waste (e.g. paper products, rags, glass, metal, bottles, crockery, etc.)					
D. Cooking Oil					
E. Incinerator ashes					
F. Operational waste					
G. Animal carcass(es)					
H. Fishing gear					
I. E-waste					

(1) Indicate the proper shipping name of the NLS involved.

Type	Waste to be delivered (m^3)	Maximum dedicated storage capacity (m^3)	Amount of waste retained on board (m^3)	Port at which remaining waste will be delivered	Estimated amount of waste to be generated between notification and next port of call (m^3)
J. Cargo residues (1) (Harmful to the Marine Environment – HME)					
K. Cargo residues (2) (non-HME)					
MARPOL Annex VI – Air Pollution related					
Ozone depleting substances and equipment containing such substances (3)					
Exhaust gas cleaning residues					

Other waste, not covered by MARPOL					
Passively fished waste					

Notes

1. This information shall be used for port State control and other inspection purposes.
2. This form is to be completed unless the ship is covered by an exemption in accordance with Article 9 of Directive (EU) 2019/883

(1) May be estimates. Indicate the proper shipping name of the dry cargo.
(2) May be estimates. Indicate the proper shipping name of the dry cargo.
(3) Arising from normal maintenance activities on board.

ANNEX 3

STANDARD FORMAT FOR THE WASTE DELIVERY RECEIPT

The designated representative of the port reception facility provider shall provide the following form to the master of a ship that has delivered waste in accordance with Article 7 of Directive (EU) 2019/883

This form shall be retained on board the ship along with the appropriate Oil Record Book, Cargo Record Book, Garbage Record Book or Garbage Management Plan as required by the MARPOL Convention.

1. PORT RECEPTION FACILITY AND PORT PARTICULARS

1.1. Location/terminal name:
1.2. Port reception facility provider(s):
1.3. Treatment facility provider(s) – if different from above:
1.4. Waste delivery date and time from: to:

2. SHIP PARTICULARS

2.1. Name of the ship:	2.5. Owner or operator:
2.2. IMO number:	2.6. Distinctive number or letters: MMSI (Maritime Mobile Service Identity) number:
2.3. Gross tonnage:	2.7. Flag State:
2.4. Type of ship: ☐ Oil tanker ☐ Chemical tanker ☐ Bulk carrier ☐ Container ☐ Other cargo ship ☐ Passenger ship ☐ Ro-ro ☐ Other (specify)	

3. TYPE AND AMOUNT OF WASTE RECEIVED

MARPOL Annex I – Oil	Quantity (m^3)
Oily bilge water	
Oily residues (sludge)	
Oily tank washings	
Dirty ballast water	
Scale and sludge from tank cleaning	
Other (please specify)	
MARPOL Annex II – NOXIOUS LIQUID SUBSTANCES (NLS)	Quantity (m^3)/ Name (1)
Category X substance	
Category Y substance	
Category Z substance	
OS – other substance	
MARPOL Annex IV – Sewage	Quantity (m^3)

MARPOL Annex V – Garbage	Quantity (m^3)
A. Plastics	
B. Food waste	
C. Domestic waste (e.g. paper products, rags, glass, metal, bottles, crockery, etc.)	
D. Cooking oil	
E. Incinerator ashes	
F. Operational waste	
G. Animal carcass(es)	
H. Fishing gear	
I. E-waste	
J. Cargo residues (2) (Harmful to the Marine Environment – HME)	
K. Cargo residues (2) (non-HME)	
MARPOL Annex VI – Air Pollution related	Quantity (m^3)
Ozone-depleting substances and equipment containing such substances	
Exhaust gas-cleaning residues	
Other waste, not covered by MARPOL	Quantity (m^3)
Passively fished waste	

(1) Indicate the proper shipping name of the NLS involved.
(2) Indicate the proper shipping name of the dry cargo.

ANNEX 4

CATEGORIES OF COSTS AND NET REVENUES RELATED TO THE OPERATION AND ADMINISTRATION OF PORT RECEPTION FACILITIES

Direct costs	Indirect costs	Net revenues
Direct operational costs that arise from the actual delivery of waste from ships, including the cost items listed below.	Indirect administrative costs that arise from the management of the system in the port, including the cost items listed below.	Net proceeds from waste management schemes and national/regional funding available, including the revenue elements listed below.
— Provision of port reception facilities infrastructure, including the containers, tanks, processing tools, barges, trucks, waste reception, treatment installations; — Concessions due for site leasing, if applicable, or for leasing the equipment necessary for the operation of port reception facilities; — The actual operation of the port reception facilities: collection of waste from the ship, transport of waste from the port reception facilities for final treatment, maintenance and cleaning of port reception facilities, costs for staff, including overtime, provision of electricity, waste analysis and insurance; — Preparing for reuse, recycling or disposal of the waste from ships, including separate collection of waste; — Administration: invoicing, issuing of waste delivery receipts to the ship, reporting.	— Development and approval of the waste reception and handling plan, including any audits of that plan and its implementation; — Updating the waste reception and handling plan, including labour costs and consultancy costs, where applicable; — Organising the consultation procedures for the (re)evaluation of the waste reception and handling plan; — Management of the notification and cost recovery systems, including the application of reduced fees for 'green ships', the provision of IT systems at port level, statistical analysis and associated labour costs; — Organisation of public procurement procedures for the provision of port reception facilities, as well as the issuing of the necessary authorisations for the provision of port reception facilities in ports; — Communication of information to port users through the distribution of flyers, putting up signs and posters in the port, or publication of the information on the port's website, and electronic transmission of the information as required in Article 5; — Management of waste management schemes: Extended Producer Responsibility (EPR) schemes, recycling and application for and implementing of national/regional funds; — Other administrative costs: costs of monitoring and electronic reporting of exemptions required in Article 9.	— Net financial benefits provided by extended producer responsibility schemes; — Other net revenues from waste management such as recycling schemes; — Funding under the European Maritime and Fisheries Fund (EMFF); — Other funding or subsidies available to ports for waste management and fisheries.

ANNEX 5

EXEMPTION CERTIFICATE PURSUANT TO ARTICLE 9 IN RELATION TO THE REQUIREMENTS UNDER ARTICLE 6, ARTICLE 7(1) AND ARTICLE 8 OF DIRECTIVE (EU) 2019/883 AT THE PORT[S] OF *[INSERT PORT]* IN *[INSERT MEMBER STATE]* [1]

Name of ship	Distinctive number or letters	Flag State
[*insert name of the ship*]	[*insert IMO number*]	[*insert name of the Flag State*]

is in scheduled traffic with frequent and regular port calls at the following port(s) located in [*insert name of the Member State*] according to a schedule or predetermined route:

[ ]

and calls at these ports at least once a fortnight:

[ ]

and has made an arrangement to ensure the payment of the fees and the delivery of waste to the port or a third party at the port of:

[ ]

and is thus exempted, in accordance with [*insert relevant provision in national legislation of the country*], [*from the requirements on*:

☐ *mandatory delivery of waste from ships*,

☐ *the advance waste notification, and*

☐ *the payment of the mandatory fee, at the following port(s):*]

This certificate is valid until [*insert date*], unless the grounds for issuing the certificate are changed before that date.

Place and date

.....

Name
Title

[1] Delete if not appropriate.

DIRECTIVE (EU) 2019/884 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 17 April 2019

amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA

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 82(1), second subparagraph, point (d) thereof,

Having regard to the proposal from the European Commission,

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

Acting in accordance with the ordinary legislative procedure ([1]),

Whereas:

(1) The Union has set itself the objective of offering its citizens an area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured. That objective should be achieved by means of, among others, appropriate measures to prevent and combat crime, including organised crime and terrorism.

(2) That objective requires that information on convictions handed down in the Member States be taken into account outside the convicting Member State in the course of new criminal proceedings, as laid down in Council Framework Decision 2008/675/JHA ([2]), as well as in order to prevent new offences.

(3) That objective presupposes the exchange of information extracted from criminal records between the competent authorities of the Member States. Such an exchange of information is organised and facilitated by the rules set out in Council Framework Decision 2009/315/JHA ([3]) and by the European Criminal Records Information System (ECRIS), established in accordance with Council Decision 2009/316/JHA ([4]).

(4) The existing ECRIS legal framework, however, does not sufficiently address the particularities of requests concerning third-country nationals. Although it is already possible to exchange information on third-country nationals through ECRIS, there is no common Union procedure or mechanism in place to do so efficiently, rapidly and accurately.

(5) Within the Union, information on third-country nationals is not gathered as it is for nationals of Member States — in the Member States of nationality- but only stored in the Member States where the convictions have been handed down. A complete overview of the criminal history of a third-country national can therefore be ascertained only if such information is requested from all Member States.

(6) Such 'blanket requests' impose a disproportionate administrative burden on all Member States, including those not holding information on the particular third-country national. In practice, that burden deters Member States from requesting information on third-country nationals from other Member States, which seriously hinders the exchange of information between them, limiting their access to criminal records information to information stored in their national register. As a consequence, the risk of information exchange between Member States being inefficient and incomplete is increased.

([1]) Position of the European Parliament of 12 March 2019 (not yet published in the Official Journal) and decision of the Council of 9 April 2019.

([2]) Council Framework Decision 2008/675/JHA of 24 July 2008 on taking account of convictions in the Member States of the European Union in the course of new criminal proceedings (OJ L 220, 15.8.2008, p. 32).

([3]) Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States (OJ L 93, 7.4.2009, p. 23).

([4]) Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA (OJ L 93, 7.4.2009, p. 33).

(7) In order to improve the situation, the Commission submitted a proposal, which led to the adoption of Regulation (EU) 2019/816 of the European Parliament and of the Council ([5]), which establishes a centralised system at Union level containing the personal data of convicted third-country nationals allowing identification of the Member States holding information on their previous convictions ('ECRIS-TCN').

(8) ECRIS-TCN will allow the central authority of a Member State to find out promptly and efficiently in which other Member States criminal records information on a third-country national is stored so that the existing ECRIS framework can be used to request the criminal records information from those Member States in accordance with Framework Decision 2009/315/JHA.

(9) The exchange of information on criminal convictions is important in any strategy to combat crime and counter terrorism. It would contribute to the criminal justice response to radicalisation leading to terrorism and violent extremism if Member States used ECRIS to its full potential.

(10) In order to increase the utility of information on convictions and disqualifications arising from convictions for sexual offences against children, Directive 2011/93/EU of the European Parliament and of the Council ([6]) laid down the obligation for Member States to take the necessary measures to ensure that for the purpose of recruiting a person for a post involving direct and regular contact with children, information concerning the existence of criminal convictions for sexual offences against children entered in the criminal records, or of any disqualifications arising from those criminal convictions, be transmitted in accordance with the procedures set out in Framework Decision 2009/315/JHA. The aim of that mechanism is to ensure that a person convicted of a sexual offence against children is not able to conceal that conviction or disqualification with a view to performing a professional activity involving direct and regular contact with children in another Member State.

(11) This Directive aims to introduce the necessary modifications to Framework Decision 2009/315/JHA that will allow for an effective exchange of information on convictions of third-country nationals via ECRIS. It obliges Member States to take the necessary measures to ensure that convictions are accompanied by information on the nationality, or nationalities, of the convicted person, in so far as the Member States have such information at their disposal. It also introduces procedures for replying to requests for information, ensures that a criminal records extract requested by a third-country national is supplemented with information from other Member States, and provides for the technical changes necessary to make the information exchange system work.

(12) Directive (EU) 2016/680 of the European Parliament and of the Council ([7]) should apply to the processing of personal data by competent national authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security. Regulation (EU) 2016/679 of the European Parliament and of the Council ([8]) should apply to the processing of personal data by national authorities when such processing does not fall within the scope of Directive (EU) 2016/680.

(13) In order to ensure uniform conditions for the implementation of Framework Decision 2009/315/JHA, the principles of Decision 2009/316/JHA should be incorporated in that Framework Decision and implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and the Council ([9]).

([5]) Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 (OJ L 135, 22.5.2019, p. 1).

([6]) Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).

([7]) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

([8]) 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).

([9]) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(14) The common communication infrastructure used for the exchange of criminal records information should be the secured Trans European Services for Telematics between Administrations (sTESTA), any further development of it or any alternative secure network.

(15) Notwithstanding the possibility of using the Union's financial programmes in accordance with the applicable rules, each Member State should bear its own costs arising from the implementation, administration, use and maintenance of its criminal records database, and from the implementation, administration, use and maintenance of the technical alterations needed to be able to use ECRIS.

(16) This Directive respects fundamental rights and freedoms enshrined, in particular, in the Charter of Fundamental Rights of the European Union, including the right to protection of personal data, the rights to judicial and administrative redress, the principle of equality before the law, the right to a fair trial, the presumption of innocence and the general prohibition of discrimination. This Directive should be implemented in accordance with those rights and principles.

(17) Since the objective of this Directive, namely to enable rapid and efficient exchange of accurate criminal records information on third-country nationals, cannot be sufficiently achieved by the Member States, but can rather, by putting in place common rules 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 (TEU). In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary to achieve that objective.

(18) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the TEU and to the Treaty on the Functioning of the European Union (TFEU), Denmark is not taking part in the adoption of this Directive and is not bound by it or subject to its application.

(19) In accordance with Articles 1 and 2 and Article 4a(1) of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the TEU and to the TFEU, and without prejudice to Article 4 of that Protocol, Ireland is not taking part in the adoption of this Directive and is not bound by it or subject to its application.

(20) In accordance with Article 3 and Article 4a(1) of Protocol No 21, the United Kingdom has notified its wish to take part in the adoption and application of this Directive.

(21) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council [10] and delivered an opinion on 13 April 2016 [11].

(22) Framework Decision 2009/315/JHA should therefore be amended accordingly,

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Amendments to Framework Decision 2009/315/JHA

Framework Decision 2009/315/JHA is amended as follows:

(1) Article 1 is replaced by the following:

'*Article 1*

Subject matter

This Framework Decision:

(a) defines the conditions under which a convicting Member State shares information with other Member States on convictions;

[10] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

[11] OJ C 186, 25.5.2016, p. 7.

(b) defines obligations for the convicting Member State and for the Member State of the convicted person's nationality (the "Member State of the person's nationality"), and specifies the methods to be followed when replying to a request for information extracted from criminal records;

(c) establishes a decentralised information technology system for the exchange of information on convictions based on the criminal records databases in each Member State, the European Criminal Records Information System (ECRIS).';

(2) in Article 2, the following points are added:

'(d) "convicting Member State" means the Member State where a conviction is handed down;

(e) "third-country national" means a person who is not a citizen of the Union within the meaning of Article 20(1) TFEU, or who is a stateless person or a person whose nationality is unknown;

(f) "fingerprint data" means the data relating to plain and rolled impressions of the fingerprints of each of a person's fingers;

(g) "facial image" means a digital image of a person's face;

(h) "ECRIS reference implementation" means the software developed by the Commission and made available to the Member States for the exchange of criminal records information through ECRIS.';

(3) in Article 4, paragraph 1 is replaced by the following:

'1. Each convicting Member State shall take all the necessary measures to ensure that convictions handed down within its territory are accompanied by information on the nationality or nationalities of the convicted person if the person is a national of another Member State or a third-country national. Where a convicted person is of unknown nationality or stateless, the criminal record shall reflect this.';

(4) Article 6 is amended as follows:

(a) paragraph 3 is replaced by the following:

'3. Where a national of one Member State asks the central authority of another Member State for information on his or her own criminal record, that central authority shall submit a request to the central authority of the Member State of the person's nationality for information and related data to be extracted from the criminal records and shall include such information and related data in the extract to be provided to the person concerned.';

(b) the following paragraph is inserted:

'3a. Where a third-country national asks the central authority of a Member State for information on his or her own criminal record, that central authority shall submit a request only to those central authorities of the Member States which hold information on the criminal record of that person for information and related data to be extracted from the criminal records and shall include such information and related data in the extract to be provided to the person concerned.';

(5) Article 7 is amended as follows:

(a) paragraph 4 is replaced by the following:

'4. Where information extracted from the criminal records on convictions handed down against a national of a Member State is requested under Article 6 from the central authority of a Member State other than the Member State of the person's nationality, the requested Member State shall transmit such information to the same extent as provided for in Article 13 of the European Convention on Mutual Assistance in Criminal Matters.';

(b) the following paragraph is inserted:

'4a. Where information extracted from the criminal records on convictions handed down against a third-country national is requested under Article 6 for the purposes of criminal proceedings, the requested Member State shall transmit information on any conviction handed down in the requested Member State and entered in the criminal records and on any conviction handed down in third countries and subsequently transmitted to it and entered into the criminal records.

If such information is requested for any purpose other than that of criminal proceedings, paragraph 2 of this Article shall apply accordingly.';

(6) in Article 8, paragraph 2 is replaced by the following:

'2. Replies to the requests referred to in Article 6(2), (3) and (3a) shall be transmitted within twenty working days from the date the request was received.';

(7) Article 9 is amended as follows:

(a) in paragraph 1, the words 'Article 7(1) and (4)' are replaced by 'Article 7(1), (4) and (4a)';

(b) in paragraph 2, the words 'Article 7(2) and (4)' are replaced by 'Article 7(2), (4) and (4a)';

(c) in paragraph 3, the words 'Article 7(1), (2) and (4)' are replaced by 'Article 7(1), (2), (4) and (4a)';

(8) Article 11 is amended as follows:

(a) in point (c) of the first subparagraph of paragraph 1, the following point is added:

'(iv) facial image.';

(b) paragraphs 3 to 7 are replaced by the following:

'3. Central authorities of Member States shall transmit the following information electronically using ECRIS and a standardised format in accordance with the standards to be laid down in implementing acts:

(a) information referred to in Article 4;

(b) requests referred to in Article 6;

(c) replies referred to in Article 7; and

(d) other relevant information.

4. If the mode of transmission referred to in paragraph 3 is not available, central authorities of Member States shall transmit all information referred to in paragraph 3 by any means capable of producing a written record under conditions allowing the central authority of the receiving Member State to establish the authenticity of the information, taking the security of transmission into consideration.

If the mode of transmission referred to in paragraph 3 is not available for an extended period of time, the Member State concerned shall inform the other Member States and the Commission.

5. Each Member State shall carry out the technical alterations necessary for its use of the standardised format to electronically transmit all information as referred to in paragraph 3 to other Member States via ECRIS. Each Member State shall notify the Commission of the date from which it will be able to carry out such transmissions.';

(9) the following Articles are inserted:

'*Article 11a*

European Criminal Records Information System (ECRIS)

1. In order to exchange information extracted from criminal records in accordance with this Framework Decision electronically, a decentralised information technology system based on the criminal records databases in each Member State, the European Criminal Records Information System (ECRIS), is established. It is composed of the following elements:

(a) ECRIS reference implementation;

(b) a common communication infrastructure between central authorities that provides an encrypted network.

To ensure the confidentiality and integrity of criminal records information transmitted to other Member States, appropriate technical and organisational measures shall be used, taking into account the state of the art, the cost of implementation and the risks posed by the processing of information.

2. All criminal records data shall be stored solely in databases operated by the Member States.

3. The central authorities of the Member States shall not have direct access to the criminal records databases of other Member States.

4. The ECRIS reference implementation and databases storing, sending and receiving information extracted from criminal records shall operate under the responsibility of the Member State concerned. The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) established by Regulation (EU) 2018/1726 of the European Parliament and of the Council (*) shall support the Member States in accordance with its tasks as laid down in Regulation (EU) 2019/816 of the European Parliament and of the Council (**).

5. The common communication infrastructure shall be operated under the responsibility of the Commission. It shall fulfil the necessary security requirements and fully meet the needs of ECRIS.

6. eu-LISA shall provide, further develop and maintain the ECRIS reference implementation.

7. Each Member State shall bear its own costs arising from the implementation, administration, use and maintenance of its criminal records database and the installation and use of the ECRIS reference implementation.

The Commission shall bear the costs arising from the implementation, administration, use, maintenance and future development of the common communication infrastructure.

8. The Member States which use their national ECRIS implementation software in accordance with paragraphs 4 to 8 of Article 4 of Regulation (EU) 2019/816 may continue to use their national ECRIS implementation software instead of the ECRIS reference implementation, provided that they fulfil all the conditions set out in those paragraphs.

Article 11b

Implementing Acts

1. The Commission shall lay down the following in implementing acts:

(a) the standardised format referred to in Article 11(3), including as regards information on the offence giving rise to the conviction and information on the content of the conviction;

(b) the rules concerning the technical implementation of ECRIS and the exchange of fingerprint data;

(c) any other technical means of organising and facilitating exchanges of information on convictions between central authorities of Member States, including:

(i) the means of facilitating the understanding and automatic translation of transmitted information;

(ii) the means by which information may be exchanged electronically, particularly as regards the technical specifications to be used and, if need be, any applicable exchange procedures.

2. The implementing acts referred to in paragraph 1 of this Article shall be adopted in accordance with the examination procedure referred to in Article 12a(2).

_____

(*) Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011 (OJ L 295, 21.11.2018, p. 99).

(**) Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 (OJ L 135, 22.5.2019, p. 1).';

(10) the following Article is inserted:

'*Article 12a*

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Where the committee delivers no opinion, the Commission shall not adopt the draft implementing act and the third subparagraph of Article 5(4) of Regulation (EU) No 182/2011 shall apply.';

(11) the following Article is inserted:

'*Article 13a*

Reporting by the Commission and review

1. By 29 June 2023, the Commission shall submit a report on the application of this Framework Decision to the European Parliament and to the Council. The report shall assess the extent to which the Member States have taken the necessary measures to comply with this Framework Decision, including its technical implementation.

2. The report shall be accompanied, where appropriate, by relevant legislative proposals.

3. The Commission shall regularly publish a report concerning the exchange of information extracted from the criminal record through ECRIS and concerning the use of ECRIS-TCN based in particular on the statistics provided by eu-LISA and the Member States in accordance with Regulation (EU) 2019/816. The report shall be published for the first time one year after the report referred to in paragraph 1 is submitted.

4. The Commission report referred to in paragraph 3 shall cover in particular the level of exchange of information between Member States, including that relating to third-country nationals, as well as the purpose of requests and their respective number, including requests for purposes other than criminal proceedings, such as background checks and requests for information from the persons concerned on their own criminal record.'.

Article 2

Replacement of Decision 2009/316/JHA

Decision 2009/316/JHA is replaced with regard to the Member States bound by this Directive, without prejudice to the obligations of those Member States with regard to the date for implementation of that Decision.

Article 3

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 28 June 2022. They shall immediately communicate the text of those measures to the Commission.

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

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

3. Member States shall carry out the technical alterations referred to in Article 11(5) of Framework Decision 2009/315/JHA, as amended by this Directive, by 28 June 2022.

Article 4

Entry into force and application

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

Article 2 shall apply from 28 June 2022.

Article 5

Addressees

This Directive is addressed to the Member States in accordance with the Treaties.

Done at Strasbourg, 17 April 2019.

For the European Parliament	*For the Council*
The President	*The President*
A. TAJANI	G. CIAMBA

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

Publications Office of the European Union
2985 Luxembourg
LUXEMBOURG

EN