Official Journal of the European Union

L 295

English edition

Legislation

Volume 61

21 November 2018

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) 2018/1724 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 2 October 2018

establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012

(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 21(2) and Article 114(1) 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 internal market is one of the Union's most tangible achievements. By allowing people, goods, services and capital to move freely it offers new opportunities for citizens and businesses. This Regulation is a key element of the Single Market Strategy established by the communication of the Commission of 28 October 2015 entitled 'Upgrading the Single Market: more opportunities for people and business'. That strategy has the objective of unlocking the full potential of the internal market by making it easier for citizens and businesses to move within the Union and to trade, establish themselves and expand their businesses across borders.

(2) The communication of the Commission of 6 May 2015 entitled 'A Digital Single Market Strategy for Europe' recognised the role of the internet and digital technologies in transforming our lives, changing the way in which citizens and businesses access information, acquire knowledge, buy goods and services, participate in the market and work, thereby facilitating opportunities for innovation, growth and jobs. That communication, along with several resolutions adopted by the European Parliament, acknowledged that the needs of citizens and businesses in their own country and across borders could be better met by extending and integrating existing European-level portals, websites, networks, services and systems and by linking them with different national solutions, thereby creating a single digital gateway serving as a European single entry point ('the gateway'). The communication of the Commission of 19 April 2016 entitled 'EU eGovernment Action Plan 2016-2020 — Accelerating the digital transformation of government' listed the gateway amongst one of its actions for 2017. The Commission's report of 24 January 2017, entitled 'Strengthening Citizens' Rights in a Union of Democratic Change — EU Citizenship Report 2017' considered the gateway to be a priority for the rights of the Union's citizens.

(3) The European Parliament and the Council have repeatedly called for a more comprehensive and more user-friendly package of information and assistance to help citizens and businesses navigate the internal market and to strengthen and streamline internal market tools in order to better meet the needs of citizens and businesses in their cross-border activities.

([1]) OJ C 81, 2.3.2018, p. 88.
([2]) Position of the European Parliament of 13 September 2018 (not yet published in the Official Journal) and decision of the Council of 27 September 2018.

(4) This Regulation responds to those calls by offering citizens and businesses easy access to the information, the procedures, and the assistance and problem-solving services that they need in order to exercise their rights in the internal market. The gateway could contribute to the greater transparency of rules and regulations relating to different business and life events, in areas such as travel, retirement, education, employment, healthcare, consumer rights and family rights. Furthermore, it could help improve consumers' confidence, address the lack of knowledge about consumer protection and internal market rules and reduce compliance costs for businesses. This Regulation establishes a user-friendly, interactive gateway which, based on users' needs, should guide them to the most appropriate services. In that context, the Commission and Member States should play an important role in achieving those objectives.

(5) The gateway should facilitate interactions between citizens and businesses, on the one hand, and competent authorities, on the other hand, by providing access to online solutions, facilitating the day-to-day activities of citizens and businesses and minimising the obstacles encountered in the internal market. The existence of a single digital gateway providing online access to accurate and up-to-date information, to procedures and to assistance and problem-solving services could help raise the users' awareness of the different existing online services and could save them time and expense.

(6) This Regulation has three objectives, namely to reduce any additional administrative burden on citizens and businesses that exercise or want to exercise their internal market rights, including the free movement of citizens, in full compliance with national rules and procedures, to eliminate discrimination and to ensure the functioning of the internal market with regard to the provision of information, of procedures and of assistance and problem-solving services. Since it covers free movement of citizens, which cannot be considered to be merely incidental, this Regulation should be based on Article 21(2) and Article 114(1) of the Treaty on the Functioning of the European Union (TFEU).

(7) In order for Union citizens and businesses to enjoy their right to free movement within the internal market, the Union should adopt specific, non-discriminatory measures allowing citizens and businesses to have easy access to sufficiently comprehensive and reliable information about their rights under Union law and to information about the applicable national rules and procedures which they need to comply with when they move to, live or study, or when they establish or carry on a business, in a Member State other than their own. Information should be considered to be sufficiently comprehensive if it includes all the information that is necessary for the users to understand what their rights and obligations are and identifies the rules that apply to them in relation to the activities they want to undertake as cross-border users. The information should be stated in a clear, concise and understandable way and be operational and well adapted to the target user group. Information on procedures should cover all foreseeable procedural steps that are relevant for the user. It is important for citizens and businesses facing complex regulatory environments, such as those active in e-commerce and the collaborative economy, that they can easily find the applicable rules and how they apply to their activities. Easy and user-friendly access to information means enabling the users to easily find the information, to easily identify which parts of the information are relevant for their particular situation and to easily understand the relevant information. The information to be provided at national level should not only concern national rules implementing Union law, but also any other national rules that apply both to non-crossborder and cross-border users.

(8) Rules on the provision of information in this Regulation should not apply to national judicial systems, since information in that area relevant for cross-border users is already included in the e-Justice portal. In some situations covered by this Regulation, courts should be considered to be competent authorities, for instance where courts are managing business registers. In addition, the non-discrimination principle should also apply to online procedures that give access to court proceedings.

(9) It is clear that citizens and businesses from other Member States can be at a disadvantage due to their lack of familiarity with the national rules and administrative systems, the different languages used and their lack of geographic proximity to the competent authorities in a Member State other than their own. The most efficient way to reduce the ensuing obstacles to the internal market is to enable cross-border and non-crossborder users to access information online in a language they are able to understand in order to enable them to complete procedures for compliance with national rules fully online and to offer them assistance where rules and procedures are not clear enough or where they encounter obstacles to the exercise of their rights.

(10) A number of Union acts have aimed to provide solutions by creating sectorial one-stop shops, including points of single contact established by Directive 2006/123/EC of the European Parliament and of the Council ([1]) which offer online information, assistance services and access to procedures relevant for the provision of services; Product Contact Points, established by Regulation (EC) No 764/2008 of the European Parliament and of the Council ([2]), and Product Contact Points for Construction, established by Regulation (EU) No 305/2011 of the European Parliament and of the Council ([3]), which provide access to product-specific technical rules; and national assistance centres for professional qualifications, established by Directive 2005/36/EC of the European Parliament and of the Council ([4]), which assist professionals moving cross-border. In addition, networks have been established, such as European Consumer Centres, in order to promote the understanding of Union consumers' rights and to assist in resolving complaints about purchases made in other Member States within the network, when travelling or shopping online. Furthermore, SOLVIT as referred to in Commission Recommendation 2013/461/EU ([5]) seeks to deliver fast, effective and informal solutions to individuals and businesses when their internal market rights are denied by public authorities. Finally, several information portals, such as Your Europe, in respect of the internal market, and the e-Justice portal, in relation to the area of justice, were established to inform users about Union and national rules.

(11) As a result of the sectorial nature of those Union acts, the current provision of online information and of assistance and problem-solving services together with online procedures for citizens and businesses remains very fragmented. There are discrepancies in the availability of online information and procedures, there is a lack of quality in relation to the services and a lack of awareness regarding that information and those assistance and problem-solving services. Cross-border users also experience problems finding and accessing those services.

(12) This Regulation should establish a single digital gateway to act as the single entry point through which citizens and businesses are able to access information about the rules and requirements that they have to comply with, by virtue of Union or national law. The gateway should simplify citizens' and businesses' contact with the assistance and problem-solving services established at Union or national level and make that contact more effective. The gateway should also facilitate access to and completion of online procedures. This Regulation should not affect in any way the existing rights and obligations under Union or national law within those policy areas. For the procedures listed in Annex II to this Regulation and the procedures provided for in Directives 2005/36/EC and 2006/123/EC, and in Directives 2014/24/EU ([6]) and 2014/25/EU ([7]) of the European Parliament and of the Council, this Regulation should support the use of the 'once-only' principle and should fully respect the fundamental right to the protection of personal data, for the purpose of the exchange of evidence between competent authorities in different Member States.

(13) The gateway and its content should be user-centric and user-friendly. The gateway should aim to avoid overlaps and should provide links to existing services. It should allow citizens and businesses to interact with public bodies at national and Union level by providing them with the opportunity to give feedback in relation to both the services offered through the gateway and the functioning of the internal market as they experience it. The feedback tool should enable the user to point out, in a way that makes it possible for the user to remain anonymous, perceived problems, deficiencies and needs in order to encourage the continuous improvement of the quality of the services.

([1]) 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).

([2]) Regulation (EC) No 764/2008 of the European Parliament and of the Council of 9 July 2008 laying down procedures relating to the application of certain national technical rules to products lawfully marketed in another Member State and repealing Decision No 3052/95/EC (OJ L 218, 13.8.2008, p. 21).

([3]) Regulation (EU) No 305/2011 of the European Parliament and of the Council of 9 March 2011 laying down harmonised conditions for the marketing of construction products and repealing Council Directive 89/106/EEC (OJ L 88, 4.4.2011, p. 5).

([4]) Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications (OJ L 255, 30.9.2005, p. 22).

([5]) Commission Recommendation 2013/461/EU of 17 September 2013 on the principles governing SOLVIT (OJ L 249, 19.9.2013, p. 10).

([6]) 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).

([7]) 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).

(14) The success of the gateway will depend on the joint effort of the Commission and the Member States. The gateway should include a common user interface integrated into the existing Your Europe portal, to be managed by the Commission. The common user interface should provide links to information, to procedures and to assistance or problem-solving services available on portals managed by competent authorities in Member States and by the Commission. In order to facilitate the use of the gateway, the common user interface should be available in all official languages of the institutions of the Union ('official languages of the Union'). The existing Your Europe portal and its main access webpage, adapted to the requirements of the gateway, should preserve this multilingual approach to the information provided. The functioning of the gateway should be supported by technical tools developed by the Commission in close cooperation with the Member States.

(15) In the Charter for the electronic Points of Single Contact under Directive 2006/123/EC, which was endorsed by the Council in 2013, Member States made a voluntary commitment to take a user-centric approach in the provision of information through the points of single contact, in order to cover areas of particular importance for businesses including VAT, income taxes, social security or labour law requirements. Based on the Charter and in the light of experience with the Your Europe portal, that information should also include a description of the assistance and problem-solving services. Citizens and businesses should be able to refer to such services when they have problems understanding the information, applying that information to their situation or completing a procedure.

(16) This Regulation should list the information areas which are relevant for citizens and businesses exercising their rights and complying with their obligations within the internal market. For those areas, sufficiently comprehensive information should be provided at national level, including at regional and local levels, and at Union level, explaining the applicable rules and obligations and the procedures to be completed by citizens and businesses in order to comply with those rules and obligations. In order to ensure the quality of the services offered, the information provided through the gateway should be clear, accurate and up-to-date, the use of complex terminology should be minimised and the use of acronyms should be limited to those which provide simplified and easily understandable terms that do not require a pre-existing knowledge of the issue or area of law. That information should be provided in such a way that users can easily understand the basic rules and requirements applicable to their situation in such areas. Users should also be informed about the absence, in certain Member States, of national rules in the information areas listed in Annex I, especially where those areas are subject to national rules in other Member States. Such information about the absence of national rules could be included in the Your Europe portal.

(17) Wherever possible, information already collected by the Commission from the Member States under existing Union law or voluntary arrangements — such as information collected for the EURES portal, established by Regulation (EU) 2016/589 of the European Parliament and of the Council ([1]), the e-Justice portal, established by Council Decision 2001/470/EC ([2]), or the Regulated professions database, established by Directive 2005/36/EC — should be used to cover part of the information to be made accessible to citizens and businesses at Union and national level in accordance with this Regulation. Member States should not be required to provide on their national websites information which is already available in the relevant databases managed by the Commission. Where Member States already have to provide online information pursuant to other Union acts, such as Directive 2014/67/EU of the European Parliament and of the Council ([3]), it should be sufficient for Member States to provide links to the existing online information. Where certain policy areas have already been fully harmonised through Union law, for instance consumer rights, information provided at Union level should generally be sufficient for users to be able to understand their relevant rights or obligations. In such cases, Member States should be required only to provide additional information regarding their national administrative procedures and assistance services or any other

([1]) Regulation (EU) 2016/589 of the European Parliament and of the Council of 13 April 2016 on a European network of employment services (EURES), workers' access to mobility services and the further integration of labour markets, and amending Regulations (EU) No 492/2011 and (EU) No 1296/2013 (OJ L 107, 22.4.2016, p. 1).

([2]) Council Decision 2001/470/EC of 28 May 2001 establishing a European Judicial Network in civil and commercial matters (OJ L 174, 27.6.2001, p. 25).

([3]) Directive 2014/67/EU of the European Parliament and of the Council of 15 May 2014 on the enforcement of Directive 96/71/EC concerning the posting of workers in the framework of the provision of services and amending Regulation (EU) No 1024/2012 on administrative cooperation through the Internal Market Information System ('the IMI Regulation') (OJ L 159, 28.5.2014, p. 11),

national administrative rules if it is relevant for users. Information regarding consumer rights, for instance, should not affect contract law, but should rather inform users about their rights under Union and national law in the context of commercial transactions.

(18) This Regulation should enhance the internal market dimension of online procedures, and thereby contribute to the digitalisation of the internal market, by upholding the general principle of non-discrimination, inter alia, in relation to the access by citizens or businesses to online procedures already established at national level on the basis of Union or national law and to procedures that are to be made available fully online in accordance with this Regulation. Where a user, in a situation exclusively confined to a single Member State, is able to access and complete a procedure online in that Member State in an area covered by this Regulation, a cross-border user should also be able to access and complete that procedure online, either by using the same technical solution or an alternative, technically separate solution leading to the same outcome, without any discriminatory obstacles. Such obstacles might consist of nationally-designed solutions, such as using form fields that require national phone numbers, national prefixes for phone numbers or national postal codes, payment of fees that can only be done through systems which do not provide for cross-border payments, the lack of detailed explanations in a language understood by cross-border users, the lack of possibilities to submit electronic evidence from authorities located in another Member State and the lack of acceptance of electronic means of identification issued in other Member States. Member States should provide solutions for those obstacles.

(19) When users are completing online procedures across borders, they should be able to receive all the relevant explanations in an official language of the Union that is broadly understood by the largest possible number of cross-border users. This does not mean that Member States are required to translate their administrative forms related to the procedure, or the output of that procedure, into that language. Member States are however encouraged to use technical solutions which would allow users to complete the procedures in as many cases as possible, in that language, while respecting the Member States' rules on the use of languages.

(20) The online national procedures that are relevant for cross-border users to enable them to exercise their internal market rights depend on whether they are resident or established in the Member State concerned, or want to access the procedures of that Member State while being resident or established in another Member State. This Regulation should not prevent Member States from requiring that cross-border users who are resident or established on their territory obtain a national identification number in order to get access to the online national procedures, provided this does not entail an unjustifiable additional burden or cost for those users. For cross-border users who are not resident or established in the Member State concerned, online national procedures that are not relevant for the exercise of their internal market rights, for instance enrolment in order to receive local services, such as garbage collection and parking permits, do not need to be made fully accessible online.

(21) This Regulation should build on Regulation (EU) No 910/2014 of the European Parliament and of the Council ([1]), which lays down conditions under which Member States recognise certain electronic identification means for natural and legal persons subject to a notified electronic identification scheme of another Member State. Regulation (EU) No 910/2014 lays down the conditions subject to which users are permitted to use their means of electronic identification and authentication to access online public services in cross-border situations. Union institutions, bodies, offices and agencies are encouraged to accept means of electronic identification and authentication for the procedures for which they are responsible.

(22) A number of sectorial Union acts such as Directives 2005/36/EC, 2006/123/EC, 2014/24/EU and 2014/25/EU require that procedures are made fully available online. This Regulation should require a number of other procedures of key importance to the majority of citizens and businesses exercising their rights and complying with their obligations across borders to be fully made available online.

([1]) 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).

(23) In order to allow citizens and businesses to directly enjoy the benefits of the internal market without incurring an unnecessary additional administrative burden, this Regulation should require a full digitalisation of the user interface of certain key procedures for cross-border users, which are listed in Annex II to this Regulation. This Regulation should also lay down the criteria for determining how those procedures qualify as fully online. The obligation to make such a procedure fully available online should only apply where the procedure has been established in the Member State concerned. This Regulation should not cover the initial registration of a business activity, the procedures leading to the constitution of companies or firms as legal entities or any subsequent filing by such companies or firms, since such procedures necessitate a comprehensive approach aimed at facilitating digital solutions throughout a company's lifecycle. When businesses establish themselves in another Member State, they are required to register with a social security scheme and an insurance scheme in order to register their employees and pay contributions to both schemes. They might need to notify their business activities, obtain permissions or register changes to their business activity. Those procedures are common for businesses operating in many sectors of the economy, and it is therefore appropriate to require that those procedures are made available online.

(24) This Regulation should clarify what offering a procedure fully online entails. A procedure should be considered to be fully online if the user can take all steps, from access to completion, interacting with the competent authority, the 'front office', electronically, at a distance and through an online service. This online service should guide the user through a list of all the requirements to be fulfilled and all supporting evidence to be provided, should enable the user to provide the information and proof of compliance with all such requirements and should provide an automatic acknowledgement of receipt to the user, unless the output of the procedure is delivered immediately. This should not prevent competent authorities from contacting the users directly, where necessary in order to obtain further clarifications needed for the procedure. The output of the procedure, as set out in this Regulation, should also be provided by the competent authorities to the user in an electronic way, where possible under applicable Union and national law.

(25) This Regulation should not affect the substance of the procedures listed in Annex II which are established at national, regional or local level and does not lay down material or procedural rules within the areas covered by Annex II, including the area of taxation. The purpose of this Regulation is to lay down the technical requirements in order to ensure that such procedures, where they have been established in the Member State concerned, are made available fully online.

(26) This Regulation should not affect the competences of national authorities in any procedure, including the verification of the accuracy and the validity of information or evidence submitted and the verification of authenticity where evidence is submitted by means other than the technical system based on the 'once-only' principle. This Regulation should also not affect the procedural workflows within and between the competent authorities, the 'back office', whether digitalised or not. Where necessary, as part of some of the procedures for registering changes of business activities, Member States should continue to be able to require the involvement of notaries or lawyers who might want to use means of verification including videoconference or other online means that provide real-time audiovisual connection. However, such involvement should not prevent the completion of procedures for registering such changes in their entirety online.

(27) In some cases users might be required to submit evidence to prove facts that cannot be established by online means. Such evidence could include a medical certificate, proof of being alive, proof of roadworthiness of motor vehicles or confirmation of their chassis numbers. Provided that such evidence can be submitted in electronic format, this should not constitute an exception to the principle that a procedure should be offered fully online. In other cases, it might still be necessary for users of a procedure to appear in person before a competent authority as part of an online procedure. Any such exceptions, other than those resulting from Union law, should be limited to situations which are justified by an overriding reason of public interest in the areas of public security, public health or the fight against fraud. In order to ensure transparency, Member States should share with the Commission and the other Member States information about such exceptions and the grounds on which, and circumstances in which, they can be applied. Member States should not be required to report about each individual case in which, exceptionally, physical presence was required, but should rather communicate the national provisions which provide for such cases. Best practices at national level and technical developments allowing further digitalisation in this regard should be discussed regularly in a gateway coordination group.

(28) In cross-border situations, the procedure to register a change of address might consist of two separate procedures, one in the Member State of origin to request deregistration from the old address, and the other in the Member State of destination to request registration at the new address. Both procedures should be covered by this Regulation.

(29) Since the digitalisation of requirements, procedures and formalities relating to the recognition of professional qualifications is already covered by Directive 2005/36/EC, this Regulation should only cover the digitalisation of the procedure to request the academic recognition of diplomas, certificates or other proof of courses completed with regard to a person wishing to begin or to continue studying, or to use an academic title outside the formalities relating to the recognition of professional qualifications.

(30) This Regulation should not affect the social security coordination rules set out in Regulations (EC) No 883/2004 ([1]) and (EC) No 987/2009 ([2]) of the European Parliament and of the Council, which define the rights and obligations of insured persons and social security institutions, as well as the procedures applicable in the field of social security coordination.

(31) Several networks and services have been established at Union and national level to assist citizens and businesses in their cross-border activities. It is important that those services, including existing assistance or problem-solving services established at Union level, such as the European Consumer Centres, Your Europe Advice, SOLVIT, the Intellectual Property Rights helpdesk, Europe Direct and the Enterprise Europe Network, form part of the gateway in order to ensure that all potential users can find them. The services listed in Annex III were established by binding Union acts, whilst other services operate on a voluntary basis. Services established by binding Union acts should be bound by the quality requirements laid down in this Regulation. Services operated on a voluntary basis should comply with those quality requirements if the intention is to make them accessible through the gateway. The scope and nature of those services, their governance arrangements, existing deadlines, and the voluntary, contractual or other basis on which they operate should not be altered by this Regulation. For instance, where the assistance that they provide is of an informal nature, this Regulation should not have the effect of changing such assistance into legal advice of a binding nature.

(32) Furthermore, the Member States and the Commission should be able to add to the gateway other national assistance or problem-solving services provided by competent authorities or by private or semi-private entities, or public bodies, such as chambers of commerce or non-governmental assistance services for citizens, under the conditions laid down in this Regulation. In principle, competent authorities should be responsible for assisting citizens and businesses with any queries they have in relation to applicable rules and procedures that cannot be fully addressed by online services. However, in very specialised areas and where the service provided by private or semi-private bodies meets the users' needs, Member States can propose to the Commission that it includes such services in the gateway, provided that those services meet all conditions laid down in this Regulation and do not duplicate the assistance or problem-solving services already included.

(33) In order to assist users to identify the appropriate service, this Regulation should provide an assistance service finder that automatically guides users to the right service.

(34) Compliance with a minimum list of quality requirements is essential for the success of the gateway in order to ensure that the provision of information or services is reliable, since, otherwise, the credibility of the gateway as a whole would be seriously undermined. The overarching objective of compliance is to ensure that the information or service is presented in a clear and user-friendly way. It is the responsibility of the Member States to determine how information is presented over the course of the user journey in order to meet this objective. For instance, while it is helpful for users to be informed, before launching a procedure, about the generally available means of redress when a procedure results in a negative outcome, it is much more user-friendly to provide any specific information about the possible steps to take in such a case at the end of the procedure.

([1]) Regulation (EC) No 883/2004 of the European Parliament and of the Council of 29 April 2004 on the coordination of social security systems (OJ L 166, 30.4.2004, p. 1).

([2]) Regulation (EC) No 987/2009 of the European Parliament and of the Council of 16 September 2009 laying down the procedure for implementing Regulation (EC) No 883/2004 on the coordination of social security systems (OJ L 284, 30.10.2009, p. 1).

(35) The accessibility of information for cross-border users can be substantially improved where that information is made available in an official language of the Union broadly understood by the largest possible number of cross-border users. This language should in most cases be the foreign language most widely studied by users across the Union, but in some specific cases, more particularly in the case of information to be provided at local level by small municipalities close to the border of a Member State, the most suitable language may be the one used as a first language by the cross-border users in the neighbouring Member State. The translation from the official language or languages of the Member State in question into this other official language of the Union should accurately reflect the content of the information provided in the original language or languages. Translation may be limited to the information that users need in order to understand the basic rules and requirements that apply to their situation. While Member States should be encouraged to translate as much information as possible into an official language of the Union that is broadly understood by the largest possible number of cross-border users, the volume of information to be translated under this Regulation will depend on the financial resources available for this purpose, in particular those from the Union budget. The Commission should make the appropriate arrangements to ensure the efficient delivery of translations to the Member States at their request. The gateway coordination group should discuss and provide guidance on the official language or languages of the Union into which such information should be translated.

(36) In accordance with Directive (EU) 2016/2102 of the European Parliament and of the Council ([1]), Member States are required to ensure that the websites of their public bodies are accessible in accordance with the principles of perceivability, operability, understandability and robustness and that they comply with the requirements laid down in that Directive. The Commission and the Member States should ensure compliance with the United Nations Convention on the Rights of Persons with Disabilities, in particular Articles 9 and 21 thereof, and, in order to foster access to information for persons with intellectual disabilities, alternatives in easy-to-read language should be provided to the greatest possible extent in accordance with the principle of proportionality. The Member States, by ratifying, and the Union, by concluding ([2]), that Convention, have committed themselves to taking appropriate measures to ensure access for persons with disabilities, on an equal basis with others, to new information and communication technologies and systems, including the internet, by facilitating access to information for persons with intellectual disabilities, providing alternatives in easy-to-read language to the greatest possible extent and proportionately.

(37) Directive (EU) 2016/2102 does not apply to websites and mobile applications of Union institutions, bodies, offices and agencies, but the Commission should ensure that the common user interface and the webpages under its responsibility that are to be included in the gateway are accessible to persons with disabilities, meaning that they are perceivable, operable, understandable and robust. Perceivability means that information and the common user interface components must be presentable to users in ways they can perceive; operability means that the common user interface components and navigation must be operable; understandability means that information and the operation of the common user interface must be understandable; and robustness means that content must be robust enough to be interpreted reliably by a wide variety of user agents, including assistive technologies. In respect of the terms perceivable, operable, understandable and robust, the Commission is encouraged to comply with the relevant harmonised standards.

(38) In order to facilitate the payment of fees required as part of online procedures or for the provision of assistance or problem-solving services, cross-border users should be able to use credit transfers or direct debits as specified in Regulation (EU) No 260/2012 of the European Parliament and of the Council ([3]) or other generally used cross-border payment means including debit or credit cards.

(39) It is useful for users to be informed about the expected time a procedure may take. Accordingly, users should be informed about applicable deadlines or tacit approval or administrative silence arrangements or, if these are not applicable, at least of the average, estimated or indicative time that the procedure in question usually requires. Such estimates or indications should only help the users in planning their activities or any subsequent administrative steps and should have no legal effect.

([1]) 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).

([2]) Council Decision 2010/48/EC of 26 November 2009 concerning the conclusion, by the European Community, of the United Nations Convention on the Rights of Persons with Disabilities (OJ L 23, 27.1.2010, p. 35).

([3]) Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009 (OJ L 94, 30.3.2012, p. 22).

(40) This Regulation should also allow for the verification of the evidence provided in electronic format by the users, where that evidence is submitted without electronic seal or certification from the issuing competent authority, or where the technical tool established by this Regulation or another system enabling the direct exchange or verification of evidence between competent authorities of different Member States is not available. For such cases, this Regulation should provide for an effective mechanism for administrative cooperation among the competent authorities of the Member States, based on the Internal Market Information System ('IMI') established by Regulation (EU) No 1024/2012 of the European Parliament and of the Council ([1]). In such cases, the decision of a competent authority to use IMI should be voluntary, but once that authority has submitted a request for information or cooperation through IMI, the requested competent authority should be bound to cooperate and to provide a response. The request can be sent through IMI either to the competent authority issuing the evidence or to the central authority to be designated by Member States in accordance with their own administrative rules. To avoid unnecessary duplication and as Regulation (EU) 2016/1191 of the European Parliament and of the Council ([2]) covers part of the evidence relevant for the procedures covered by this Regulation, the cooperation arrangements for IMI laid down in Regulation (EU) 2016/1191 can also be used for the purpose of other evidence required in procedures covered by this Regulation. In order to allow Union bodies, offices or agencies to become actors within IMI, Regulation (EU) No 1024/2012 should be amended.

(41) Online services provided by competent authorities are crucial for increasing the quality and security of the services provided to citizens and businesses. Public administrations within Member States are increasingly working towards the reuse of data, dispensing with the requirement that citizens and businesses supply the same information several times. The reuse of data should be facilitated for cross-border users in order to reduce additional burden.

(42) In order to enable the lawful cross-border exchange of evidence and information by means of the Union-wide application of the 'once-only' principle, the application of this Regulation and of the 'once-only' principle should comply with all applicable data protection rules, including the principle of data minimisation, accuracy, storage limitation, integrity and confidentiality, necessity, proportionality and purpose limitation. Its implementation should also comply fully with the principles of security by design and of privacy by design, and should also respect the fundamental rights of individuals, including those related to fairness and transparency.

(43) Member States should ensure that users of procedures are provided with clear information on how personal data relating to them will be processed in accordance with Articles 13 and 14 of Regulation (EU) 2016/679 of the European Parliament and of the Council ([3]) and Articles 15 and 16 of Regulation (EU) 2018/1725 ([4]).

(44) In order to further facilitate the use of online procedures, this Regulation should, in line with the 'once-only' principle, provide the basis for the creation and use of a fully operational, safe and secure technical system for the automated cross-border exchange of evidence between the actors involved in the procedure, where this is explicitly requested by citizens and businesses. Where the exchange of evidence includes personal data, the request should be considered to be explicit if it contains a freely given, specific, informed and unambiguous indication of the individual's wish to have the relevant personal data exchanged, either by statement or by affirmative action. If the user is not the person concerned by the data, the online procedure should not affect his or her rights under Regulation (EU) 2016/679. The cross-border application of the 'once-only' principle should result in citizens and businesses not having to supply the same data to public authorities more than once, and that it should also be possible to use those data at the request of the user for the purposes of completing cross-border online procedures involving cross-border users. For the issuing competent authority, the obligation to use the technical system for the automated exchange of evidence between different Member States should apply only where authorities lawfully issue, in their own Member State, evidence in an electronic format that makes such an automated exchange possible.

([1]) Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC ('the IMI Regulation') (OJ L 316, 14.11.2012, p. 1).

([2]) Regulation (EU) 2016/1191 of the European Parliament and of the Council of 6 July 2016 on promoting the free movement of citizens by simplifying the requirements for presenting certain public documents in the European Union and amending Regulation (EU) No 1024/2012 (OJ L 200, 26.7.2016, p. 1).

([3]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

([4]) 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 (see page 39 of this Official Journal).

(45) Any cross-border exchange of evidence should have an appropriate legal basis such as Directive 2005/36/EC, 2006/123/EC, 2014/24/EU or 2014/25/EU or, for the procedures listed in Annex II, other applicable Union or national law.

(46) It is appropriate that this Regulation lays down, as a general rule, that the cross-border automated exchange of evidence takes place at the explicit request of the user. However, this requirement should not apply where the relevant Union or national law allows for automated cross-border data exchange without an explicit user request.

(47) The use of the technical system established by this Regulation should remain voluntary and the user should remain free to submit evidence by other means outside the technical system. The user should have the possibility to preview the evidence and the right to choose not to proceed with the exchange of evidence in cases where the user, after previewing the evidence to be exchanged, discovers that the information is inaccurate, out-of-date, or goes beyond what is necessary for the procedure in question. The data included in the preview should not be stored longer than is technically necessary.

(48) The secure technical system that should be set up to enable the exchange of evidence under this Regulation should also give requesting competent authorities certainty that the evidence has been provided by the right issuing authority. Before accepting information provided by a user in the context of a procedure, the competent authority should be able to verify the information where it gives rise to doubts, and to conclude that it is accurate.

(49) A number of building blocks offering basic capabilities exist that can be used to set up the technical system, such as the Connecting Europe Facility, established by Regulation (EU) No 1316/2013 of the European Parliament and of the Council ([1]), and the eDelivery and eID building blocks that form a part of that facility. Those building blocks consist of technical specifications, sample software and supporting services, and aim to ensure interoperability between the existing information and communication technology (ICT) systems in different Member States so that citizens, businesses and administrations, wherever they are in the Union, can benefit from seamless digital public services.

(50) The technical system established by this Regulation should be available in addition to other systems providing mechanisms for cooperation between authorities, such as IMI, and should not affect other systems, including the system provided for in Regulation (EC) No 987/2009, the European Single Procurement Document, under Directive 2014/24/EU, the Electronic Exchange of Social Security Information, under Regulation (EC) No 987/2009, the European Professional Card, under Directive 2005/36/EC, the interconnection of national registers and the interconnection of central, commercial and company registers, under Directive (EU) 2017/1132 of the European Parliament and of the Council ([2]), and the interconnection of insolvency registers, under Regulation (EU) 2015/848 of the European Parliament and of the Council ([3]).

(51) In order to ensure uniform conditions for the implementation of a technical system allowing for the automated exchange of evidence, implementing powers should be conferred on the Commission to lay down, in particular the technical and operational specifications of a system for the processing of a user's request for evidence to be exchanged and for the transfer of such evidence, as well as to lay down the rules necessary to ensure the integrity and confidentiality of the transfer. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council ([4]).

(52) With a view to ensuring that the technical system provides a high level of security for the cross-border application of the 'once-only' principle, the Commission should, when adopting implementing acts setting out the specifications for such a technical system, take due account of the standards and technical specifications drawn up by European and international standardisation organisations and bodies, in particular the European Committee for

([1]) Regulation (EU) No 1316/2013 of the European Parliament and of the Council of 11 December 2013 establishing the Connecting Europe Facility, amending Regulation (EU) No 913/2010 and repealing Regulations (EC) No 680/2007 and (EC) No 67/2010 (OJ L 348, 20.12.2013, p. 129).

([2]) Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law (OJ L 169, 30.6.2017, p. 46).

([3]) Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings (OJ L 141, 5.6.2015, p. 19).

([4]) 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).

Standardisation (CEN), the European Telecommunications Standards Institute (ETSI), the International Organisation for Standardisation (ISO) and the International Telecommunication Union (ITU), as well as of the security standards referred to in Article 32 of Regulation (EU) 2016/679 and Article 22 of Regulation (EU) 2018/1725.

(53) Where necessary in order to ensure the development, availability, maintenance, supervision, monitoring and security management of the parts of the technical system for which the Commission is responsible, the Commission should request the advice of the European Data Protection Supervisor.

(54) The competent authorities and the Commission should ensure that the information, procedures and services for which they are responsible comply with the quality criteria. The national coordinators appointed under this Regulation and the Commission should, at regular intervals, supervise compliance with the quality and security criteria at national and Union level respectively, and address any problems that arise. The national coordinators should in addition assist the Commission in monitoring the functioning of the technical system enabling the cross-border exchange of evidence. This Regulation should afford the Commission a range of means to address any deterioration in the quality of services offered through the gateway, depending on the seriousness and persistence of such deterioration, involving, where necessary, the gateway coordination group. This should not prejudge the overall responsibility of the Commission regarding the monitoring of the compliance with this Regulation.

(55) This Regulation should specify the main functionalities of the technical tools supporting the functioning of the gateway, in particular the common user interface, the repository for links, and the common assistance service finder. The common user interface should ensure that users can easily find information, procedures and assistance and problem-solving services on national and Union level websites. Member States and the Commission should aim to provide links to a single source of the information required for the gateway in order to avoid confusion among the users as a result of different or fully or partly duplicative sources of the same information. This should not exclude the possibility of providing links to the same information offered by local or regional competent authorities regarding different geographical areas. It should also not prevent some duplication of information where this is unavoidable or desirable, for instance where some Union rights, obligations and rules are repeated or described on national webpages to improve user-friendliness. To minimise human intervention in the updating of the links to be used by the common user interface, a direct connection between the relevant technical systems of the Member States and the repository for links should, where technically possible, be established. The common ICT support tools might use the Core Public Services Vocabulary (CPSV) to facilitate interoperability with national service catalogues and semantics. Member States should be encouraged to use the CPSV, but are free to decide to use national solutions. The information included in the repository for links should be made publicly available in open, commonly used and machine-readable format, for example by application programming interfaces (APIs), in order to enable its reuse.

(56) The search facility of the common user interface should lead users to the information they need wherever it is on Union or national level webpages. In addition, as an alternative way to guide users to useful information, it will continue to be helpful to create links between existing and complementary websites or webpages, streamlining and grouping them together as much as possible, and to create links between webpages and websites at Union and national level providing access to online services and information.

(57) This Regulation should also specify quality requirements for the common user interface. The Commission should ensure that the common user interface complies with those requirements, and the interface should in particular be available and accessible online through various channels, as well as being easy to use.

(58) In order to ensure uniform conditions for the implementation of the technical solutions supporting the gateway, implementing powers should be conferred on the Commission to lay down, where necessary, the applicable standards and interoperability requirements in order to make it easier to find the information on rules and obligations, on procedures and on assistance and problem-solving services for which the Member States and Commission are responsible. Those powers should be exercised in accordance with Regulation (EU) No 182/2011.

(59) This Regulation should also clearly allocate the responsibility regarding the development, availability, maintenance and security of the ICT applications supporting the gateway between the Commission and Member States. As part of their maintenance tasks, the Commission and the Member States should regularly monitor the proper functioning of those ICT applications.

(60) In order to develop the full potential of the different areas of information, the procedures and the assistance and problem-solving services that should be included in the gateway, target audiences' awareness of their existence and operation needs to be improved significantly. Their inclusion in the gateway should make it much easier for users to find the information, the procedures and the assistance and problem-solving services that they need, even when they are not familiar with any of them. In addition, coordinated promotional activities will be needed to ensure that citizens and businesses across the Union become aware of the existence of the gateway and of the advantages it offers. Such promotional activities should include search engine optimisation and other online awareness raising actions, since they are the most cost-effective and have the potential to reach the largest possible target audience. For maximum efficiency, those promotional activities should be coordinated within the framework of the gateway coordination group and Member States should adjust their promotional efforts so that there is a common brand reference in all relevant contexts, with a possibility of co-branding the gateway with national initiatives.

(61) All Union institutions, bodies and agencies should be encouraged to promote the gateway by including its logo and links to it on all relevant webpages for which they are responsible.

(62) The name by which the gateway is to be known and promoted to the general public should be 'Your Europe'. The common user interface should be prominent and easy to find, particularly on relevant Union and national webpages. The logo of the gateway should be visible on relevant Union and national websites.

(63) In order to obtain adequate information for measuring and improving the performance of the gateway, this Regulation should require the competent authorities and the Commission to collect and analyse the data related to the use of the different information areas, procedures and services offered through the gateway. The collection of user statistics, such as data relating to the number of visits to specific webpages, the number of users within a Member State compared to the number of users from other Member States, the search terms used, the most visited webpages, the referral webpages, or the number, origin and subject matter of requests for assistance should improve the functioning of the gateway by helping to identify the audience, to develop promotional activities and to improve the quality of the services offered. The collection of such data should take into account the annual eGovernment Benchmarking done by the Commission in order to avoid any duplication.

(64) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to lay down uniform rules on the method of collecting and exchanging user statistics. Those powers should be exercised in accordance with Regulation (EU) No 182/2011.

(65) The quality of the gateway depends on the quality of Union and national services provided through the gateway. Therefore, the quality of the information, procedures, assistance and problem-solving services available through the gateway should also be regularly monitored through a user feedback tool that asks users to assess and give feedback on the coverage and quality of the information, procedure or assistance and problem-solving service which they have used. This feedback should be collected in a common tool to which the Commission, the competent authorities and the national coordinators should have access. In order to ensure uniform conditions for implementation of this Regulation in relation to the common functionalities of user feedback tools and the detailed arrangements for the collection and sharing of the user feedback, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011. The Commission should publish, in anonymised form, online summary overviews of the problems emerging from the information, the main user statistics and the main user feedback collected in accordance with this Regulation.

(66) In addition, the gateway should include a feedback tool that enables users to signal, voluntarily and anonymously, any problems and difficulties that they encountered while exercising their internal market rights. This tool should be considered only to be complementary to the complaint handling mechanisms, since it cannot offer a personalised response to users. The received input should be combined with aggregated information from assistance and problem-solving services about the cases that they have handled in order to produce an overview of the internal market as perceived by its users and to identify problem areas for possible future action in order to improve the functioning of the internal market. That overview should be linked to existing reporting tools, such as the Single Market Scoreboard.

(67) The right of Member States to decide who should carry out the role of the national coordinator should be unaffected by this Regulation. Member States should be able to adapt the functions and responsibilities of their national coordinators in relation to the gateway to their internal administrative structures. Member States should be able to appoint additional national coordinators to carry out the tasks under this Regulation alone or jointly with others, with responsibility for a division of the administration or a geographic region, or in accordance with other criteria. Member States should inform the Commission of the identity of the single national coordinator that they have appointed for contacts with the Commission.

(68) The gateway coordination group composed of the national coordinators and chaired by the Commission should be set up with a view to facilitating the application of this Regulation, in particular by exchanging best practices and working together to improve the consistency of the presentation of information as required by this Regulation. The work of the gateway coordination group should take into account the objectives set out in the annual work programme, which the Commission should submit to it for consideration. The annual work programme should take the form of guidelines or recommendations, which are not binding for Member States. The Commission, upon the request of the European Parliament, can decide to invite Parliament to send experts to attend meetings of the gateway coordination group.

(69) This Regulation should clarify which parts of the gateway are to be financed through the Union budget and which parts are to be the responsibility of the Member States. The Commission should assist the Member States in identifying reusable ICT building blocks and financing available through various Union level funds and programmes that can contribute to covering the costs for ICT adaptations and developments needed at national level to comply with this Regulation. The budget required for the implementation of this Regulation should be compatible with the applicable Multiannual Financial Framework.

(70) Member States are encouraged to coordinate, exchange and collaborate more with one another in order to increase their strategic, operational, research and development capacities in the area of cybersecurity, in particular through the implementation of the network and information security, as referred to in Directive (EU) 2016/1148 of the European Parliament and of the Council ([1]), to strengthen the security and resilience of their public administration and services. Member States are encouraged to increase the security of transactions and to ensure a sufficient level of confidence in electronic means by using the eIDAS framework laid down by Regulation (EU) No 910/2014 and in particular adequate assurance levels. Member States can take measures in accordance with Union law to safeguard cybersecurity and to prevent identity fraud or other forms of fraud.

(71) Where the application of this Regulation entails the processing of personal data, it should be carried out in accordance with Union law on the protection of personal data, in particular Regulation (EU) 2016/679 and Regulation (EU) 2018/1725. Directive (EU) 2016/680 of the European Parliament and of the Council ([2]) should also apply in the context of this Regulation. As provided for in Regulation (EU) 2016/679, Member States can maintain or introduce further conditions, including limitations, with regard to the processing of data concerning health, and they can also provide for more specific rules on the processing of employees' personal data in the context of employment.

(72) This Regulation should promote and facilitate the streamlining of governance arrangements for the services covered by the gateway. For this purpose, the Commission should, in close cooperation with the Member States, review the existing governance arrangements and adapt them where necessary, in order to avoid duplication and inefficiencies.

(73) The objective of this Regulation is to ensure that users who operate in other Member States have online access to comprehensive, reliable, accessible and understandable Union and national information on rights, rules and obligations, to online procedures that are fully transactional cross-border and to assistance and problem-solving services. As that objective cannot be sufficiently achieved by the Member States, but can rather, by reason of the scale and effects of this Regulation, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

([1]) 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).

([2]) 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).

(74) In order for the Member States and the Commission to develop and implement the necessary tools to give effect to this Regulation, certain of its provisions should apply from two years after its entry into force. Municipal authorities should be given until four years after the entry into force of this Regulation to implement the requirement to provide information regarding the rules, procedures and assistance and problem-solving services within their responsibility. The provisions of this Regulation regarding procedures to be offered fully online, the cross-border access to online procedures and the technical system for the cross-border automated exchange of evidence in accordance with the 'once-only' principle should be implemented by five years after the entry into force of this Regulation at the latest.

(75) This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union, and should be implemented in accordance with those rights and principles.

(76) 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 ([1]) and delivered an opinion on 1 August 2017 ([2]),

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

1. This Regulation lays down rules for:

(a) the establishment and operation of a single digital gateway to provide citizens and businesses with easy access to high quality information, to efficient procedures and to effective assistance and problem-solving services with regard to Union and national rules applicable to citizens and businesses exercising or intending to exercise their rights derived from Union law in the field of the internal market, within the meaning of Article 26(2) TFEU;

(b) the use of procedures by cross-border users and the implementation of the 'once-only' principle in connection with the procedures listed in Annex II to this Regulation and the procedures provided for in Directives 2005/36/EC, 2006/123/EC, 2014/24/EU and 2014/25/EU;

(c) the reporting on obstacles in the internal market based on the collection of user feedback and statistics from the services covered by the gateway.

2. Where this Regulation conflicts with a provision of another Union act governing specific aspects of the subject matter covered by this Regulation, the provision of that other Union act shall prevail.

3. This Regulation shall not affect the substance of, or the rights granted through, any procedure laid down at Union or national level in any of the areas covered by this Regulation. Furthermore, this Regulation shall not affect measures taken in accordance with Union law to safeguard cybersecurity and to prevent fraud.

([1]) 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).

([2]) OJ C 340, 11.10.2017, p. 6.

Article 2

Establishment of the single digital gateway

1. A single digital gateway ('the gateway') shall be established by the Commission and the Member States in accordance with this Regulation. The gateway shall consist of a common user interface managed by the Commission ('the common user interface'), which shall be integrated into the Your Europe portal and shall give access to relevant Union and national webpages.

2. The gateway shall give access to:

(a) information on rights, obligations and rules laid down in Union and national law that are applicable to users exercising or intending to exercise their rights derived from Union law in the field of the internal market in the areas listed in Annex I;

(b) information on online and offline procedures and links to online procedures, including procedures covered by Annex II, established at Union or national level in order to enable users to exercise the rights and to comply with the obligations and rules in the field of the internal market in the areas listed in Annex I;

(c) information on, and links to, the assistance and problem-solving services listed in Annex III or referred to in Article 7 which citizens and businesses can refer to if they have questions or problems related to the rights, obligations, rules or procedures referred to in points (a) and (b) of this paragraph.

3. The common user interface shall be accessible in all official languages of the Union.

Article 3

Definitions

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

(1) 'user' means either a citizen of the Union, a natural person residing in a Member State or a legal person having its registered office in a Member State, and who accesses the information, the procedures, or the assistance or problem-solving services, referred to in Article 2(2), through the gateway;

(2) 'cross-border user' means a user in a situation which is not confined in all respects within a single Member State;

(3) 'procedure' means a sequence of actions that must be taken by users to satisfy the requirements, or to obtain from a competent authority a decision, in order to be able to exercise their rights as referred to in point (a) of Article 2(2);

(4) 'competent authority' means any Member State authority or body established at national, regional or local level with specific responsibilities relating to the information, procedures, assistance and problem-solving services covered by this Regulation;

(5) 'evidence' means any document or data, including text or sound, visual or audiovisual recording, irrespective of the medium used, required by a competent authority to prove facts or compliance with procedural requirements referred to in point (b) of Article 2(2).

CHAPTER II

GATEWAY SERVICES

Article 4

Access to information

1. Member States shall ensure that users have easy, online access on their national webpages to the following:

(a) information about those rights, obligations and rules referred to in point (a) of Article 2(2) that are derived from national law;

(b) information about those procedures referred to in point (b) of Article 2(2) that are established at national level;

(c) information about those assistance and problem-solving services referred to in point (c) of Article 2(2) that are provided at national level.

2. The Commission shall ensure that the Your Europe portal provides users with easy, online access to the following:

(a) information about those rights, obligations and rules referred to in point (a) of Article 2(2) that are derived from Union law;

(b) information about those procedures referred to in point (b) of Article 2(2) that are established at Union level;

(c) information about those assistance and problem-solving services referred to in point (c) of Article 2(2) that are provided at Union level.

Article 5

Access to information not included in Annex I

1. The Member States and the Commission may provide links to information not listed in Annex I which is offered by competent authorities, the Commission or bodies, offices and agencies of the Union, provided that this information falls within the scope of the gateway as defined in point (a) of Article 1(1) and complies with the quality requirements laid down in Article 9.

2. The links to the information referred to in paragraph 1 of this Article shall be provided in accordance with Article 19 (2) and (3).

3. Before activating any links, the Commission shall verify that the conditions laid down in paragraph 1 are met and consult the gateway coordination group.

Article 6

Procedures to be offered fully online

1. Each Member State shall ensure that users can access and complete any of the procedures listed in Annex II fully online, provided that the relevant procedure has been established in the Member State concerned.

2. The procedures referred to in paragraph 1 shall be considered to be fully online where:

(a) the identification of users, the provision of information and supporting evidence, signature and final submission can all be carried out electronically at a distance, through a service channel which enables users to fulfil the requirements related to the procedure in a user-friendly and structured way;

(b) users are provided with an automatic acknowledgement of receipt, unless the output of the procedure is delivered immediately;

(c) the output of the procedure is delivered electronically, or where necessary to comply with applicable Union or national law, delivered by physical means; and

(d) users are provided with an electronic notification of completion of the procedure.

3. Where, in exceptional cases justified by overriding reasons of public interest in the areas of public security, public health or the fight against fraud, the objective pursued cannot be fully achieved online, Member States may require the user to appear in person before the competent authority as a step in the procedure. In such exceptional cases, Member States shall limit such physical presence to what is strictly necessary and objectively justified and shall ensure that other steps of the procedure can be completed fully online. Member States shall also ensure that physical presence requirements do not result in discrimination against cross-border users.

4. Member States shall notify and explain, through a common repository accessible to the Commission and the other Member States, the grounds on which, and the circumstances in which, physical presence might be required for the procedural steps referred to in paragraph 3, and the grounds on which, and the circumstances in which, physical delivery is necessary, as referred to in point (c) of paragraph 2.

5. This Article shall not prevent Member States from offering users the additional possibility of accessing and completing the procedures referred to in point (b) of Article 2(2) by means other than an online channel, or from contacting users directly.

Article 7

Access to assistance and problem-solving services

1. The Member States and the Commission shall ensure that users, including cross-border users, have easy online access through different channels to the assistance and problem-solving services referred to in point (c) of Article 2(2).

2. The national coordinators referred to in Article 28 and the Commission may provide links to assistance and problem-solving services offered by competent authorities, the Commission or bodies, offices and agencies of the Union, other than those listed in Annex III, in accordance with Article 19(2) and (3), provided that such services comply with the quality requirements laid down in Articles 11 and 16.

3. Where necessary to meet the needs of the users, the national coordinator may propose to the Commission that links to assistance or problem-solving services provided by private or semi-private entities are included in the gateway, where those services meet the following conditions:

(a) they offer information or assistance within the areas, and for the purposes, covered by this Regulation and are complementary to services already included in the gateway;

(b) they are offered free of charge or at a price which is affordable for micro-enterprises, non-profit organisations and citizens; and

(c) they comply with the requirements laid down in Articles 8, 11 and 16.

4. Where the national coordinator has proposed the inclusion of a link in accordance with paragraph 3 of this Article, and provides such link in accordance with Article 19(3), the Commission shall assess whether the conditions in paragraph 3 of this Article are met by the service to be included through the link, and if so, shall activate the link.

Where the Commission finds that the conditions in paragraph 3 are not met by the service to be included, it shall inform the national coordinator of the reasons for not activating the link.

Article 8

Quality requirements related to web accessibility

The Commission shall make those of its websites and webpages through which it grants access to the information referred to in Article 4(2) and to the assistance and problem-solving services referred to in Article 7 more accessible by making them perceivable, operable, understandable and robust.

CHAPTER III

QUALITY REQUIREMENTS

SECTION 1

Quality requirements related to information on rights, obligations and rules, on procedures and on assistance and problem-solving services

Article 9

Quality of information on rights, obligations and rules

1. Where Member States and the Commission are responsible in accordance with Article 4 for ensuring access to information referred to in point (a) of Article 2(2), they shall make sure that such information complies with the following requirements:

(a) it is user-friendly, enabling users to easily find and understand the information and to easily identify which parts of the information are relevant to their particular situation;

(b) it is accurate and sufficiently comprehensive to cover information that users need to know in order to exercise their rights in full compliance with applicable rules and obligations;

(c) it includes references, links to legal acts, technical specifications and guidelines, where relevant;

(d) it includes the name of the competent authority or entity responsible for the content of the information;

(e) it includes the contact details of any relevant assistance or problem-solving services, such as a phone number, an email address, an online enquiry form or any other commonly used means of electronic communication that is most suitable for the type of service offered and for the target audience of that service;

(f) it includes the date of the last update of the information, if any, or, where the information has not been updated, the date of publication of the information;

(g) it is well-structured and presented, so that users can quickly find the information they need;

(h) it is kept up-to-date; and

(i) it is written in clear and plain language adapted to the needs of the target users.

2. Member States shall make the information referred to in paragraph 1 of this Article accessible in an official language of the Union that is broadly understood by the largest possible number of cross-border users, in accordance with Article 12.

Article 10

Quality of information on procedures

1. The Member States and the Commission shall, for the purposes of complying with Article 4, ensure that, before users have to identify themselves prior to launching the procedure, they have access to a sufficiently comprehensive, clear and user-friendly explanation of the following elements, where applicable, of the procedures referred to in point (b) of Article 2 (2):

(a) the relevant steps of the procedure to be taken by the user, including any exception, under Article 6(3), to the obligation of Member States to offer the procedure fully online;

(b) the name of the competent authority responsible for the procedure, including its contact details;

(c) the accepted means of authentication, identification and signature for the procedure;

(d) the type and format of evidence to be submitted;

(e) the means of redress or appeal which are generally available in the event of disputes with the competent authorities;

(f) the applicable fees and the online methods of payment;

(g) any deadlines to be respected by the user or by the competent authority and where no deadlines exist, the average, estimated or indicative time that the competent authority needs to complete the procedure;

(h) any rules concerning a lack of reply from the competent authority and the legal consequences thereof for the users, including tacit approval or administrative silence arrangements;

(i) any additional languages in which the procedure can be carried out.

2. If no tacit approval, administrative silence or similar arrangements exist, competent authorities shall, where applicable, inform users of any delays and of any extension of deadlines or any consequences thereof.

3. Where the explanation referred to in paragraph 1 is already made available for non-crossborder users, it may be used or reused for the purposes of this Regulation, provided that it also covers the situation of cross-border users, where applicable.

4. Member States shall make the explanation referred to in paragraph 1 of this Article accessible in an official language of the Union that is broadly understood by the largest possible number of cross-border users, in accordance with Article 12.

Article 11

Quality of information on assistance and problem-solving services

1. The Member States and the Commission shall, for the purposes of complying with Article 4, ensure that, before submitting a request for a service as referred to in point (c) of Article 2(2), users have access to a clear and user-friendly explanation of the following:

(a) the type, purpose and expected results of the service offered;

(b) the contact details of the entities responsible for the service such as a phone number, an email address, an online enquiry form or any other commonly used means of electronic communication that is most suitable for the type of service offered and for the target audience of that service;

(c) where relevant, the applicable fees and the online methods of payment;

(d) any applicable deadlines to be respected and where none exist, an average, or estimated time required to deliver the service;

(e) any additional languages in which the request can be submitted and which can be used in subsequent contacts.

2. Member States shall make the explanation referred to in paragraph 1 of this Article accessible in an official language of the Union that is broadly understood by the largest possible number of cross-border users, in accordance with Article 12.

Article 12

Translation of information

1. Where a Member State does not provide the information, explanations and instructions set out in Articles 9, 10 and 11, and in point (a) of Article 13(2), in an official language of the Union broadly understood by the largest possible number of cross-border users, that Member State shall request the Commission to provide translations into that language, within the limits of the available Union budget referred to in point (c) of Article 32(1).

2. Member States shall ensure the texts submitted for translation under paragraph 1 of this Article cover at least the basic information in all areas listed in Annex I and that, where sufficient Union budget is available, they cover any further information, explanations and instructions referred to in Articles 9, 10 and 11, and in point (a) of Article 13(2), taking the most important needs of cross-border users into account. Member States shall provide to the repository for links referred to in Article 19 the links to such translated information.

3. The language referred to in paragraph 1 shall be the official language of the Union that is most widely studied as a foreign language by users across the Union. By way of exception, where the information, explanations or instructions to be translated are expected to be of predominant interest for cross-border users originating from one other Member State, the language referred to in paragraph 1 may be the official language of the Union used as the first language by those cross-border users.

4. Where a Member State requests a translation into an official language of the Union that is not the language most widely studied as a foreign language by users across the Union, it shall provide reasons for its request. Where the Commission finds that the conditions referred to in paragraph 3 for the choice of such other language are not met, it may refuse the request and shall inform the Member State of the reasons thereof.

SECTION 2

Requirements related to online procedures

Article 13

Cross-border access to online procedures

1. Member States shall ensure that, where a procedure referred to in point (b) of Article 2(2) and established at national level can be accessed and completed online by non-cross-border users, it can also be accessed and completed online by cross-border users in a non-discriminatory way by means of the same or an alternative technical solution.

2. Member States shall ensure that, for the procedures referred to in paragraph 1 of this Article, at least the following requirements are met:

(a) users are able to access the instructions for completing the procedure in an official language of the Union that is broadly understood by the largest possible number of cross-border users, in accordance with Article 12;

(b) cross-border users are able to submit the required information, including where the structure of such information differs from similar information in the Member State concerned;

(c) cross-border users are able to identify and authenticate themselves, sign or seal documents electronically, as provided for in Regulation (EU) No 910/2014, in all cases where this is also possible for non-crossborder users;

(d) cross-border users are able to provide evidence of compliance with applicable requirements and to receive the outcome of the procedures in electronic format in all cases where this is also possible for non-crossborder users;

(e) where the completion of a procedure requires a payment, users are able to pay any fees online through widely available cross-border payment services, without discrimination based on the place of establishment of the payment service provider, the place of issue of the payment instrument or the location of the payment account within the Union.

3. Where the procedure does not require electronic identification or authentication, as referred to in point (c) of paragraph 2, and where competent authorities are allowed under applicable national law or administrative practices to accept digitalised copies of non-electronic evidence of identity, such as identity cards or passports, in respect of non-crossborder users, those authorities shall also accept such digitalised copies in respect of cross-border users.

Article 14

Technical system for the cross-border automated exchange of evidence and application of the 'once-only' principle

1. For the purpose of the exchange of evidence for the online procedures listed in Annex II to this Regulation and the procedures provided for in Directives 2005/36/EC, 2006/123/EC, 2014/24/EU and 2014/25/EU, a technical system for the automated exchange of evidence between competent authorities in different Member States ('the technical system') shall be established by the Commission in cooperation with the Member States.

2. Where competent authorities lawfully issue, in their own Member State and in an electronic format that allows automated exchange, evidence that is relevant for the online procedures referred to in paragraph 1, they shall also make such evidence available to requesting competent authorities from other Member States in an electronic format that allows automated exchange.

3. The technical system shall, in particular:

(a) enable the processing of requests for evidence at the explicit request of the user;

(b) enable the processing of requests for evidence to be accessed or exchanged;

(c) allow the transmission of evidence between competent authorities;

(d) allow the processing of the evidence by the requesting competent authority;

(e) ensure the confidentiality and integrity of the evidence;

(f) enable the possibility for the user to preview the evidence to be used by the requesting competent authority and to choose whether or not to proceed with the exchange of evidence;

(g) ensure an adequate level of interoperability with other relevant systems;

(h) ensure a high level of security for the transmission and processing of evidence;

(i) not process evidence beyond what is technically necessary for the exchange of evidence, and then only for the duration necessary for that purpose.

4. The use of the technical system shall not be obligatory for users and shall only be permitted at their explicit request, unless otherwise provided under Union or national law. The users shall be permitted to submit evidence by means other than the technical system and directly to the requesting competent authority.

5. The possibility of previewing the evidence, referred to in point (f) of paragraph 3 of this Article shall not be required for procedures where the automated cross-border data exchange without such preview is allowed under applicable Union or national law. That possibility of previewing the evidence shall be without prejudice to the obligation to provide the information under Articles 13 and 14 of Regulation (EU) 2016/679.

6. Member States shall integrate the fully operational technical system as part of the procedures referred to in paragraph 1.

7. The competent authorities responsible for the online procedures referred to in paragraph 1 shall, upon an explicit, freely given, specific, informed and unambiguous request of the user concerned, request evidence directly from competent authorities issuing evidence in other Member States through the technical system. The issuing competent authorities referred to in paragraph 2 shall, in accordance with point (e) of paragraph 3, make such evidence available through the same system.

8. The evidence made available to the requesting competent authority shall be limited to what has been requested and shall only be used by that authority for the purpose of the procedure for which the evidence was exchanged. The evidence exchanged through the technical system shall, for the purposes of the requesting competent authority, be deemed to be authentic.

9. By 12 June 2021, the Commission shall adopt implementing acts to set out the technical and operational specifications of the technical system necessary for the implementation of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).

10. Paragraphs 1 to 8 shall not apply to procedures established at Union level which provide for different mechanisms for the exchange of evidence, unless the technical system necessary for the implementation of this Article is integrated into those procedures in accordance with the rules of the Union acts that establish those procedures.

11. The Commission and each of the Member States shall be responsible for the development, availability, maintenance, supervision, monitoring and security management of their respective parts of the technical system.

Article 15

Verification of evidence between Member States

Where the technical system, or other systems for the exchange or verification of evidence between Member States are not available or are not applicable, or where the user does not request the use of the technical system, competent authorities shall cooperate through the Internal Market Information System (IMI) where this is necessary in order to verify the authenticity of evidence that was submitted to one of them in an electronic format by the user for the purpose of an online procedure.

SECTION 3

Quality requirements related to assistance and problem-solving services

Article 16

Quality requirements related to assistance and problem-solving services

The competent authorities and the Commission shall, within their respective competences, ensure that the assistance and problem-solving services listed in Annex III and those that have been included in the gateway in accordance with Article 7 (2), (3) and (4) comply with the following quality requirements:

(a) they are provided within a reasonable timeframe taking into account the complexity of the request;

(b) when deadlines are extended, users are informed in advance of the reasons thereof and of the new deadline given;

(c) where the provision of a service requires a payment, users are able to pay any fees online through widely available cross-border payment services without discrimination based on the place of establishment of the payment service provider, the place of issue of the payment instrument or the location of the payment account within the Union.

SECTION 4

Quality monitoring

Article 17

Quality monitoring

1. The national coordinators referred to in Article 28 and the Commission shall, within their respective competences, regularly monitor the compliance of the information, procedures and assistance and problem-solving services available through the gateway with the quality requirements laid down in Articles 8 to 13 and 16. The monitoring shall be carried out on the basis of the data gathered in accordance with Articles 24 and 25.

2. In the event of a deterioration in the quality of the information, of the procedures and of the assistance or problem-solving services referred to in paragraph 1 provided by the competent authorities, the Commission shall, taking into account the seriousness and persistence of the deterioration, take one or more of the following measures:

(a) inform the relevant national coordinator and ask for remedial action;

(b) submit for discussion in the gateway coordination group recommended actions to improve compliance with the quality requirements;

(c) send a letter with recommendations to the Member State concerned;

(d) temporarily disconnect the information, the procedure, or the assistance or problem-solving service from the gateway.

3. Where an assistance or problem-solving service to which links are provided in accordance with Article 7(3) consistently does not comply with requirements laid down in Articles 11 and 16, or no longer meets the needs of the users as indicated by the data gathered in accordance with Articles 24 and 25, the Commission may, after consultation with the relevant national coordinator and, where necessary, with the gateway coordination group, disconnect it from the gateway.

CHAPTER IV

TECHNICAL SOLUTIONS

Article 18

Common user interface

1. The Commission shall, in close cooperation with the Member States, provide a common user interface, integrated into the 'Your Europe' portal, to ensure the proper functioning of the gateway.

2. The common user interface shall give access to the information, procedures and assistance or problem-solving services by means of links to the relevant Union and national level websites or webpages included in the repository for links referred to in Article 19.

3. The Member States and the Commission, acting in accordance with their respective roles and responsibilities, as provided for in Article 4, shall ensure that the information on rules and obligations, on procedures and on assistance and problem-solving services is organised and marked in a way that makes it easier to find through the common user interface.

4. The Commission shall ensure that the common user interface complies with the following quality requirements:

(a) it is easy to use;

(b) it is accessible online through various electronic devices;

(c) it is developed and optimised for different web browsers;

(d) it meets the following web accessibility requirements: perceivability, operability, understandability and robustness.

5. The Commission may adopt implementing acts laying down interoperability requirements to make it easier to find the information on rules and obligations, on procedures and on assistance and problem-solving services through the common user interface. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).

Article 19

Repository for links

1. The Commission, in close cooperation with the Member States, shall establish and maintain an electronic repository for links to the information, procedures and assistance and problem-solving services referred to in Article 2(2) allowing the connection between such services and the common user interface.

2. The Commission shall provide the repository for links with the links to the information, procedures and assistance and problem-solving services accessible on the webpages managed at Union level, and it shall keep those links accurate and up-to-date.

3. The national coordinators shall provide the repository for links with the links to the information, procedures and assistance and problem-solving services accessible on the webpages managed by competent authorities, or by private or semi-private entities as referred to in Article 7(3), and they shall keep those links accurate and up-to-date.

4. Where technically possible, the provision, referred to in paragraph 3, of the links may be carried out automatically between the relevant systems of the Member States and the repository for links.

5. The Commission shall make the information included in the repository for links publicly available in an open and machine-readable format.

6. The Commission and the national coordinators shall ensure that the links to information, procedures and assistance or problem-solving services offered through the gateway do not contain any unnecessary full or partial duplication and overlaps that are likely to confuse users.

7. Where the making available of information referred to in Article 4 is provided for in other provisions of Union law, the Commission and the national coordinators may provide links to that information in order to comply with the requirements of that Article.

Article 20

Common assistance service finder

1. In order to facilitate access to the assistance and problem-solving services listed in Annex III or referred to in Article 7 (2) and (3), the competent authorities and the Commission shall ensure that users can access them through a common assistance and problem-solving service finder ('the common assistance service finder') available through the gateway.

2. The Commission shall develop and manage the common assistance service finder, and decide on the structure and format in which the descriptions and contact details of the assistance and problem-solving services need to be provided, to enable the proper functioning of the common assistance service finder.

3. The national coordinators shall provide the descriptions and contact details as referred to in paragraph 2 to the Commission.

Article 21

Responsibilities for the ICT applications supporting the gateway

1. The Commission shall be responsible for the development, availability, monitoring, updating, maintenance, security and hosting of the following ICT applications and webpages:

(a) the Your Europe portal, referred to in Article 2(1);

(b) the common user interface, referred to in Article 18(1), including the search engine or any other ICT tool that enables searchability of web information and services;

(c) the repository for links, referred to in Article 19(1);

(d) the common assistance service finder, referred to in Article 20(1);

(e) the user feedback tools, referred to in Article 25(1) and point (a) of Article 26(1).

The Commission shall work in close cooperation with the Member States to develop the ICT applications.

2. The Member States shall be responsible for the development, availability, monitoring, updating, maintenance and security of ICT applications related to the national websites and webpages that they manage and that are linked to the common user interface.

CHAPTER V

PROMOTION

Article 22

Name, logo and quality label

1. The name by which the gateway is to be known and promoted to the general public shall be 'Your Europe'.

The logo by which the gateway is to be known and promoted to the general public shall be decided by the Commission in close cooperation with the gateway coordination group by 12 June 2019 at the latest.

The logo of the gateway and a link to the gateway shall be made visible and available on the relevant Union-level and national-level websites that are connected to the gateway.

2. As proof of adherence to the quality requirements referred to in Articles 9, 10 and 11, the name and the logo of the gateway shall also serve as a quality label. However, the logo of the gateway shall only be used as a quality label by webpages and websites included in the repository for links referred to in Article 19.

Article 23

Promotion

1. The Member States and the Commission shall promote the awareness and the use of the gateway amongst citizens and businesses and shall ensure that the gateway and its information, procedures and assistance and problem-solving services are visible to the public and can be easily found through search engines which are accessible to the public.

2. The Member States and the Commission shall coordinate their promotion activities referred to in paragraph 1 and shall refer to the gateway and use its logo in such activities, along with any other brand names, as appropriate.

3. The Member States and the Commission shall ensure that the gateway can be easily found through the related websites for which they are responsible, and that clear links to the common user interface are available on all relevant websites at Union and national level.

4. The national coordinators shall promote the gateway to the national competent authorities.

CHAPTER VI

COLLECTION OF USER FEEDBACK AND STATISTICS

Article 24

User statistics

1. The competent authorities and the Commission shall ensure that statistics are collected in relation to users' visits on the gateway and on the webpages to which the gateway links in a way that guarantees anonymity of the users, in order to improve the functionality of the gateway.

2. The competent authorities, the providers of assistance or problem-solving services as referred to in Article 7(3) and the Commission shall collect and exchange, in an aggregated way, the number, the origin and the subject matter of requests for assistance and problem-solving services and their response times.

3. The statistics collected in accordance with paragraphs 1 and 2 in relation to the information, procedures and assistance and problem-solving services to which the gateway links shall include the following data categories:

(a) data related to the number, origin and type of users of the gateway;

(b) data related to the user preferences and user journeys;

(c) data related to the usability, findability and quality of the information, procedures and assistance and problem-solving services.

Those data shall be made available to the public in an open and commonly used, machine-readable format.

4. The Commission shall adopt implementing acts laying down the method of collecting and exchanging the user statistics referred to in paragraphs 1, 2 and 3 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).

Article 25

User feedback on the services of the gateway

1. In order to gather direct information from users about their satisfaction with the services provided through the gateway and the information made available therein, the Commission shall provide users through the gateway with a user-friendly feedback tool that enables them, immediately after using any of the services referred to in Article 2(2), to comment anonymously on the quality and availability of the services provided through the gateway, of the information made available therein and of the common user interface.

2. The competent authorities and the Commission shall ensure that users can access the tool referred to in paragraph 1 from all webpages that are part of the gateway.

3. The Commission, the competent authorities and the national coordinators shall have direct access to the user feedback collected through the tool referred to in paragraph 1 for the purpose of addressing any problems raised.

4. The competent authorities shall not be required on those of their webpages that are part of the gateway to give users access to the user feedback tool referred to in paragraph 1, where another user feedback tool with similar functionalities to the user feedback tool referred to in paragraph 1 is already available on their webpages for the purpose of monitoring service quality. The competent authorities shall collect the user feedback received through their own user feedback tool and shall share it with the Commission and the national coordinators of the other Member States.

5. The Commission shall adopt implementing acts laying down rules for the collection and sharing of the user feedback. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).

Article 26

Reporting on the functioning of the internal market

1. The Commission shall:

(a) provide users of the gateway with a user-friendly tool to signal and give feedback anonymously on any obstacles encountered by them in exercising their internal market rights;

(b) collect aggregated information from the assistance and problem-solving services that form part of the gateway about the subject matter of requests and responses.

2. The Commission, the competent authorities and the national coordinators shall have direct access to the feedback collected in accordance with point (a) of paragraph 1.

3. The Member States and the Commission shall analyse and investigate the problems raised by users pursuant to this Article and address them, wherever possible, by appropriate means.

Article 27

Online summary overviews

The Commission shall publish in an anonymised form online summary overviews of the problems emerging from the information collected in accordance with Article 26(1), the main user statistics referred to in Article 24, and the main user feedback referred to in Article 25.

CHAPTER VII

GOVERNANCE OF THE GATEWAY

Article 28

National coordinators

1. Each Member State shall appoint a national coordinator. In addition to their obligations in accordance with Articles 7, 17, 19, 20, 23 and 25, the national coordinators shall:

(a) act as a contact point for their respective administrations for all matters relating to the gateway;

(b) promote the uniform application of Articles 9 to 16 by their respective competent authorities;

(c) ensure that the recommendations referred to in point (c) of Article 17(2) are properly implemented.

2. Each Member State may, in accordance with its internal administrative structure, appoint one or more coordinators in order to carry out any of the tasks listed in paragraph 1. One national coordinator for each Member State shall be responsible for contacts with the Commission in respect of all matters relating to the gateway.

3. Each Member State shall inform the other Member States and the Commission of the name and contact details of its national coordinator.

Article 29

Coordination group

A coordination group is hereby established ('the gateway coordination group'). It shall be composed of one national coordinator from each Member State and shall be chaired by a representative of the Commission. It shall adopt its rules of procedure. The Commission shall provide the secretariat.

Article 30

Tasks of the gateway coordination group

1. The gateway coordination group shall support the implementation of this Regulation. In particular it shall:

(a) facilitate the exchange and regular updating of best practices;

(b) encourage the uptake of fully online procedures beyond those included in Annex II to this Regulation, and of online means of authentication, identification and signatures, in particular those provided for in Regulation (EU) No 910/2014;

(c) discuss improvements to the user-friendly presentation of information within the areas listed in Annex I, in particular on the basis of the data collected in accordance with Articles 24 and 25;

(d) assist the Commission in developing the common ICT solutions supporting the gateway;

(e) discuss the draft annual work programme;

(f) assist the Commission in monitoring the execution of the annual work programme;

(g) discuss additional information provided in accordance with Article 5 with a view to encouraging other Member States to provide similar information, where relevant to the users;

(h) assist the Commission in monitoring compliance with the requirements set out in Articles 8 to 16, in accordance with Article 17;

(i) inform about the implementation of Article 6(1);

(j) discuss and recommend actions to the competent authorities and the Commission with a view to avoiding or eliminating unnecessary duplication of the services available through the gateway;

(k) provide opinions on procedures or measures to address efficiently any problems with the quality of the services raised by users or suggestions for its improvement;

(l) discuss the application of the principles of security by design and privacy by design in the context of this Regulation;

(m) discuss issues related to the collection of the user feedback and statistics referred to in Articles 24 and 25, so that the services offered at Union and national level are continuously improved;

(n) discuss issues related to the quality requirements of the services offered through the gateway;

(o) exchange best practices and assist the Commission in the organisation, structuring and presentation of services referred to in Article 2(2), to enable the proper functioning of the common user interface;

(p) facilitate the development and implementation of the coordinated promotion;

(q) cooperate with the governance bodies or networks of information services, and of assistance or problem-solving services;

(r) provide guidance on the additional official language, or languages, of the Union to be used by competent authorities in accordance with Articles 9(2), 10(4) and 11(2), and point (a) of Article 13(2).

2. The Commission may consult the gateway coordination group on any matter relating to the application of this Regulation.

Article 31

Annual work programme

1. The Commission shall adopt the annual work programme which shall specify, in particular:

(a) actions to improve the presentation of specific information within the areas listed in Annex I and actions to facilitate the timely implementation, by competent authorities at all levels, including municipal level, of the requirement to provide information;

(b) actions to facilitate compliance with Articles 6 and 13;

(c) actions required to ensure the consistent compliance with the requirements set out in Articles 9 to 12;

(d) activities related to the promotion of the gateway in accordance with Article 23.

2. When preparing the draft annual work programme, the Commission shall take account of the user statistics and feedback collected in accordance with Articles 24 and 25 and of any suggestions made by Member States. Prior to adoption, the Commission shall submit the draft annual work programme to the gateway coordination group for discussion.

CHAPTER VIII

FINAL PROVISIONS

Article 32

Costs

1. The general budget of the European Union shall cover the costs of:

(a) development and maintenance of the ICT tools supporting the implementation of this Regulation at Union level;

(b) promotion of the gateway at Union level;

(c) translation of information, explanations and instructions in accordance with Article 12 within a maximum annual volume per Member State, without prejudice to possible reallocation where this is necessary in order to enable full use of the available budget.

2. The costs related to national webportals, information platforms, assistance services and procedures established at Member State level shall be met from the respective budgets of the Member States, unless otherwise provided for in Union legislation.

Article 33

Protection of personal data

The processing of personal data by competent authorities within the framework of this Regulation shall comply with Regulation (EU) 2016/679. Processing of personal data by the Commission within the framework of this Regulation shall comply with Regulation (EU) 2018/1725.

Article 34

Cooperation with other information and assistance networks

1. After consulting the Member States, the Commission shall decide which existing informal governance arrangements for any of the assistance or problem-solving services listed in Annex III or for any of the areas of information covered by Annex I are to become the responsibility of the gateway coordination group.

2. Where the information and assistance services or networks have been created by a legally binding Union act for any of the areas of information covered by Annex I, the Commission shall coordinate the work of the gateway coordination group and the governance bodies of such services or networks with a view to achieving synergies and avoiding duplication.

Article 35

Internal Market Information System

1. The Internal Market Information System (IMI), established by Regulation (EU) No 1024/2012, shall be used for the purposes of, and in accordance with, Article 6(4) and Article 15.

2. The Commission may decide to use IMI as the electronic repository for links referred to in Article 19(1).

Article 36

Reporting and review

By 12 December 2022 and once every two years thereafter, the Commission shall review the application of this Regulation and submit to the European Parliament and to the Council an assessment report on the functioning of the gateway and on the functioning of the internal market on the basis of the statistics and feedback collected in accordance with Articles 24, 25 and 26. The review shall, in particular, evaluate the scope of Article 14, taking into account technological, market and legal developments concerning the exchange of evidence between competent authorities.

Article 37

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 38

Amendment to Regulation (EU) No 1024/2012

Regulation (EU) No 1024/2012 is amended as follows:

(1) Article 1 is replaced by the following:

'Article 1

Subject matter

This Regulation lays down rules for the use of an Internal Market Information System ("IMI") for administrative cooperation among the IMI actors, including the processing of personal data.';

(2) in Article 3, paragraph 1 is replaced by the following:

'1. IMI shall be used for exchanges of information, including of personal data, among the IMI actors and for the processing of that information for the purposes of either of the following:

(a) administrative cooperation required in accordance with the acts listed in the Annex;

(b) administrative cooperation subject to a pilot project carried out in accordance with Article 4.';

(3) in Article 5, the second paragraph is amended as follows:

(a) point (a) is replaced by the following:

'(a) "IMI" means the electronic tool provided by the Commission to facilitate administrative cooperation among the IMI actors;';

(b) point (b) is replaced by the following:

'(b) "administrative cooperation" means the collaboration between IMI actors by exchanging and processing information for the purpose of better application of Union law;';

(c) point (g) is replaced by the following:

'(g) "IMI actors" means the competent authorities, the IMI coordinators, the Commission and the Union bodies, offices and agencies;';

(4) in Article 8(1), the following point is added:

'(f) ensuring coordination with Union bodies, offices and agencies and granting them access to IMI.';

(5) in Article 9, paragraph 4 is replaced by the following:

'4. Appropriate means shall be put in place by the Member States, the Commission and Union bodies, offices and agencies to ensure that IMI users are allowed to access personal data processed in IMI only on a need-to-know basis and within the internal market area or areas for which they were granted access rights in accordance with paragraph 3.';

(6) Article 21 is amended as follows:

(a) paragraph 2 is replaced by the following:

'2. The European Data Protection Supervisor shall be responsible for monitoring and ensuring the application of this Regulation when the Commission or Union bodies, offices and agencies, in their role as IMI actors, process personal data. The duties and powers referred to in Articles 57 and 58 of Regulation (EU) 2018/1725 (*) shall apply accordingly.

(*) 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).';

(b) paragraph 3 is replaced by the following:

'3. The National Supervisory Authorities and the European Data Protection Supervisor, each acting within the scope of their respective competences, shall cooperate with each other to ensure the coordinated supervision of IMI and its use by IMI actors in accordance with Article 62 of Regulation (EU) 2018/1725.';

(c) paragraph 4 is deleted;

(7) in Article 29, paragraph 1 is deleted;

(8) in the Annex, the following points are added:

'11. 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) (*): Article 56, Articles 60 to 66 and Article 70 (1).

12. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (**): Articles 6(4), 15 and 19.

(*) OJ L 119, 4.5.2016, p. 1.
(**) OJ L 295, 21.11.2018, p. 39'.

Article 39

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 2, Article 4, Articles 7 to 12, Article 16, Article 17, Article 18(1) to (4), Article 19, Article 20, Article 24(1), (2) and (3), Article 25(1) to (4), Article 26 and Article 27 shall apply from 12 December 2020.

Article 6, Article 13, Article 14(1) to (8) and (10) and Article 15 shall apply from 12 December 2023.

Notwithstanding the date of application of Articles 2, 9, 10 and 11, municipal authorities shall make the information, explanations and instructions referred to in those Articles available by 12 December 2022 at the latest.

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

Done at Strasbourg, 2 October 2018.

For the European Parliament	*For the Council*
The President	*The President*
A. TAJANI	J. BOGNER-STRAUSS

ANNEX I

List of areas of information relevant for citizens and business exercising their internal market rights referred to in point (a) of Article 2(2)

Areas of information areas related to citizens:

Area	INFORMATION REGARDING RIGHTS, OBLIGATIONS AND RULES ARISING FROM UNION AND NATIONAL LAW
A. Travel within the Union	1. documents required of Union citizens, their family members who are not Union citizens, minors travelling alone and non-Union citizens when travelling across borders within the Union (ID card, visa, passport) 2. rights and obligations of travellers by plane, train, ship, bus in and from the Union, and of those who buy travel packages or linked travel arrangements 3. assistance in case of reduced mobility when travelling in and from the Union 4. transport of animals, plants, alcohol, tobacco, cigarettes and other goods when travelling in the Union 5. voice calling and sending and receiving electronic messages and electronic data within the Union
B. Work and retirement within the Union	1. seeking employment in another Member State 2. taking up employment in another Member State 3. recognition of qualifications with a view to employment in another Member State 4. taxation in another Member State 5. rules on liability and mandatory insurance linked to residence or employment in another Member State 6. terms and conditions of employment, including for posted workers, as stipulated by law or statutory instrument (including information on working hours, paid leave, holiday entitlements, rights and obligations regarding overtime work, health checks, termination of contracts, dismissal and redundancies) 7. equal treatment (rules prohibiting discrimination in the workplace, rules on equal pay for men and women and on equal pay for employees on fixed-term or permanent employment contracts) 8. health and safety obligations in relation to different types of activity 9. social security rights and obligations in the Union including those related to getting pensions
C. Vehicles in the Union	1. taking a motor vehicle temporarily or permanently to another Member State 2. acquiring and renewing a driving licence 3. taking out mandatory motor vehicle insurance 4. buying and selling a motor vehicle in another Member State 5. national traffic rules and requirements for drivers, including general rules for the use of the national road infrastructure: time-based charges (vignette), distance-based charges (toll), emission stickers

Area	INFORMATION REGARDING RIGHTS, OBLIGATIONS AND RULES ARISING FROM UNION AND NATIONAL LAW
D. Residence in another Member State	1. moving temporarily or permanently to another Member State 2. purchasing and selling of immovable property, including any conditions and obligations related to taxation, ownership, or use of such property, including its use as a secondary residence 3. participating in municipal elections and elections to the European Parliament 4. requirements for residence cards for Union citizens and their family members, including family members who are not Union citizens 5. conditions applicable to the naturalisation of nationals from another Member State 6. rules applicable in the case of death, including rules on the repatriation of remains to another Member State
E. Education or traineeship in another Member State	1. education system in another Member State, including early childhood education and care, primary and secondary education, higher education and adult learning 2. volunteering in another Member State 3. traineeships in another Member State 4. conducting research in another Member State as part of an education programme
F. Healthcare	1. getting medical treatment in another Member State 2. buying prescribed pharmaceutical products in a Member State other than the one where the prescription was issued, online or in person 3. health insurance rules applicable in the case of short-term or long-term stays in another Member State, including how to apply for a European Health Insurance Card 4. general information on access rights or obligations to participate in available public preventive healthcare measures 5. services provided through national emergency numbers, including '112' and '116' numbers 6. rights and conditions for moving to a residential care home
G. Citizens' and family rights	1. birth, custody for minor children, parental responsibilities, rules on surrogacy and adoption, including second-parent-adoption, maintenance obligations in relation to children in a cross-border family situation 2. living in a couple with different nationalities, including same-sex couples (marriage, civil or registered partnership, separation, divorce, marital property rights, the rights of cohabitants) 3. rules of gender recognition 4. rights and obligations in relation to succession in another Member State, including tax rules 5. rights and rules applicable in the case of cross-border parental child abduction

Area	INFORMATION REGARDING RIGHTS, OBLIGATIONS AND RULES ARISING FROM UNION AND NATIONAL LAW
H. Consumer rights	1. buying goods, digital content or services (including financial services) from another Member State, online or in person 2. holding a bank account in another Member State 3. connection to utilities, such as gas, electricity, water, household waste disposal, telecoms and the internet 4. payments, including credit transfers, delays in cross-border payments 5. consumer rights and guarantees related to buying goods and services, including procedures for consumer dispute resolution and compensation 6. safety and security of consumer products 7. renting a motor vehicle
I. Protection of personal data	1. exercising data subjects' rights in relation to the protection of personal data

Areas of information related to businesses:

Area	INFORMATION REGARDING RIGHTS, OBLIGATIONS AND RULES
J. Starting, running and closing a business	1. registering, changing the legal form of or closing a business (registration procedures and legal forms for carrying out business) 2. moving a business to another Member State 3. intellectual property rights (applying for a patent, registering a trademark, a drawing or a design, getting a licence for reproduction) 4. fairness and transparency in commercial practices, including consumer rights and guarantees related to selling goods and services 5. offering online facilities for cross-border payments when selling goods and services online 6. rights and obligations arising under contract law, including late payment interests 7. insolvency proceedings and liquidation of companies 8. credit insurance 9. mergers of companies or selling a business 10. civil liability of directors of a company 11. rules and obligations regarding the processing of personal data

Area	INFORMATION REGARDING RIGHTS, OBLIGATIONS AND RULES
K. Employees	1. terms of employment stipulated by law or statutory instrument (including working hours, paid leave, holiday entitlements, rights and obligations regarding overtime work, health checks, termination of contracts, dismissals and redundancies) 2. social security rights and obligations in the Union (registering as employer, registering employees, notifying the end of contract of an employee, paying social contributions, rights and obligations related to pensions) 3. employment of workers in other Member States (posting of workers, rules on freedom to provide services, residency requirements for workers) 4. equal treatment (rules prohibiting discrimination in the workplace, rules on equal pay for men and women and equal pay for employees on fixed-term or under permanent employment contracts) 5. rules on staff representation
L. Taxes	1. VAT: information on the general rules, rates and exemptions, registering for and paying VAT, obtaining a refund 2. excise duties: information on the general rules, rates and exemptions, registration for excise tax purposes and payment of excise tax, obtaining a refund 3. customs duties and other taxes and duties collected on imports 4. customs procedures for imports and exports under the Union Customs Code 5. other taxes: payment, rates, tax returns
M. Goods	1. obtaining CE marking 2. product rules and requirements 3. identifying applicable standards, technical specifications and getting products certified 4. mutual recognition of products not subject to Union specifications 5. requirements regarding classification, labelling and packaging for hazardous chemicals 6. distance/off-premises selling: information to be given to customers in advance, confirmation of the contract in writing, withdrawal from a contract, delivering of the goods, other specific obligations 7. defective products: consumer rights and guarantees, after-sale responsibilities, means of redress for an injured party 8. certification, labels (EMAS, energy labels, Eco-design, EU eco-label) 9. recycling and waste management
N. Services	1. acquiring licences, authorisations or permits with a view to starting and operating a business 2. notifying the authorities of cross-border activities 3. recognition of professional qualifications, including vocational education and training

Area	INFORMATION REGARDING RIGHTS, OBLIGATIONS AND RULES
O. Funding a business	1. obtaining access to finance at the Union level, including Union funding programmes and business grants 2. obtaining access to finance at national level 3. initiatives addressed to entrepreneurs (exchanges organised for new entrepreneurs, mentoring programmes, etc.)
P. Public contracts	1. participating in public tenders: rules and procedures 2. submitting a bid online in response to a public call for tender 3. reporting irregularities in relation to the tender process
Q. Health and safety at work	1. health and safety obligations in relation to different types of activity, including risk prevention, information and training

ANNEX II

Procedures referred to in Article 6(1)

Life events	Procedures	Expected output subject to an assessment of the application by the competent authority in accordance with national law, where relevant
Birth	Requesting proof of registration of birth	Proof of registration of birth or birth certificate
Residence	Requesting proof of residence	Confirmation of registration at the current address
Studying	Applying for a tertiary education study financing, such as study grants and loans from a public body or institution	Decision on the application for financing or acknowledgement of receipt
	Submitting an initial application for admission to public tertiary education institution	Confirmation of the receipt of application
	Requesting academic recognition of diplomas, certificates or other proof of studies or courses	Decision on the request for recognition
Working	Request for determination of applicable legislation in accordance with Title II of Regulation (EC) No 883/2004 ([1])	Decision on applicable legislation
	Notifying changes in the personal or professional circumstances of the person receiving social security benefits, relevant for such benefits	Confirmation of receipt of notification of such changes
	Application for a European Health Insurance Card (EHIC)	European Health Insurance Card (EHIC)
	Submitting an income tax declaration	Confirmation of the receipt of the declaration
Moving	Registering a change of address	Confirmation of deregistration at the previous address and of the registration of the new address
	Registering a motor vehicle originating from or already registered in a Member State, in standard procedures ([2])	Proof of registration of a motor vehicle
	Obtaining stickers for the use of the national road infrastructure: time-based charges (vignette), distance-based charges (toll), issued by a public body or institution	Receipt of toll sticker or vignette or other proof of payment
	Obtaining emission stickers issued by a public body or institution	Receipt of emission sticker or other proof of payment

Life events	Procedures	Expected output subject to an assessment of the application by the competent authority in accordance with national law, where relevant
Retiring	Claiming pension and pre-retirement benefits from compulsory schemes	Confirmation of the receipt of the claim or decision regarding the claim for a pension or pre-retirement benefits
	Requesting information on the data related to pension from compulsory schemes	Statement of personal pension data
Starting, running and closing a business	Notification of business activity, permission for exercising a business activity, changes of business activity and the termination of a business activity not involving insolvency or liquidation procedures, excluding the initial registration of a business activity with the business register and excluding procedures concerning the constitution of or any subsequent filing by companies or firms within the meaning of the second paragraph of Article 54 TFEU	Confirmation of the receipt of notification or change, or of the request for permission for business activity
	Registration of an employer (a natural person) with compulsory pension and insurance schemes	Confirmation of registration or social security registration number
	Registration of employees with compulsory pension and insurance schemes	Confirmation of registration or social security registration number
	Submitting a corporate tax declaration	Confirmation of the receipt of the declaration
	Notification to the social security schemes of the end of contract with an employee, excluding procedures for the collective termination of employee contracts	Confirmation of the receipt of the notification
	Payment of social contributions for employees	Receipt or other form of confirmation of payment of social contributions for employees

([1]) Regulation (EC) No 883/2004 of the European Parliament and of the Council of 29 April 2004 on the coordination of social security systems (OJ L 166, 30.4.2004, p. 1).

([2]) This covers the following vehicles: (a) any motor vehicle or trailer as referred to in Article 3 of Directive 2007/46/EC of the European Parliament and of the Council (OJ L 263, 9.10.2007, p. 1); and (b) any two- or three-wheel motor vehicle, whether twin-wheeled or otherwise, intended to travel on the road, as referred to in Article 1 of Regulation (EU) No 168/2013 of the European Parliament and of the Council (OJ L 60, 2.3.2013, p. 52).

ANNEX III

List of the assistance and problem-solving services referred to in point (c) of Article 2(2)

(1) Points of single contact ([1])

(2) Product Contact Points ([2])

(3) Product Contact Points for Construction ([3])

(4) National assistance centres for professional qualifications ([4])

(5) National contact points for cross-border healthcare ([5])

(6) European network of employment services (EURES) ([6])

(7) Online dispute resolution (ODR) ([7])

([1]) 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).

([2]) Regulation (EC) No 764/2008 of the European Parliament and of the Council of 9 July 2008 laying down procedures relating to the application of certain national technical rules to products lawfully marketed in another Member State and repealing Decision No 3052/95/EC (OJ L 218, 13.8.2008, p. 21).

([3]) Regulation (EU) No 305/2011 of the European Parliament and of the Council of 9 March 2011 laying down harmonised conditions for the marketing of construction products and repealing Council Directive 89/106/EEC (OJ L 88, 4.4.2011, p. 5).

([4]) Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications (OJ L 255, 30.9.2005, p. 22).

([5]) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

([6]) Regulation (EU) 2016/589 of the European Parliament and of the Council of 13 April 2016 on a European network of employment services (EURES), workers' access to mobility services and the further integration of labour markets, and amending Regulations (EU) No 492/2011 and (EU) No 1296/2013 (OJ L 107, 22.4.2016, p. 1).

([7]) Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR) (OJ L 165, 18.6.2013, p. 1).

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

(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 16(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]),

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

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her. This right is also guaranteed under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(2) Regulation (EC) No 45/2001 of the European Parliament and of the Council ([3]) provides natural persons with legally enforceable rights, specifies the data processing obligations of controllers within the Community institutions and bodies, and creates an independent supervisory authority, the European Data Protection Supervisor, responsible for monitoring the processing of personal data by the Union institutions and bodies. However, it does not apply to the processing of personal data in the course of an activity of Union institutions and bodies which fall outside the scope of Union law.

(3) Regulation (EU) 2016/679 of the European Parliament and of the Council ([4]) and Directive (EU) 2016/680 of the European Parliament and of the Council ([5]) were adopted on 27 April 2016. While the Regulation lays down general rules to protect natural persons with regard to the processing of personal data and to ensure the free movement of personal data within the Union, the Directive lays down the specific rules to protect natural persons with regard to the processing of personal data and to ensure the free movement of personal data within the Union in the fields of judicial cooperation in criminal matters and police cooperation.

(4) Regulation (EU) 2016/679 provides for the adaptation of Regulation (EC) No 45/2001 in order to ensure a strong and coherent data protection framework in the Union and to allow its application in parallel with Regulation (EU) 2016/679.

(5) It is in the interest of a coherent approach to personal data protection throughout the Union, and of the free movement of personal data within the Union, to align as far as possible the data protection rules for Union institutions, bodies, offices and agencies with the data protection rules adopted for the public sector in the Member States. Whenever the provisions of this Regulation follow the same principles as the provisions of Regulation (EU)

([1]) OJ C 288, 31.8.2017, p. 107.

([2]) Position of the European Parliament of 13 September 2018 (not yet published in the Official Journal) and decision of the Council of 11 October 2018.

([3]) Regulation (EC) No 45/2001 of the European Parliament and 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).

([4]) 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).

([5]) 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).

2016/679, those two sets of provisions should, under the case law of the Court of Justice of the European Union (the 'Court of Justice'), be interpreted homogeneously, in particular because the scheme of this Regulation should be understood as equivalent to the scheme of Regulation (EU) 2016/679.

(6) Persons whose personal data are processed by Union institutions and bodies in any context whatsoever, for example, because they are employed by those institutions and bodies, should be protected. This Regulation should not apply to the processing of personal data of deceased persons. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

(7) In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used.

(8) This Regulation should apply to the processing of personal data by all Union institutions, bodies, offices and agencies. It should apply to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

(9) In Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the conference acknowledged that specific rules on the protection of personal data and on the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU could prove necessary because of the specific nature of those fields. A distinct Chapter of this Regulation containing general rules should therefore apply to the processing of operational personal data, such as personal data processed for the purposes of a criminal investigation by Union bodies, offices or agencies when carrying out activities in the fields of judicial cooperation in criminal matters and police cooperation.

(10) Directive (EU) 2016/680 sets out harmonised rules for the protection and the free movement of personal data processed for the purposes of the prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. In order to ensure the same level of protection for natural persons through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between Union bodies, offices or agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU and competent authorities, the rules for the protection and the free movement of operational personal data processed by such Union bodies, offices or agencies should be consistent with Directive (EU) 2016/680.

(11) The general rules of the Chapter of this Regulation on the processing of operational personal data should apply without prejudice to the specific rules applicable to the processing of operational personal data by Union bodies, offices and agencies when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU. Such specific rules should be regarded as *lex specialis* to the provisions in the Chapter of this Regulation on the processing of operational personal data (*lex specialis derogat legi generali*). In order to reduce legal fragmentation, specific data protection rules applicable to the processing of operational personal data by Union bodies, offices or agencies when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU should be consistent with the principles underpinning the Chapter of this Regulation on the processing of operational personal data, as well as with the provisions of this Regulation relating to independent supervision, remedies, liability and penalties.

(12) The Chapter of this Regulation on the processing of operational personal data should apply to Union bodies, offices and agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU, whether they exercise such activities as their main or ancillary tasks, for the purposes of the prevention, detection, investigation or prosecution of criminal offences. However, it should not apply to Europol or to the European Public Prosecutor's Office until the legal acts establishing Europol and the European Public Prosecutor's Office are amended with a view to rendering the Chapter of this Regulation on the processing of operational personal data, as adapted, applicable to them.

(13) The Commission should conduct a review of this Regulation, in particular the Chapter of this Regulation on the processing of operational personal data. The Commission should also conduct a review of other legal acts adopted on the basis of the Treaties which regulate the processing of operational personal data by Union bodies, offices or

agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU. After such a review, in order to ensure uniform and consistent protection of natural persons with regard to the processing of personal data, the Commission should be able to make any appropriate legislative proposals, including any necessary adaptations of the Chapter of this Regulation on the processing of operational personal data, with a view to applying it to Europol and to the European Public Prosecutor's Office. The adaptations should take into account provisions relating to independent supervision, remedies, liability and penalties.

(14) The processing of administrative personal data, such as staff data, by Union bodies, offices or agencies carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU should be covered by this Regulation.

(15) This Regulation should apply to the processing of personal data by Union institutions, bodies, offices or agencies carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union (TEU). This Regulation should not apply to the processing of personal data by missions referred to in Articles 42(1), 43 and 44 TEU, which implement the common security and defence policy. Where appropriate, relevant proposals should be put forward to further regulate the processing of personal data in the field of the common security and defence policy.

(16) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person, to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

(17) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

(18) Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

(19) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided. At the same time, the data subject should have the right to withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal. In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller and it is therefore unlikely that consent was freely given

in all the circumstances of that specific situation. It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have an opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

(20) Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing and for preventing its unauthorised disclosure when it is transmitted.

(21) In accordance with the principle of accountability, where Union institutions and bodies transmit personal data within the same Union institution or body and the recipient is not part of the controller, or to other Union institutions or bodies, they should verify whether such personal data are required for the legitimate performance of tasks within the competence of the recipient. In particular, following a recipient's request for transmission of personal data, the controller should verify the existence of a relevant ground for lawfully processing personal data and the competence of the recipient. The controller should also make a provisional evaluation of the necessity of the transmission of the data. If doubts arise as to this necessity, the controller should seek further information from the recipient. The recipient should ensure that the necessity of the transmission of the data can be subsequently verified.

(22) In order for processing to be lawful, personal data should be processed on the basis of the necessity for the performance of a task carried out in the public interest by Union institutions and bodies or in the exercise of their official authority, the necessity for compliance with a legal obligation to which the controller is subject or some other legitimate basis under this Regulation, including the consent of the data subject concerned, the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. Processing of personal data for the performance of tasks carried out in the public interest by the Union institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies. The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject, as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread, or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

(23) The Union law referred to in this Regulation should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the requirements set out in the Charter and the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(24) The internal rules referred to in this Regulation should be clear and precise acts of general application intended to produce legal effects vis-à-vis data subjects. They should be adopted at the highest level of management of the Union institutions and bodies, within their competencies and in matters relating to their operation. They should be published in the *Official Journal of the European Union*. The application of those rules should be foreseeable to persons subject to them in accordance with the requirements set out in the Charter and the European Convention for the Protection of Human Rights and Freedoms. Internal rules may take the form of decisions, in particular when adopted by Union institutions.

(25) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

(26) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC ([1]), a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

(27) Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to creating personality profiles and to the collection of personal data with regard to children when services are offered directly to a child on websites of Union institutions and bodies, such as interpersonal communication services or online selling of tickets, and the processing of personal data is based on consent.

(28) When recipients established in the Union other than Union institutions and bodies would like to have personal data transmitted to them by Union institutions and bodies, those recipients should demonstrate that it is necessary to have the data transmitted to these recipients either for the performance of their task carried out in the public interest or in the exercise of official authority vested in them. Alternatively, those recipients should demonstrate that the transmission is necessary for a specific purpose in the public interest and the controller should establish whether there is any reason to assume that the data subject's legitimate interests might be prejudiced. In such cases, the controller should demonstrably weigh the various competing interests in order to assess the proportionality of the

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

requested transmission of personal data. The specific purpose in the public interest could relate to the transparency of Union institutions and bodies. Furthermore, Union institutions and bodies should demonstrate such necessity when they themselves initiate a transmission, in compliance with the principle of transparency and good administration. The requirements laid down in this Regulation for transmissions to recipients established in the Union other than Union institutions and bodies should be understood as supplementary to the conditions for lawful processing.

(29) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection, as the context of their processing could create significant risks to the fundamental rights and freedoms. Such personal data should not be processed unless the specific conditions set out in this Regulation are met. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. In addition to the specific requirements for processing of sensitive data, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs, in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

(30) Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union law should provide for specific and suitable measures so as to protect fundamental rights and the personal data of natural persons.

(31) The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council ([1]), namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, healthcare needs, resources allocated to healthcare, the provision of, and universal access to, healthcare as well as healthcare expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes.

(32) If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through an authentication mechanism such as the same credentials, used by the data subject to log in to the online service offered by the data controller.

(33) The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be

([1]) Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70).

carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Union institutions and bodies should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in Union law, which may include internal rules adopted by Union institutions and bodies in matters relating to their operation.

(34) Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

(35) The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.

(36) The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.

(37) A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

(38) A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union law to which the controller is subject. A data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is

not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

(39) To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.

(40) Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.

(41) To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.

(42) Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.

(43) The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects

concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.

However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union law. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child. In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject. and prevent, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or processing that results in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.

(44) Legal acts adopted on the basis of the Treaties or internal rules adopted by Union institutions and bodies in matters relating to their operation may impose restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, confidentiality of electronic communications data as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers, as far as necessary and proportionate in a democratic society to safeguard public security and for the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties. This includes safeguarding against and the prevention of threats to public security, protection of human life especially in response to natural or manmade disasters, internal security of Union institutions and bodies, other important objectives of general public interest of the Union or of a Member State, in particular the objectives of the Common Foreign and Security Policy of the Union or an important economic or financial interest of the Union or of a Member State, and keeping of public registers for reasons of general public interest or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes.

(45) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

(46) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

(47) The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

(48) The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

(49) Regulation (EU) 2016/679 provides for controllers to demonstrate compliance by adherence to approved certification mechanisms. Likewise, Union institutions and bodies should be able to demonstrate compliance with this Regulation by obtaining certification in accordance with Article 42 of Regulation (EU) 2016/679.

(50) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(51) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which meet the requirements of this Regulation, including for the security of processing. The adherence of processors other than Union institutions and bodies to an approved code of conduct or an approved certification mechanism can be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor other than a Union institution or body should be governed by a contract, or, in case of Union institutions and bodies acting as processors, by a contract or other legal act under Union law, binding the processor to the controller, setting out the subject matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor should be able to choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by the European Data Protection Supervisor and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store that personal data under Union or Member State law to which the processor is subject.

(52) In order to demonstrate compliance with this Regulation, controllers should maintain records of processing activities under their responsibility and processors should maintain records of categories of processing activities under their responsibility. Union institutions and bodies should be obliged to cooperate with the European Data Protection Supervisor and make their records available to it on request, so that they might serve for monitoring those processing operations. Unless it is not appropriate taking into account the size of a Union institution or body, Union institutions and bodies should be able to establish a central register of records of their processing activities. For reasons of transparency, they should also be able to make such a register public.

(53) In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal

data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

(54) Union institutions and bodies should ensure the confidentiality of electronic communications provided for by Article 7 of the Charter. In particular, Union institutions and bodies should ensure the security of their electronic communications networks. They should protect the information related to the terminal equipment of users accessing their publicly available websites and mobile applications, in accordance with the Directive 2002/58/EC of the European Parliament and of the Council ([1]). They should also protect the personal data stored in directories of users.

(55) A personal data breach could, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify that personal data breach to the European Data Protection Supervisor without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, it should be accompanied by the reasons for the delay and information can be provided in phases without further undue delay. Where such delay is justified, less sensitive or less specific information on the breach should be released as early as possible, rather than fully resolving the underlying incident before notifying.

(56) The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the European Data Protection Supervisor, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities.

(57) Regulation (EC) No 45/2001 provides for a general obligation on a controller to notify the processing of personal data to the data protection officer. Unless it is not appropriate taking into account the size of the Union institution or body, the data protection officer is to keep a register of notified processing operations. Besides this general obligation, effective procedures and mechanisms should be put in place to monitor processing operations that are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such procedures should, in particular, also be in place where types of processing operations involve using new technologies, or are of a new kind in relation to which no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing. In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.

(58) Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the European Data Protection Supervisor should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which could result also in a realisation of damage or interference with the rights and freedoms of the natural person. The European Data Protection Supervisor should respond to the request for consultation within a specified period. However, the absence of a reaction of the European Data Protection

([1]) 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).

Supervisor within that period should be without prejudice to any intervention of the European Data Protection Supervisor in accordance with his or her tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, it should be possible to submit the outcome of a data protection impact assessment carried out with regard to the processing at issue to the European Data Protection Supervisor, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.

(59) The European Data Protection Supervisor should be informed of administrative measures and consulted on internal rules adopted by Union institutions and bodies in matters relating to their operation when they provide for the processing of personal data, lay down conditions for restricting the rights of data subjects or provide appropriate safeguards for data subject rights, in order to ensure that the intended processing complies with this Regulation, in particular as regards mitigating the risks involved for the data subject.

(60) Regulation (EU) 2016/679 established the European Data Protection Board as an independent body of the Union with legal personality. The Board should contribute to the consistent application of Regulation (EU) 2016/679 and Directive (EU) 2016/680 throughout the Union, including by advising the Commission. At the same time, the European Data Protection Supervisor should continue to exercise his or her supervisory and advisory functions in respect of all Union institutions and bodies, on his or her own initiative or upon request. In order to ensure consistency of data protection rules throughout the Union, when preparing proposals or recommendations, the Commission should endeavour to consult the European Data Protection Supervisor. A consultation by the Commission should be obligatory following the adoption of legislative acts or during the preparation of delegated acts and implementing acts as defined in Article 289, 290 and 291 TFEU and following the adoption of recommendations and proposals relating to agreements with third countries and international organisations as provided for in Article 218 TFEU which have an impact on the right to protection of personal data. In such cases, the Commission should be obliged to consult the European Data Protection Supervisor, except where the Regulation (EU) 2016/679 provides for mandatory consultation of the European Data Protection Board, for example on adequacy decisions or delegated acts on standardised icons and requirements for certification mechanisms. Where the act in question is of particular importance for the protection of rights and freedoms of natural persons with regard to the processing of personal data, the Commission should be able, in addition, to consult the European Data Protection Board. In those cases, the European Data Protection Supervisor should, as a member of the European Data Protection Board, coordinate his or her work with the latter with a view to issuing a joint opinion. The European Data Protection Supervisor, and where applicable, the European Data Protection Board should provide their written advice within eight weeks. That time-frame should be shorter in urgent cases or where otherwise appropriate, for example when the Commission is preparing delegated and implementing acts.

(61) In accordance with Article 75 of Regulation (EU) 2016/679, the European Data Protection Supervisor should provide the secretariat of the European Data Protection Board.

(62) In all Union institutions and bodies a data protection officer should ensure that the provisions of this Regulation are applied and should advise controllers and processors on fulfilling their obligations. That officer should be a person with expert knowledge of data protection law and practices, which should be determined in particular according to the data processing operations carried out by the controller or the processor and the protection required for the personal data involved. Such data protection officers should be in a position to perform their duties and tasks in an independent manner.

(63) When personal data are transferred from the Union institutions and bodies to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should be guaranteed. The same guarantees should apply in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation and respecting the fundamental rights and freedoms enshrined in the Charter. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.

(64) The Commission can decide, under Article 45 of Regulation (EU) 2016/679 or under Article 36 of Directive (EU) 2016/680, that a third country, a territory or specified sector within a third country or an international organisation offers an adequate level of data protection. In such cases, transfers of personal data to that third country or international organisation by a Union institution or body can take place without the need to obtain any further authorisation.

(65) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards can consist of making use of standard data protection clauses adopted by the Commission, standard data protection clauses adopted by the European Data Protection Supervisor or contractual clauses authorised by the European Data Protection Supervisor. Where the processor is not a Union institution or body those appropriate safeguards can also consist of binding corporate rules, codes of conduct and certification mechanisms used for international transfers under Regulation (EU) 2016/679. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by Union institutions and bodies to public authorities or bodies in third countries or to international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the European Data Protection Supervisor should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding.

(66) The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by the European Data Protection Supervisor should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by the European Data Protection Supervisor or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard data-protection clauses.

(67) Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of Union institutions and bodies. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement in force between the requesting third country and the Union. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union law.

(68) Provision should be made in specific situations for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In the latter case, such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register, unless authorised by Union law, and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.

(69) Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between Union institutions and bodies and competition authorities, tax or customs administrations, financial supervisory authorities and services competent for social security matters or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should also be regarded as lawful where it is

necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. In the absence of an adequacy decision, Union law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organisation. Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject.

(70) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.

(71) When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights, in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, national supervisory authorities and the European Data Protection Supervisor can be unable to pursue complaints or conduct investigations relating to the activities outside their jurisdiction. Their efforts to work together in the cross-border context can also be hampered by insufficient preventive or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, closer cooperation between the European Data Protection Supervisor and national supervisory authorities should be promoted to help the exchange of information with their international counterparts.

(72) The establishment in Regulation (EC) No 45/2001 of the European Data Protection Supervisor, who is empowered to perform his or her tasks and exercise his or her powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. This Regulation should further strengthen and clarify his or her role and independence. The European Data Protection Supervisor should be a person whose independence is beyond doubt and who is acknowledged as having the experience and skills required to perform the duties of European Data Protection Supervisor, for example because he or she has belonged to one of the supervisory authorities established under Article 51 of Regulation (EU) 2016/679.

(73) In order to ensure consistent monitoring and enforcement of data protection rules throughout the Union, the European Data Protection Supervisor should have the same tasks and effective powers as the national supervisory authorities, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, powers to bring infringements of this Regulation to the attention of the Court of Justice and powers to engage in legal proceedings in accordance with the primary law. Such powers should also include the power to impose a temporary or definitive limitation, including a ban, on processing. In order to avoid superfluous costs and excessive inconveniencies for the persons concerned who might be adversely affected, each measure of the European Data Protection Supervisor should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, should take into account the circumstances of each individual case and respect the right of every person to be heard before any individual measure concerned is taken. Each legally binding measure of the European Data Protection Supervisor should be in writing, be clear and unambiguous, indicate the date of issue of the measure, bear the signature of the European Data Protection Supervisor, give the reasons for the measure, and refer to the right to an effective remedy.

(74) The supervisory competence of the European Data Protection Supervisor should not cover the processing of personal data by the Court of Justice when acting in its judicial capacity, in order to safeguard the independence of the Court in the performance of its judicial tasks, including decision-making. For such processing operations, the Court should establish independent supervision, in accordance with Article 8(3) of the Charter, for example through an internal mechanism.

(75) The decisions of the European Data Protection Supervisor regarding exemptions, guarantees, authorisations and conditions relating to data processing operations, as defined in this Regulation, should be published in the activities report. Independently of the publication of an annual activities report, the European Data Protection Supervisor can publish reports on specific subjects.

(76) The European Data Protection Supervisor should comply with Regulation (EC) No 1049/2001 of the European Parliament and of the Council ([1]).

(77) The national supervisory authorities monitor the application of Regulation (EU) 2016/679 and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. In order to increase consistency in the application of data protection rules applicable in Member States and of data protection rules applicable to Union institutions and bodies, the European Data Protection Supervisor should cooperate effectively with the national supervisory authorities.

(78) In certain instances, Union law provides for a model of coordinated supervision, shared between the European Data Protection Supervisor and the national supervisory authorities. The European Data Protection Supervisor is also the supervisory authority of Europol and for these purposes, a specific model of cooperation with the national supervisory authorities has been established through a cooperation board with an advisory function. In order to improve the effective supervision and enforcement of substantive data protection rules, a single, coherent model of coordinated supervision should be introduced in the Union. The Commission should therefore make legislative proposals where appropriate with a view to amending Union legal acts providing for a model of coordinated supervision, in order to align them with the coordinated supervision model of this Regulation. The European Data Protection Board should serve as a single forum for ensuring effective coordinated supervision in all areas.

(79) Every data subject should have the right to lodge a complaint with the European Data Protection Supervisor, and the right to an effective judicial remedy before the Court of Justice in accordance with the Treaties, if the data subject considers that his or her rights under this Regulation are infringed or where the European Data Protection Supervisor does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The European Data Protection Supervisor should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further coordination with a national supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, the European Data Protection Supervisor should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

(80) Any person who has suffered material or non-material damage as a result of an infringement of this Regulation should have the right to receive compensation from the controller or processor for the damage suffered, subject to the conditions provided for in the Treaties.

(81) In order to strengthen the supervisory role of the European Data Protection Supervisor and the effective enforcement of this Regulation, the European Data Protection Supervisor should, as a sanction of last resort, have the power to impose administrative fines. The fines should aim at sanctioning the Union institution or body — rather than individuals — for non-compliance with this Regulation, to deter future violations of this Regulation and to foster a culture of personal data protection within the Union institutions and bodies. This Regulation should indicate the infringements subject to administrative fines and the upper limits and criteria for setting the associated fines. The European Data Protection Supervisor should determine the amount of the fine in each individual case, by taking into account all relevant circumstances of the specific situation, with due regard to the nature, gravity and duration of the infringement, its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. When imposing an administrative fine on a Union institution or body, the European Data Protection Supervisor should consider the proportionality of amount of the fine. The administrative procedure for the imposition of fines on Union institutions and bodies should respect the general principles of Union law as interpreted by the Court of Justice.

(82) Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with Union law or the law of a Member State, has statutory objectives which are in the public interest and is active in the field of

([1]) 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).

the protection of personal data to lodge a complaint on his or her behalf with the European Data Protection Supervisor. Such a body, organisation or association should also be able to exercise the right to a judicial remedy on behalf of data subjects or exercise the right to receive compensation on behalf of data subjects.

(83) An official or other servant of the Union who fails to comply with the obligations in this Regulation should be liable to disciplinary or other action, in accordance with the rules and procedures laid down in the Staff Regulations of Officials of the European Union and the Conditions of Employment of Other Servants of the Union, laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68 ([1]) ('Staff Regulations').

(84) 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 the Council ([2]). The examination procedure should be used for the adoption of standard contractual clauses between controllers and processors and between processors, for the adoption of a list of processing operations requiring prior consultation of the European Data Protection Supervisor by controllers processing personal data for the performance of a task carried out in the public interest, and for the adoption of standard contractual clauses providing appropriate safeguards for international transfers.

(85) The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in accordance with the statistical principles set out in Article 338(2) TFEU. Regulation (EC) No 223/2009 of the European Parliament and of the Council ([3]) provides further specifications on statistical confidentiality for European statistics.

(86) Regulation (EC) No 45/2001 and Decision No 1247/2002/EC of the European Parliament, of the Council and of the Commission ([4]) should be repealed. The references to the repealed Regulation and Decision should be construed as references to this Regulation.

(87) In order to safeguard the full independence of the members of the independent supervisory authority, the terms of office of the current European Data Protection Supervisor and the current Assistant Supervisor should not be affected by this Regulation. The current Assistant Supervisor should remain in place until the end of his term of office, unless one of the conditions for the premature end of term of the European Data Protection Supervisor laid down in this Regulation is met. The relevant provisions of this Regulation should apply to the Assistant Supervisor until the end of his term of office.

(88) In accordance with the principle of proportionality, it is necessary and appropriate for the achievement of the basic objective of ensuring an equivalent level of protection of natural persons with regard to the processing of personal data and the free flow of personal data throughout the Union to lay down rules on processing of personal data in Union institutions and bodies. This Regulation does not go beyond what is necessary in order to achieve the objectives pursued in accordance with Article 5(4) of the TEU.

(89) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 15 March 2017 ([5]),

---

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

([2]) 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).

([3]) Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (OJ L 87, 31.3.2009, p. 164).

([4]) Decision No 1247/2002/EC of the European Parliament, of the Council and of the Commission of 1 July 2002 on the regulations and general conditions governing the performance of the European Data protection Supervisor's duties (OJ L 183, 12.7.2002, p. 1).

([5]) OJ C 164, 24.5.2017, p. 2.

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data by the Union institutions and bodies and rules relating to the free movement of personal data between them or to other recipients established in the Union.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The European Data Protection Supervisor shall monitor the application of the provisions of this Regulation to all processing operations carried out by a Union institution or body.

Article 2

Scope

1. This Regulation applies to the processing of personal data by all Union institutions and bodies.

2. Only Article 3 and Chapter IX of this Regulation shall apply to the processing of operational personal data by Union bodies, offices and agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU.

3. This Regulation shall not apply to the processing of operational personal data by Europol and the European Public Prosecutor's Office, until Regulation (EU) 2016/794 of the European Parliament and of the Council ([1]) and Council Regulation (EU) 2017/1939 ([2]) are adapted in accordance with Article 98 of this Regulation.

4. This Regulation shall not apply to the processing of personal data by missions referred to in Articles 42(1), 43 and 44 TEU.

5. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Article 3

Definitions

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

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) 'operational personal data' means all personal data processed by Union bodies, offices or agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU to meet the objectives and tasks laid down in the legal acts establishing those bodies, offices or agencies;

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

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

(3) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(4) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

(5) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(6) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(7) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(8) 'controller' means the Union institution or body or the directorate-general or any other organisational entity which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by a specific Union act, the controller or the specific criteria for its nomination can be provided for by Union law;

(9) 'controllers other than Union institutions and bodies' means controllers within the meaning of point (7) of Article 4 of Regulation (EU) 2016/679 and controllers within the meaning of point (8) of Article 3 of Directive (EU) 2016/680;

(10) 'Union institutions and bodies' means the Union institutions, bodies, offices and agencies set up by, or on the basis of, the TEU, the TFEU or the Euratom Treaty;

(11) 'competent authority' means any public authority in a Member State competent for the 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;

(12) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(13) 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(14) 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

(15) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(16) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(17) 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(18) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(19) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about his or her health status;

(20) 'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council ([1]);

(21) 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

(22) 'national supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51 of Regulation (EU) 2016/679 or pursuant to Article 41 of Directive (EU) 2016/680;

(23) 'user' means any natural person using a network or terminal equipment operated under the control of a Union institution or body;

(24) 'directory' means a publicly available directory of users or an internal directory of users available within a Union institution or body or shared between Union institutions and bodies, whether in printed or electronic form;

(25) 'electronic communications network' means a transmission system, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched including internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;

(26) 'terminal equipment' means terminal equipment as defined in point (1) of Article 1 of Commission Directive 2008/63/EC ([2]).

CHAPTER II

GENERAL PRINCIPLES

Article 4

Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 13, not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

([1]) 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).

([2]) Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (OJ L 162, 21.6.2008, p. 20).

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 13 subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 5

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body;

(b) processing is necessary for compliance with a legal obligation to which the controller is subject;

(c) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(d) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(e) processing is necessary in order to protect the vital interests of the data subject or of another natural person.

2. The basis for the processing referred to in points (a) and (b) of paragraph 1 shall be laid down in Union law.

Article 6

Processing for another compatible purpose

Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on Union law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 25(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 10, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 11;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 7

Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 8

Conditions applicable to a child's consent in relation to information society services

1. Where point (d) of Article 5(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 13 years old. Where the child is below the age of 13 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

Article 9

Transmissions of personal data to recipients established in the Union other than Union institutions and bodies

1. Without prejudice to Articles 4 to 6 and 10, personal data shall only be transmitted to recipients established in the Union other than Union institutions and bodies if:

(a) the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the recipient; or

(b) the recipient establishes that it is necessary to have the data transmitted for a specific purpose in the public interest and the controller, where there is any reason to assume that the data subject's legitimate interests might be prejudiced, establishes that it is proportionate to transmit the personal data for that specific purpose after having demonstrably weighed the various competing interests.

2. Where the controller initiates the transmission under this Article, it shall demonstrate that the transmission of personal data is necessary for and proportionate to the purposes of the transmission by applying the criteria laid down in points (a) or (b) of paragraph 1.

3. Union institutions and bodies shall reconcile the right to the protection of personal data with the right of access to documents in accordance with Union law.

Article 10

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law insofar as it is authorised by Union law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) the processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent;

(d) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a non-profit-seeking body which constitutes an entity integrated in a Union institution or body and with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of this body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects;

(e) the processing relates to personal data which are manifestly made public by the data subject;

(f) the processing is necessary for the establishment, exercise or defence of legal claims or whenever the Court of Justice is acting in its judicial capacity;

(g) the processing is necessary for reasons of substantial public interest, on the basis of Union law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) the processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of Union law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; or

(j) the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on Union law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by, or under the responsibility of, a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies, or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

Article 11

Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 5(1) shall be carried out only under control of official authority or when the processing is authorised by Union law providing for appropriate safeguards for the rights and freedoms of data subjects.

Article 12

Processing which does not require identification

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 17 to 22 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

Article 13

Safeguards relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

CHAPTER III

RIGHTS OF THE DATA SUBJECT

SECTION 1

Transparency and modalities

Article 14

Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Articles 15 and 16 and any communication under Articles 17 to 24 and 35 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 17 to 24. In the cases referred to in Article 12(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 17 to 24, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 17 to 24 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the European Data Protection Supervisor and seeking a judicial remedy.

5. Information provided under Articles 15 and 16 and any communication and any actions taken under Articles 17 to 24 and 35 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 12, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 17 to 23, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 15 and 16 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. Where the Commission adopts delegated acts pursuant to Article 12(8) of Regulation (EU) 2016/679 determining the information to be presented by the icons and the procedures for providing standardised icons, Union institutions and bodies shall, where appropriate, provide the information pursuant to Articles 15 and 16 of this Regulation in combination with such standardised icons.

SECTION 2

Information and access to personal data

Article 15

Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller;

(b) the contact details of the data protection officer;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the recipients or categories of recipients of the personal data, if any;

(e) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 48, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or, where applicable, the right to object to processing or the right to data portability;

(c) where the processing is based on point (d) of Article 5(1) or point (a) of Article 10(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with the European Data Protection Supervisor;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 24(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Article 16

Information to be provided where personal data have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller;

(b) the contact details of the data protection officer;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 48, reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following further information necessary to ensure fair and transparent processing in respect of the data subject:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or, where applicable, the right to object to processing or the right to data portability;

(c) where the processing is based on point (d) of Article 5(1) or point (a) of Article 10(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with the European Data Protection Supervisor;

(e) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

(f) the existence of automated decision-making, including profiling, referred to in Article 24(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing;

(c) obtaining or disclosure is expressly laid down by Union law, which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union law, including a statutory obligation of secrecy.

6. In the cases referred to in point (b) of paragraph 5 the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.

Article 17

Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with the European Data Protection Supervisor;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 24(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 48 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

SECTION 3

Rectification and erasure

Article 18

Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Article 19

Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (d) of Article 5(1), or point (a) of Article 10(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 23(1) and there are no overriding legitimate grounds for the processing;

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers, or controllers other than Union institutions and bodies, which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 10(2) as well as Article 10(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

Article 20

Right to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy, including the completeness, of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 23(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

4. In automated filing systems restriction of processing shall in principle be ensured by technical means. The fact that the personal data are restricted shall be indicated in the system in such a way that it becomes clear that the personal data may not be used.

Article 21

Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 18, Article 19(1) and Article 20 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 22

Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent pursuant to point (d) of Article 5(1) or point (a) of Article 10(2) or on a contract pursuant to point (c) of Article 5(1); and

(b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another or to controllers other than Union institutions and bodies, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 19. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

SECTION 4

Right to object and automated individual decision-making

Article 23

Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (a) of Article 5(1), including profiling based on that provision. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. At the latest at the time of the first communication with the data subject, the right referred to in paragraph 1 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

3. Without prejudice to Articles 36 and 37, in the context of the use of information society services the data subject may exercise his or her right to object by automated means using technical specifications.

4. Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Article 24

Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and the controller;

(b) is authorised by Union law, which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 of this Article shall not be based on special categories of personal data referred to in Article 10(1), unless point (a) or (g) of Article 10(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

SECTION 5

Restrictions

Article 25

Restrictions

1. Legal acts adopted on the basis of the Treaties or, in matters relating to the operation of the Union institutions and bodies, internal rules laid down by the latter may restrict the application of Articles 14 to 22, 35, and 36, as well as Article 4 in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

(a) the national security, public security or defence of the Member States;

(b) the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(c) other important objectives of general public interest of the Union or of a Member State, in particular the objectives of the common foreign and security policy of the Union or an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;

(d) the internal security of Union institutions and bodies, including of their electronic communications networks;

(e) the protection of judicial independence and judicial proceedings;

(f) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(g) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (c);

(h) the protection of the data subject or the rights and freedoms of others;

(i) the enforcement of civil law claims.

2. In particular, any legal act or internal rule referred to in paragraph 1 shall contain specific provisions, where relevant, as to:

(a) the purposes of the processing or categories of processing;

(b) the categories of personal data;

(c) the scope of the restrictions introduced;

(d) the safeguards to prevent abuse or unlawful access or transfer;

(e) the specification of the controller or categories of controllers;

(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing; and

(g) the risks to the rights and freedoms of data subjects.

3. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union law, which may include internal rules adopted by Union institutions and bodies in matters relating to their operation, may provide for derogations from the rights referred to in Articles 17, 18, 20 and 23 subject to the conditions and safeguards referred to in Article 13 in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where personal data are processed for archiving purposes in the public interest, Union law, which may include internal rules adopted by Union institutions and bodies in matters relating to their operation, may provide for derogations from the rights referred to in Articles 17, 18, 20, 21, 22 and 23 subject to the conditions and safeguards referred to in Article 13 in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

5. Internal rules referred to in paragraphs 1, 3 and 4 shall be clear and precise acts of general application, intended to produce legal effects vis-à-vis data subjects, adopted at the highest level of management of the Union institutions and bodies and subject to publication in the *Official Journal of the European Union*.

6. If a restriction is imposed pursuant to paragraph 1, the data subject shall be informed in accordance with Union law of the principal reasons on which the application of the restriction is based and of his or her right to lodge a complaint with the European Data Protection Supervisor.

7. If a restriction imposed pursuant to paragraph 1 is relied upon to deny access to the data subject, the European Data Protection Supervisor shall, when investigating the complaint, only inform him or her of whether the data have been processed correctly and, if not, whether any necessary corrections have been made.

8. Provision of the information referred to in paragraphs 6 and 7 of this Article and in Article 45(2) may be deferred, omitted or denied if it would cancel the effect of the restriction imposed pursuant to paragraph 1 of this Article.

CHAPTER IV

CONTROLLER AND PROCESSOR

SECTION 1

General obligations

Article 26

Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3. Adherence to approved certification mechanisms as referred to in Article 42 of Regulation (EU) 2016/679 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Article 27

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 of Regulation (EU) 2016/679 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Article 28

Joint controllers

1. Where two or more controllers or one or more controllers together with one or more controllers other than Union institutions and bodies jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with their data protection obligations, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 15 and 16, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the joint controllers are determined by Union or Member State law to which the joint controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Article 29

Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 33;

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 33 to 41 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. When a processor is not a Union institution or body, its adherence to an approved code of conduct referred to in Article 40(5) of Regulation (EU) 2016/679 or an approved certification mechanism referred to in Article 42 of Regulation (EU) 2016/679 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to any individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the processor other than a Union institution or body pursuant to Article 42 of Regulation (EU) 2016/679.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 96(2).

8. The European Data Protection Supervisor may adopt standard contractual clauses for the matters referred to in paragraphs 3 and 4.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 65 and 66, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 30

Processing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Article 31

Records of processing activities

1. Each controller shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller, the data protection officer and, where applicable, the processor and the joint controller;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in Member States, third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 33.

2. Each processor shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and of the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 33.

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. Union institutions and bodies shall make the record available to the European Data Protection Supervisor on request.

5. Unless it is not appropriate taking into account the size of the Union institution or body, Union institutions and bodies shall keep their records of processing activities in a central register. They shall make the register publicly accessible.

Article 32

Cooperation with the European Data Protection Supervisor

Union institutions and bodies shall cooperate, on request, with the European Data Protection Supervisor in the performance of his or her tasks.

SECTION 2

Security of personal data

Article 33

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, inter alia, as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union law.

4. Adherence to an approved certification mechanism as referred to in Article 42 of Regulation (EU) 2016/679 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

Article 34

Notification of a personal data breach to the European Data Protection Supervisor

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the European Data Protection Supervisor, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the European Data Protection Supervisor is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall inform the data protection officer about the personal data breach.

6. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the European Data Protection Supervisor to verify compliance with this Article.

Article 35

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 34(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the European Data Protection Supervisor, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

SECTION 3

Confidentiality of electronic communications

Article 36

Confidentiality of electronic communications

Union institutions and bodies shall ensure the confidentiality of electronic communications, in particular by securing their electronic communications networks.

Article 37

Protection of information transmitted to, stored in, related to, processed by and collected from users' terminal equipment

Union institutions and bodies shall protect the information transmitted to, stored in, related to, processed by and collected from the terminal equipment of users accessing their publicly available websites and mobile applications, in accordance with Article 5(3) of Directive 2002/58/EC.

Article 38

Directories of users

1. Personal data contained in directories of users and access to such directories shall be limited to what is strictly necessary for the specific purposes of the directory.

2. Union institutions and bodies shall take all the necessary measures to prevent personal data contained in those directories from being used for direct marketing purposes regardless of whether they are accessible to the public or not.

SECTION 4

Data protection impact assessment and prior consultation

Article 39

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 10, or of personal data relating to criminal convictions and offences referred to in Article 11; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The European Data Protection Supervisor shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.

5. The European Data Protection Supervisor may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5 of this Article, the European Data Protection Supervisor shall request that the European Data Protection Board set up by Article 68 of Regulation (EU) 2016/679 examine such lists in accordance with point (e) of Article 70(1) of that Regulation where they refer to processing operations by a controller acting jointly with one or more controllers other than Union institutions and bodies.

7. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 of the Regulation (EU) 2016/679 by the relevant processors other than Union institutions and bodies shall be taken into due account in assessing the impact of the processing operations performed by such processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of public interests or the security of processing operations.

10. Where processing pursuant to point (a) or (b) of Article 5(1) has a legal basis in a legal act adopted on the basis of the Treaties, which regulates the specific processing operation or set of operations in question, and where a data protection impact assessment has already been carried out as part of a general impact assessment preceding the adoption of that legal act, paragraphs 1 to 6 of this Article shall not apply unless that legal act provides otherwise.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Article 40

Prior consultation

1. The controller shall consult the European Data Protection Supervisor prior to processing where a data protection impact assessment under Article 39 indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in view of the available technologies and costs of implementation. The controller shall seek the advice of the data protection officer on the need for prior consultation.

2. Where the European Data Protection Supervisor is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the European Data Protection Supervisor shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of his or her powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The European Data Protection Supervisor shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the European Data Protection Supervisor has obtained information it has requested for the purposes of the consultation.

3. When consulting the European Data Protection Supervisor pursuant to paragraph 1, the controller shall provide the European Data Protection Supervisor with:

(a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing;

(b) the purposes and means of the intended processing;

(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

(d) the contact details of the data protection officer;

(e) the data protection impact assessment provided for in Article 39; and

(f) any other information requested by the European Data Protection Supervisor.

4. The Commission may, by means of an implementing act, determine a list of cases in which the controllers shall consult with, and obtain prior authorisation from, the European Data Protection Supervisor in relation to processing of personal data for the performance of a task carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health.

SECTION 5

Information and legislative consultation

Article 41

Information and consultation

1. The Union institutions and bodies shall inform the European Data Protection Supervisor when drawing up administrative measures and internal rules relating to the processing of personal data by a Union institution or body, whether alone or jointly with others.

2. The Union institutions and bodies shall consult the European Data Protection Supervisor when drawing up the internal rules referred to in Article 25.

Article 42

Legislative consultation

1. The Commission shall, following the adoption of proposals for a legislative act, of recommendations or of proposals to the Council pursuant to Article 218 TFEU or when preparing delegated acts or implementing acts, consult the European Data Protection Supervisor where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data.

2. Where an act referred to in paragraph 1 is of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data, the Commission may also consult the European Data Protection Board. In such cases the European Data Protection Supervisor and the European Data Protection Board shall coordinate their work with a view to issuing a joint opinion.

3. The advice referred to in paragraphs 1 and 2 shall be provided in writing within a period of up to eight weeks of receipt of the request for consultation referred to in paragraphs 1 and 2. In urgent cases, or if otherwise appropriate, the Commission may shorten the deadline.

4. This Article shall not apply where the Commission is required, pursuant to Regulation (EU) 2016/679, to consult the European Data Protection Board.

SECTION 6

Data protection officer

Article 43

Designation of the data protection officer

1. Each Union institution or body shall designate a data protection officer.

2. Union institutions and bodies may designate a single data protection officer for several of them, taking into account their organisational structure and size.

3. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 45.

4. The data protection officer shall be a staff member of the Union institution or body. Taking into account their size and if the option under paragraph 2 is not exercised, Union institutions and bodies may designate a data protection officer who fulfils his or her tasks on the basis of a service contract.

5. The Union institutions and bodies shall publish the contact details of the data protection officer and communicate them to the European Data Protection Supervisor.

Article 44

Position of the data protection officer

1. The Union institutions and bodies shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The Union institutions and bodies shall support the data protection officer in performing the tasks referred to in Article 45 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The Union institutions and bodies shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his or her tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer and his or her staff shall be bound by secrecy or confidentiality concerning the performance of their tasks, in accordance with Union law.

6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

7. The data protection officer may be consulted by the controller and the processor, by the staff committee concerned and by any individual on any matter concerning the interpretation or application of this Regulation, without them going through the official channels. No one shall suffer prejudice on account of a matter brought to the attention of the competent data protection officer alleging that a breach of the provisions of this Regulation has taken place.

8. The data protection officer shall be designated for a term of three to five years and shall be eligible for reappointment. The data protection officer may be dismissed from the post by the Union institution or body which designated him or her if he or she no longer fulfils the conditions required for the performance of his or her duties and only with the consent of the European Data Protection Supervisor.

9. After his or her designation the data protection officer shall be registered with the European Data Protection Supervisor by the Union institution or body which designated him or her.

Article 45

Tasks of the data protection officer

1. The data protection officer shall have the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union data protection provisions;

(b) to ensure in an independent manner the internal application of this Regulation; to monitor compliance with this Regulation, with other applicable Union law containing data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the raising of awareness and training of staff involved in processing operations, and the related audits;

(c) to ensure that data subjects are informed of their rights and obligations pursuant to this Regulation;

(d) to provide advice where requested as regards the necessity for a notification or a communication of a personal data breach pursuant to Articles 34 and 35;

(e) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 39 and to consult the European Data Protection Supervisor in case of doubt as to the need for a data protection impact assessment;

(f) to provide advice where requested as regards the need for prior consultation of the European Data Protection Supervisor pursuant to Article 40; to consult the European Data Protection Supervisor in case of doubt as to the need for a prior consultation;

(g) to respond to requests from the European Data Protection Supervisor; within the sphere of his or her competence, to cooperate and consult with the European Data Protection Supervisor at the latter's request or on his or her own initiative;

(h) to ensure that the rights and freedoms of data subjects are not adversely affected by processing operations.

2. The data protection officer may make recommendations to the controller and the processor for the practical improvement of data protection and advise them on matters concerning the application of data protection provisions. Furthermore he or she may, on his or her own initiative or at the request of the controller or the processor, the staff committee concerned or any individual, investigate matters and occurrences directly relating to his or her tasks which come to his or her notice, and report back to the person who commissioned the investigation or to the controller or the processor.

3. Further implementing rules concerning the data protection officer shall be adopted by each Union institution or body. The implementing rules shall in particular concern the tasks, duties and powers of the data protection officer.

CHAPTER V

TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Article 46

General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Article 47

Transfers on the basis of an adequacy decision

1. A transfer of personal data to a third country or international organisation may take place where the Commission has decided pursuant to Article 45(3) of Regulation (EU) 2016/679 or to Article 36(3) of Directive (EU) 2016/680 that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection and where the personal data are transferred solely to allow tasks within the competence of the controller to be carried out.

2. The Union institutions and bodies shall inform the Commission and the European Data Protection Supervisor of cases where they consider that a third country, a territory or one or more specified sectors within a third country, or an international organisation in question does not ensure an adequate level of protection within the meaning of paragraph 1.

3. The Union institutions and bodies shall take the necessary measures to comply with decisions taken by the Commission where it establishes, pursuant to Article 45(3) or (5) of Regulation (EU) 2016/679 or to Article 36(3) or (5) of Directive (EU) 2016/680, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures or no longer ensures an adequate level of protection.

Article 48

Transfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 or to Article 36(3) of Directive (EU) 2016/680, a controller or processor may transfer personal data to a third country or to an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from the European Data Protection Supervisor, by:

(a) a legally binding and enforceable instrument between public authorities or bodies;

(b) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 96(2);

(c) standard data protection clauses adopted by the European Data Protection Supervisor and approved by the Commission pursuant to the examination procedure referred to in Article 96(2);

(d) where the processor is not a Union institution or body, binding corporate rules, codes of conduct or certification mechanisms pursuant to points (b), (e) and (f) of Article 46(2) of Regulation (EU) 2016/679.

3. Subject to the authorisation from the European Data Protection Supervisor, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4. Authorisations by the European Data Protection Supervisor on the basis of Article 9(7) of Regulation (EC) No 45/2001 shall remain valid until amended, replaced or repealed, if necessary, by the European Data Protection Supervisor.

5. The Union institutions and bodies shall inform the European Data Protection Supervisor of the categories of cases in which this Article has been applied.

Article 49

Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 50

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3) of Regulation (EU) 2016/679 or to Article 36(3) of Directive (EU) 2016/680, or of appropriate safeguards pursuant to Article 48 of this Regulation, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(g) the transfer is made from a register which, according to Union law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union law for consultation are fulfilled in the particular case.

2. Points (a), (b) and (c) of paragraph 1 shall not apply to activities carried out by Union institutions and bodies in the exercise of their public powers.

3. The public interest referred to in point (d) of paragraph 1 shall be recognised in Union law.

4. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register, unless authorised by Union law. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

5. In the absence of an adequacy decision, Union law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation.

6. The Union institutions and bodies shall inform the European Data Protection Supervisor of the categories of cases in which this Article has been applied.

Article 51

International cooperation for the protection of personal data

In relation to third countries and international organisations, the European Data Protection Supervisor, in cooperation with the Commission and the European Data Protection Board, shall take appropriate steps to:

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

CHAPTER VI

EUROPEAN DATA PROTECTION SUPERVISOR

Article 52

European Data Protection Supervisor

1. The European Data Protection Supervisor is hereby established.

2. With respect to the processing of personal data, the European Data Protection Supervisor shall be responsible for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies.

3. The European Data Protection Supervisor shall be responsible for monitoring and ensuring the application of the provisions of this Regulation and of any other Union act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Union institution or body, and for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data. To those ends, the European Data Protection Supervisor shall fulfil the tasks set out in Article 57 and exercise the powers granted in Article 58.

4. Regulation (EC) No 1049/2001 shall apply to documents held by the European Data Protection Supervisor. The European Data Protection Supervisor shall adopt detailed rules for applying Regulation (EC) No 1049/2001 with regard to those documents.

Article 53

Appointment of the European Data Protection Supervisor

1. The European Parliament and the Council shall appoint the European Data Protection Supervisor by common accord for a term of five years, on the basis of a list drawn up by the Commission following a public call for candidates. The call for candidates shall enable all interested parties throughout the Union to submit their applications. The list of candidates drawn up by the Commission shall be public and shall consist of at least three candidates. On the basis of the list drawn up by the Commission, the competent committee of the European Parliament may decide to hold a hearing in order to enable it to express a preference.

2. The list of candidates referred to in paragraph 1 shall be made up of persons whose independence is beyond doubt and who are acknowledged as having expert knowledge in data protection as well as the experience and skills required to perform the duties of European Data Protection Supervisor.

3. The term of office of the European Data Protection Supervisor shall be renewable once.

4. The duties of the European Data Protection Supervisor shall cease in the following circumstances:

(a) if the European Data Protection Supervisor is replaced;

(b) if the European Data Protection Supervisor resigns;

(c) if the European Data Protection Supervisor is dismissed or required to take compulsory retirement.

5. The European Data Protection Supervisor may be dismissed or deprived of his or her right to a pension or other benefits in his or her stead by the Court of Justice at the request of the European Parliament, the Council or the Commission, if he or she no longer fulfils the conditions required for the performance of his or her duties or if he or she is guilty of serious misconduct.

6. In the event of normal replacement or voluntary resignation, the European Data Protection Supervisor shall nevertheless remain in office until he or she has been replaced.

7. Articles 11 to 14 and 17 of the Protocol on the Privileges and Immunities of the European Union shall apply to the European Data Protection Supervisor.

Article 54

Regulations and general conditions governing the performance of the European Data Protection Supervisor's duties, staff and financial resources

1. The European Data Protection Supervisor shall be considered equivalent to a judge of the Court of Justice as regards the determination of remuneration, allowances, retirement pension and any other benefit in lieu of remuneration.

2. The budgetary authority shall ensure that the European Data Protection Supervisor is provided with the human and financial resources necessary for the performance of his or her tasks.

3. The budget of the European Data Protection Supervisor shall be shown in a separate budgetary heading in the section related to administrative expenditure of the general budget of the Union.

4. The European Data Protection Supervisor shall be assisted by a secretariat. The officials and other staff members of the secretariat shall be appointed by the European Data Protection Supervisor and their superior shall be the European Data Protection Supervisor. They shall be subject exclusively to his or her direction. Their numbers shall be decided each year as part of the budgetary procedure. Article 75(2) of Regulation (EU) 2016/679 shall apply to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the European Data Protection Board by Union law.

5. The officials and the other staff members of the secretariat of the European Data Protection Supervisor shall be subject to the rules and regulations applicable to officials and other servants of the Union.

6. The seat of the European Data Protection Supervisor shall be in Brussels.

Article 55

Independence

1. The European Data Protection Supervisor shall act with complete independence in performing his or her tasks and exercising his or her powers in accordance with this Regulation.

2. The European Data Protection Supervisor shall, in the performance of his or her tasks and exercise of his or her powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

3. The European Data Protection Supervisor shall refrain from any action incompatible with his or her duties and shall not, during his or her term of office, engage in any other occupation, whether gainful or not.

4. After his or her term of office, the European Data Protection Supervisor shall behave with integrity and discretion as regards the acceptance of appointments and benefits.

Article 56

Professional secrecy

The European Data Protection Supervisor and his or her staff shall, both during and after their term of office, be subject to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties.

Article 57

Tasks

1. Without prejudice to other tasks set out under this Regulation, the European Data Protection Supervisor shall:

(a) monitor and enforce the application of this Regulation by Union institutions and bodies, with the exception of the processing of personal data by the Court of Justice acting in its judicial capacity;

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

(c) promote the awareness of controllers and processors of their obligations under this Regulation;

(d) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the national supervisory authorities to that end;

(e) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 67, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(f) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

(g) advise, on his or her own initiative or on request, all Union institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data;

(h) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;

(i) adopt standard contractual clauses referred to in Article 29(8) and in point (c) of Article 48(2);

(j) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 39 (4);

(k) participate in the activities of the European Data Protection Board;

(l) provide the secretariat for the European Data Protection Board, in accordance with Article 75 of Regulation (EU) 2016/679;

(m) give advice on the processing referred to in Article 40(2);

(n) authorise contractual clauses and provisions referred to in Article 48(3);

(o) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2);

(p) fulfil any other tasks related to the protection of personal data; and

(q) establish his or her Rules of Procedure.

2. The European Data Protection Supervisor shall facilitate the submission of complaints referred to in point (e) of paragraph 1 by a complaint submission form which can also be completed electronically, without excluding other means of communication.

3. The performance of the tasks of the European Data Protection Supervisor shall be free of charge for the data subject.

4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the European Data Protection Supervisor may refuse to act on the request. The European Data Protection Supervisor shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 58

Powers

1. The European Data Protection Supervisor shall have the following investigative powers:

(a) to order the controller and the processor to provide any information it requires for the performance of his or her tasks;

(b) to carry out investigations in the form of data protection audits;

(c) to notify the controller or the processor of an alleged infringement of this Regulation;

(d) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of his or her tasks;

(e) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union law.

2. The European Data Protection Supervisor shall have the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(c) to refer matters to the controller or processor concerned and, if necessary, to the European Parliament, the Council and the Commission;

(d) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(e) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(f) to order the controller to communicate a personal data breach to the data subject;

(g) to impose a temporary or definitive limitation including a ban on processing;

(h) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 18, 19 and 20 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 19(2) and Article 21;

(i) to impose an administrative fine pursuant to Article 66 in the case of non-compliance by a Union institution or body with one of the measures referred to in points (d) to (h) and (j) of this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a Member State, a third country or to an international organisation.

3. The European Data Protection Supervisor shall have the following authorisation and advisory powers:

(a) to advise data subjects in the exercise of their rights;

(b) to advise the controller in accordance with the prior consultation procedure referred to in Article 40, and in accordance with Article 41(2);

(c) to issue, on his or her own initiative or on request, opinions to Union institutions and bodies and to the public on any issue related to the protection of personal data;

(d) to adopt standard data protection clauses referred to in Article 29(8) and in point (c) of Article 48(2);

(e) to authorise contractual clauses referred to in point (a) of Article 48(3);

(f) to authorise administrative arrangements referred to in point (b) of Article 48(3);

(g) to authorise processing operations pursuant to implementing acts adopted under Article 40(4).

4. The European Data Protection Supervisor shall have the power to refer the matter to the Court of Justice under the conditions provided for in the Treaties and to intervene in actions brought before the Court of Justice.

5. The exercise of the powers conferred on the European Data Protection Supervisor pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedies and due process, set out in Union law.

Article 59

Obligation of controllers and processors to react to allegations

Where the European Data Protection Supervisor exercises the powers provided for in points (a), (b) and (c) of Article 58(2), the controller or processor concerned shall inform the European Data Protection Supervisor of its views within a reasonable period to be specified by the European Data Protection Supervisor, taking into account the circumstances of each case. The reply shall also include a description of the measures taken, if any, in response to the remarks of the European Data Protection Supervisor.

Article 60

Activities report

1. The European Data Protection Supervisor shall submit an annual report on his or her activities to the European Parliament, to the Council and to the Commission and at the same time make it public.

2. The European Data Protection Supervisor shall forward the report referred to in paragraph 1 to the other Union institutions and bodies, which may submit comments with a view to possible examination of the report by the European Parliament.

CHAPTER VII

COOPERATION AND CONSISTENCY

Article 61

Cooperation between the European Data Protection Supervisor and national supervisory authorities

The European Data Protection Supervisor shall cooperate with national supervisory authorities and with the joint supervisory authority established under Article 25 of Council Decision 2009/917/JHA [1] to the extent necessary for the performance of their respective duties, in particular by providing each other with relevant information, asking each other to exercise their powers and responding to each other's requests.

Article 62

Coordinated supervision by the European Data Protection Supervisor and national supervisory authorities

1. Where a Union act refers to this Article, the European Data Protection Supervisor and the national supervisory authorities, each acting within the scope of their respective competences, shall cooperate actively within the framework of their responsibilities to ensure effective supervision of large-scale IT systems and of Union bodies, offices and agencies.

2. They shall, as necessary, each acting within the scope of their respective competences and within the framework of their responsibilities, exchange relevant information, assist each other in carrying out audits and inspections, examine difficulties of interpretation or application of this Regulation and other applicable Union acts, study problems with the exercise of independent supervision or with the exercise of the rights of data subjects, draw up harmonised proposals for solutions to any problems and promote awareness of data protection rights.

3. For the purposes laid down in paragraph 2, the European Data Protection Supervisor and the national supervisory authorities shall meet at least twice a year within the framework of the European Data Protection Board. For these purposes, the European Data Protection Board may develop further working methods as necessary.

4. The European Data Protection Board shall submit a joint report of coordinated supervision activities to the European Parliament, to the Council, and to the Commission every two years.

---

[1] Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes (OJ L 323, 10.12.2009, p. 20).

CHAPTER VIII

REMEDIES, LIABILITY AND PENALTIES

Article 63

Right to lodge a complaint with the European Data Protection Supervisor

1. Without prejudice to any judicial, administrative or non-judicial remedy, every data subject shall have the right to lodge a complaint with the European Data Protection Supervisor if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The European Data Protection Supervisor shall inform the complainant of the progress and the outcome of the complaint, including of the possibility of a judicial remedy pursuant to Article 64.

3. If the European Data Protection Supervisor does not handle the complaint or does not inform the data subject within three months on the progress or outcome of the complaint, the European Data Protection Supervisor shall be deemed to have adopted a negative decision.

Article 64

Right to an effective judicial remedy

1. The Court of Justice shall have jurisdiction to hear all disputes relating to the provisions of this Regulation, including claims for damages.

2. Actions against decisions of the European Data Protection Supervisor, including decisions under Article 63(3), shall be brought before the Court of Justice.

3. The Court of Justice shall have unlimited jurisdiction to review administrative fines referred to in Article 66. It may cancel, reduce or increase those fines within the limits of Article 66.

Article 65

Right to compensation

Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the Union institution or body for the damage suffered, subject to the conditions provided for in the Treaties.

Article 66

Administrative fines

1. The European Data Protection Supervisor may impose administrative fines on Union institutions and bodies, depending on the circumstances of each individual case, where a Union institution or body fails to comply with an order by the European Data Protection Supervisor pursuant to points (d) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case, due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) any action taken by the Union institution or body to mitigate the damage suffered by data subjects;

(c) the degree of responsibility of the Union institution or body, taking into account technical and organisational measures implemented by them pursuant to Articles 27 and 33;

(d) any similar previous infringements by the Union institution or body;

(e) the degree of cooperation with the European Data Protection Supervisor in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(f) the categories of personal data affected by the infringement;

(g) the manner in which the infringement became known to the European Data Protection Supervisor, in particular whether, and if so to what extent, the Union institution or body notified the infringement;

(h) compliance with any of the measures referred to in Article 58 previously ordered against the Union institution or body concerned with regard to the same subject matter. The proceedings leading to the imposition of those fines shall be carried out in a reasonable timeframe according to the circumstances of the case and taking into account the relevant actions and proceedings referred to in Article 69.

2. Infringements of the obligations of the Union institution or body pursuant to Articles 8, 12, 27 to 35, 39, 40, 43, 44 and 45 shall, in accordance with paragraph 1 of this Article, be subject to administrative fines of up to 25 000 EUR per infringement and up to a total of 250 000 EUR per year.

3. Infringements of the following provisions by the Union institution or body shall, in accordance with paragraph 1, be subject to administrative fines of up to 50 000 EUR per infringement and up to a total of 500 000 EUR per year:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 4, 5, 7 and 10;

(b) the data subjects' rights pursuant to Articles 14 to 24;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 46 to 50.

4. If a Union institution or body, for the same or linked or continuous processing operations, infringes several provisions of this Regulation or the same provision of this Regulation several times, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

5. Before taking decisions pursuant to this Article, the European Data Protection Supervisor shall give the Union institution or body which is the subject of the proceedings conducted by the European Data Protection Supervisor the opportunity of being heard on the matters to which the European Data Protection Supervisor has taken objection. The European Data Protection Supervisor shall base his or her decisions only on objections on which the parties concerned have been able to comment. Complainants shall be associated closely with the proceedings.

6. The rights of defence of the parties concerned shall be fully respected in the proceedings. They shall be entitled to have access to the European Data Protection Supervisor's file, subject to the legitimate interest of individuals or undertakings in the protection of their personal data or business secrets.

7. Funds collected by imposition of fines in this Article shall be the income of the general budget of the Union.

Article 67

Representation of data subjects

The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with Union law or the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint with the European Data Protection Supervisor on his or her behalf, to exercise the rights referred to in Articles 63 and 64 on his or her behalf, and to exercise the right to receive compensation referred to in Article 65 on his or her behalf.

Article 68

Complaints by Union staff

Any person employed by a Union institution or body may lodge a complaint with the European Data Protection Supervisor regarding an alleged infringement of the provisions of this Regulation, including without acting through official channels. No one shall suffer prejudice by reason of having submitted a complaint with the European Data Protection Supervisor alleging such an infringement.

Article 69

Sanctions

Where an official or other servant of the Union fails to comply with the obligations laid down in this Regulation, whether intentionally or through negligence on his or her part, the official or other servant concerned shall be liable to disciplinary or other action, in accordance with the rules and procedures laid down in the Staff Regulations.

CHAPTER IX

PROCESSING OF OPERATIONAL PERSONAL DATA BY UNION BODIES, OFFICES AND AGENCIES WHEN CARRYING OUT ACTIVITIES WHICH FALL WITHIN THE SCOPE OF CHAPTER 4 OR CHAPTER 5 OF TITLE V OF PART THREE TFEU

Article 70

Scope of the Chapter

This Chapter applies only to the processing of operational personal data by Union bodies, offices and agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU, without prejudice to specific data protection rules applicable to such a Union body, office or agency.

Article 71

Principles relating to processing of operational personal data

1. Operational personal data shall be:

(a) processed lawfully and fairly ('lawfulness and fairness');

(b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes ('purpose limitation');

(c) adequate, relevant, and not excessive in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that operational personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the operational personal data are processed ('storage limitation');

(f) processed in a manner that ensures appropriate security of the operational personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. Processing by the same or another controller for any of the purposes set out in the legal act establishing the Union body, office or agency other than that for which the operational personal data are collected shall be permitted in so far as:

(a) the controller is authorised to process such operational personal data for such a purpose in accordance with Union law; and

(b) processing is necessary and proportionate to that other purpose in accordance with Union law.

3. Processing by the same or another controller may include archiving in the public interest, scientific, statistical or historical use, for the purposes set out in the legal act establishing the Union body, office or agency, subject to appropriate safeguards for the rights and freedoms of data subjects.

4. The controller shall be responsible for, and be able to demonstrate compliance with, paragraphs 1, 2 and 3.

Article 72

Lawfulness of processing of operational personal data

1. Processing of operational personal data shall be lawful only if and to the extent that processing is necessary for the performance of a task carried out by Union bodies, offices and agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU and that it is based on Union law.

2. Specific Union legal acts regulating processing within the scope of this Chapter shall specify at least the objectives of processing, the operational personal data to be processed, the purposes of the processing and the time limits for storage of the operational personal data or for periodic review of the need for further storage of the operational personal data.

Article 73

Distinction between different categories of data subjects

The controller shall, where applicable and as far as possible, make a clear distinction between the operational personal data of different categories of data subjects, such as the categories listed in the legal acts establishing Union bodies, offices and agencies.

Article 74

Distinction between operational personal data and verification of the quality of operational personal data

1. The controller shall distinguish, as far as possible, operational personal data based on facts from operational personal data based on personal assessments.

2. The controller shall take all reasonable steps to ensure that operational personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, the controller shall, as far as practicable and where relevant, verify the quality of operational personal data before they are transmitted or made available, for example by consulting the competent authority from which the data originates. As far as possible, in all transmissions of operational personal data, the controller shall add the necessary information enabling the recipient to assess the degree to which the operational personal data are accurate, complete and reliable, and the extent to which they are up to date.

3. If it emerges that incorrect operational personal data have been transmitted or that operational personal data have been unlawfully transmitted, the recipient shall be notified without delay. In such a case, the operational personal data concerned shall be rectified or erased or their processing shall be restricted in accordance with Article 82.

Article 75

Specific processing conditions

1. When Union law applicable to the transmitting controller provides for specific conditions for processing, the controller shall inform the recipient of the operational personal data of those conditions and the requirement to comply with them.

2. The controller shall comply with specific processing conditions for processing provided by a transmitting competent authority in accordance with Article 9(3) and (4) of Directive (EU) 2016/680.

Article 76

Processing of special categories of operational personal data

1. Processing of operational personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, operational personal data concerning health or concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary for operational purposes, within the mandate of the Union body, office or agency concerned and subject to appropriate safeguards for the rights and freedoms of the data subject. Discrimination against natural persons on the basis of such personal data shall be prohibited.

2. The data protection officer shall be informed without undue delay of recourse to this Article.

Article 77

Automated individual decision-making, including profiling

1. A decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her shall be prohibited unless authorised by Union law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.

2. Decisions referred to in paragraph 1 of this Article shall not be based on the special categories of personal data referred to in Article 76 unless suitable measures to safeguard the data subject's rights, freedoms and legitimate interests are in place.

3. Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 76 shall be prohibited, in accordance with Union law.

Article 78

Communication and modalities for exercising the rights of the data subject

1. The controller shall take reasonable steps to provide any information referred to in Article 79 and make any communication with regard to Articles 80 to 84 and 92 relating to processing to the data subject in a concise, intelligible and easily accessible form, using clear and plain language. The information shall be provided by any appropriate means, including by electronic means. As a general rule, the controller shall provide the information in the same form as the request.

2. The controller shall facilitate the exercise of the rights of the data subject under Articles 79 to 84.

3. The controller shall inform the data subject in writing about the follow-up to his or her request without undue delay and in any case at the latest within three months after receipt of the request by the data subject.

4. The controller shall provide the information under Article 79 and any communication made or action taken pursuant to Articles 80 to 84 and 92 free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

5. Where the controller has reasonable doubts concerning the identity of the natural person making a request referred to in Article 80 or 82, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

Article 79

Information to be made available or given to the data subject

1. The controller shall make available to the data subject at least the following information:

(a) the identity and the contact details of the Union body, office or agency;

(b) the contact details of the data protection officer;

(c) the purposes of the processing for which the operational personal data are intended;

(d) the right to lodge a complaint with the European Data Protection Supervisor and his or her contact details;

(e) the existence of the right to request from the controller access to and rectification or erasure of operational personal data and restriction of processing of the operational personal data concerning the data subject.

2. In addition to the information referred to in paragraph 1, the controller shall give to the data subject, in the specific cases foreseen by Union law, the following further information to enable the exercise of his or her rights:

(a) the legal basis for the processing;

(b) the period for which the operational personal data will be stored, or, where that is not possible, the criteria used to determine that period;

(c) where applicable, the categories of recipients of the operational personal data, including in third countries or international organisations;

(d) where necessary, further information, in particular where the operational personal data are collected without the knowledge of the data subject.

3. The controller may delay, restrict or omit the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to:

(a) avoid obstructing official or legal inquiries, investigations or procedures;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect the public security of Member States;

(d) protect the national security of Member States;

(e) protect the rights and freedoms of others, such as victims and witnesses.

Article 80

Right of access by the data subject

The data subject shall have the right to obtain from the controller confirmation as to whether or not operational personal data concerning him or her are processed, and where that is the case, have the right to access operational personal data and the following information:

(a) the purposes of and legal basis for the processing;

(b) the categories of operational personal data concerned;

(c) the recipients or categories of recipients to whom the operational personal data have been disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the operational personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of operational personal data or restriction of processing of operational personal data concerning the data subject;

(f) the right to lodge a complaint with the European Data Protection Supervisor and his or her contact details;

(g) communication of the operational personal data undergoing processing and of any available information as to their origin.

Article 81

Limitations to the right of access

1. The controller may restrict, wholly or partly, the data subject's right of access to the extent that, and for as long as, such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to:

(a) avoid obstructing official or legal inquiries, investigations or procedures;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect the public security of Member States;

(d) protect the national security of Member States;

(e) protect the rights and freedoms of others, such as victims and witnesses.

2. In the cases referred to in paragraph 1, the controller shall inform the data subject, without undue delay, in writing of any refusal or restriction of access and of the reasons for the refusal or the restriction. Such information may be omitted where the provision thereof would undermine a purpose under paragraph 1. The controller shall inform the data subject of the possibility of lodging a complaint with the European Data Protection Supervisor or of seeking a judicial remedy before the Court of Justice. The controller shall document the factual or legal reasons on which the decision is based. That information shall be made available to the European Data Protection Supervisor on request.

Article 82

Right to rectification or erasure of operational personal data and restriction of processing

1. Any data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate operational personal data relating to him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete operational personal data completed, including by means of providing a supplementary statement.

2. The controller shall erase operational personal data without undue delay and the data subject shall have the right to obtain from the controller the erasure of operational personal data concerning him or her without undue delay where processing infringes Articles 71, 72(1) or 76, or where operational personal data must be erased in order to comply with a legal obligation to which the controller is subject.

3. Instead of erasure, the controller shall restrict processing where:

(a) the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained; or

(b) the personal data must be maintained for the purposes of evidence.

Where processing is restricted pursuant to point (a) of the first subparagraph, the controller shall inform the data subject before lifting the restriction of processing.

Restricted data shall be processed only for the purpose that prevented their erasure.

4. The controller shall inform the data subject in writing of any refusal of rectification or erasure of operational personal data or restrict processing and of the reasons for the refusal. The controller may restrict, wholly or partly, the provision of such information to the extent that such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned in order to:

(a) avoid obstructing official or legal inquiries, investigations or procedures;

(b) avoid prejudicing the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

(c) protect the public security of Member States;

(d) protect the national security of Member States;

(e) protect the rights and freedoms of others, such as victims and witnesses.

The controller shall inform the data subject of the possibility of lodging a complaint with the European Data Protection Supervisor or seeking a judicial remedy from the Court of Justice.

5. The controller shall communicate the rectification of inaccurate operational personal data to the competent authority from which the inaccurate operational personal data originate.

6. The controller shall, where operational personal data has been rectified or erased or processing has been restricted pursuant to paragraphs 1, 2 or 3, notify the recipients and inform them that they have to rectify or erase the operational personal data or restrict processing of the operational personal data under their responsibility.

Article 83

Right of access in criminal investigations and proceedings

Where operational personal data originates from a competent authority, Union bodies, offices and agencies shall, prior to deciding on a data subject's right of access, verify with the competent authority concerned whether such personal data are contained in a judicial decision or record or a case file processed in the course of criminal investigations and proceedings in the Member State of that competent authority. Where this is the case, a decision on the right of access shall be taken in consultation and in close cooperation with the competent authority concerned.

Article 84

Exercise of rights by the data subject and verification by the European Data Protection Supervisor

1. In the cases referred to in Articles 79(3), 81 and 82(4), the rights of the data subject may also be exercised through the European Data Protection Supervisor.

2. The controller shall inform the data subject of the possibility of exercising his or her rights through the European Data Protection Supervisor pursuant to paragraph 1.

3. Where the right referred to in paragraph 1 is exercised, the European Data Protection Supervisor shall at least inform the data subject that all necessary verifications or a review by him or her have taken place. The European Data Protection Supervisor shall also inform the data subject of his or her right to seek a judicial remedy before the Court of Justice.

Article 85

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing, in order to meet the requirements of this Regulation and the legal act establishing it, and protect the rights of the data subjects.

2. The controller shall implement appropriate technical and organisational measures ensuring that, by default, only operational personal data which are adequate, relevant and not excessive in relation to the purpose of the processing are processed. That obligation applies to the amount of operational personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default operational personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Article 86

Joint controllers

1. Where two or more controllers or one or more controllers together with one or more controllers other than Union institutions and bodies jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with their data protection obligations, in particular as regards the exercise of the rights of the data subject and their respective duties to provide the information referred to in Article 79, by means of an arrangement between them, unless and in so far as the respective responsibilities of the joint controllers are determined by Union or Member State law to which the joint controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subject. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Article 87

Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and the legal act establishing the controller and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation by the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of operational personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) acts only on instructions from the controller;

(b) ensures that persons authorised to process the operational personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) assists the controller by any appropriate means to ensure compliance with the provisions on the data subject's rights;

(d) at the choice of the controller, deletes or returns all the operational personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union law or Member State law requires storage of the operational personal data;

(e) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article;

(f) complies with the conditions referred to in paragraph 2 and in this paragraph for engaging another processor.

4. The contract or the other legal act referred to in paragraph 3 shall be in writing, including in electronic form.

5. If a processor infringes this Regulation or the legal act establishing the controller by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 88

Logging

1. The controller shall keep logs for any of the following processing operations in automated processing systems: the collection, alteration, access, consultation, disclosure, including transfers, combination and erasure of operational personal data. The logs of consultation and disclosure shall make it possible to establish the justification for, and the date and time of, such operations, the identification of the person who consulted or disclosed operational personal data, and, as far as possible, the identity of the recipients of such operational personal data.

2. The logs shall be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the operational personal data, and for criminal proceedings. Such logs shall be deleted after three years, unless they are required for ongoing control.

3. The controller shall make the logs available to its data protection officer and to the European Data Protection Supervisor on request.

Article 89

Data protection impact assessment

1. Where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of operational personal data.

2. The assessment referred to in paragraph 1 shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of operational personal data and to demonstrate compliance with data protection rules, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

Article 90

Prior consultation of the European Data Protection Supervisor

1. The controller shall consult the European Data Protection Supervisor prior to processing which will form part of a new filing system to be created, where:

(a) a data protection impact assessment under Article 89 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk; or

(b) the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects.

2. The European Data Protection Supervisor may establish a list of the processing operations which are subject to prior consultation pursuant to paragraph 1.

3. The controller shall provide the European Data Protection Supervisor with the data protection impact assessment referred to Article 89 and, on request, with any other information to allow the European Data Protection Supervisor to make an assessment of the compliance of the processing and in particular of the risks for the protection of operational personal data of the data subject and of the related safeguards.

4. Where the European Data Protection Supervisor is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation or the legal act establishing the Union body, office or agency, in particular where the controller has insufficiently identified or mitigated the risk, the European Data Protection Supervisor shall provide written advice to the controller within a period of up to six weeks of receipt of the request for consultation. That period may be extended by a month, taking into account the complexity of the intended processing. The European Data Protection Supervisor shall inform the controller of any such extension within one month of receipt of the request for consultation, together with the reasons for the delay.

Article 91

Security of processing of operational personal data

1. The controller and the processor shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks, in particular as regards the processing of special categories of operational personal data.

2. In respect of automated processing, the controller and the processor shall, following an evaluation of the risks, implement measures designed to:

(a) deny unauthorised persons access to data processing equipment used for processing ('equipment access control');

(b) prevent the unauthorised reading, copying, modification or removal of data media ('data media control');

(c) prevent the unauthorised input of operational personal data and the unauthorised inspection, modification or deletion of stored operational personal data ('storage control');

(d) prevent the use of automated processing systems by unauthorised persons using data communication equipment ('user control');

(e) ensure that persons authorised to use an automated processing system have access only to the operational personal data covered by their access authorisation ('data access control');

(f) ensure that it is possible to verify and establish the bodies to which operational personal data have been or may be transmitted or made available using data communication ('communication control');

(g) ensure that it is subsequently possible to verify and establish which operational personal data have been input into automated data processing systems, and when and by whom the operational personal data were input ('input control');

(h) prevent unauthorised reading, copying, modification or deletion of operational personal data during transfers of operational personal data or during transportation of data media ('transport control');

(i) ensure that installed systems may, in the case of interruption, be restored ('recovery');

(j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored operational personal data cannot be corrupted by means of a malfunctioning of the system ('integrity').

Article 92

Notification of a personal data breach to the European Data Protection Supervisor

1. In the case of a personal data breach, the controller shall notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach to the European Data Protection Supervisor, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the European Data Protection Supervisor is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of operational personal data records concerned;

(b) communicate the name and contact details of the Data Protection Officer;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

3. Where, and in so far as, it is not possible to provide the information referred to in paragraph 2 at the same time, the information may be provided in phases without undue further delay.

4. The controller shall document any personal data breaches referred to in paragraph 1, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the European Data Protection Supervisor to verify compliance with this Article.

5. Where the personal data breach involves operational personal data that have been transmitted by or to the competent authorities, the controller shall communicate the information referred to in paragraph 2 to the competent authorities concerned without undue delay.

Article 93

Communication of a personal data breach to the data subject

1. Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and shall contain at least the information and the recommendations provided for in points (b), (c) and (d) of Article 92(2).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technological and organisational protection measures, and those measures were applied to the operational personal data affected by the personal data breach, in particular those that render the operational personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve a disproportionate effort. In such a case, there shall instead be a public communication or a similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the European Data Protection Supervisor, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so, or may decide that any of the conditions referred to in paragraph 3 are met.

5. The communication to the data subject referred to in paragraph 1 of this Article may be delayed, restricted or omitted subject to the conditions and on the grounds referred to in Article 79(3).

Article 94

Transfer of operational personal data to third countries and international organisations

1. Subject to restrictions and conditions laid down in the legal acts establishing the Union body, office or agency, the controller may transfer operational personal data to an authority of a third country or to an international organisation insofar as such transfer is necessary for the performance of controller's tasks and only where the conditions laid down in this Article are met, namely:

(a) the Commission has adopted an adequacy decision in accordance with Article 36(3) of Directive (EU) 2016/680, finding that the third country or a territory or a processing sector within that third country or the international organisation in question ensures an adequate level of protection;

(b) in the absence of a Commission adequacy decision under point (a), an international agreement has been concluded between the Union and that third country or international organisation pursuant to Article 218 TFEU adducing adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals;

(c) in the absence of a Commission adequacy decision under point (a) or an international agreement under point (b), a cooperation agreement has been concluded allowing for the exchange of operational personal data before the date of application of the legal act establishing the Union body, office or agency concerned, between that Union body, office or agency and the third country in question.

2. The legal acts establishing the Union bodies, offices and agencies may maintain or introduce more specific provisions on the conditions for international transfers of operational personal data, in particular on the transfers by way of appropriate safeguards and derogations for specific situations..

3. The controller shall publish on its website and keep up to date a list of adequacy decisions referred to in point (a) of paragraph 1, agreements, administrative arrangements and other instruments relating to the transfer of operational personal data in accordance with paragraph 1.

4. The controller shall keep detailed records of all transfers made pursuant to this Article.

Article 95

Secrecy of judicial inquiries and criminal proceedings

The legal acts establishing the Union bodies, offices or agencies carrying out the activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU may oblige the European Data Protection Supervisor, in the exercise of his or her supervision powers, to take utmost account of the secrecy of judicial inquiries and criminal proceedings, in accordance with Union or Member State law.

CHAPTER X

IMPLEMENTING ACTS

Article 96

Committee procedure

1. The Commission shall be assisted by the committee established by Article 93 of Regulation (EU) 2016/679. 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.

CHAPTER XI

REVIEW

Article 97

Review clause

No later than 30 April 2022, and every five years thereafter, the Commission shall present to the European Parliament and to the Council a report on the application of this Regulation, accompanied, if necessary, by appropriate legislative proposals.

Article 98

Review of Union legal acts

1. By 30 April 2022, the Commission shall review legal acts adopted on the basis of the Treaties which regulate the processing of operational personal data by Union bodies, offices or agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU, in order to:

(a) assess their consistency with Directive (EU) 2016/680 and Chapter IX of this Regulation;

(b) identify any divergences that may hamper the exchange of operational personal data between Union bodies, offices or agencies when carrying out activities in those fields and competent authorities; and

(c) identify any divergences that may create legal fragmentation of the data protection legislation in the Union.

2. On the basis of the review, in order to ensure uniform and consistent protection of natural persons with regard to processing, the Commission may submit appropriate legislative proposals, in particular with a view to applying Chapter IX of this Regulation to Europol and the European Public Prosecutor's Office and including adaptations of Chapter IX of this Regulation, if necessary.

CHAPTER XII

FINAL PROVISIONS

Article 99

Repeal of Regulation (EC) No 45/2001 and of Decision No 1247/2002/EC

Regulation (EC) No 45/2001 and Decision No 1247/2002/EC are repealed with effect from 11 December 2018. References to the repealed Regulation and Decision shall be construed as references to this Regulation.

Article 100

Transitional measures

1. The Decision 2014/886/EU of the European Parliament and of the Council [1] and the current terms of office of the European Data Protection Supervisor and the Assistant Supervisor shall not be affected by this Regulation.

---

[1] Decision 2014/886/EU of the European Parliament and of the Council of 4 December 2014 appointing the European Data Protection Supervisor and the Assistant Supervisor (OJ L 351, 9.12.2014, p. 9).

2. The Assistant Supervisor shall be considered equivalent to the Registrar of the Court of Justice as regards the determination of remuneration, allowances, retirement pension and any other benefit in lieu of remuneration.

3. Article 53(4), (5) and (7), and Articles 55 and 56 of this Regulation shall apply to the current Assistant Supervisor until the end of his term of office.

4. The Assistant Supervisor shall assist the European Data Protection Supervisor in fulfilling the latter's duties and act as a replacement when the European Data Protection Supervisor is absent or prevented from attending to those duties until the end of the current Assistant Supervisor's term of office.

Article 101

Entry into force and application

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. However, this Regulation shall apply to processing of personal data by Eurojust from 12 December 2019.

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

Done at Strasbourg, 23 October 2018.

For the European Parliament	*For the Council*
The President	*The President*
A. TAJANI	K. EDTSTADLER

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

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 74, Article 77(2)(a) and (b), Article 78(2)(e), Article 79(2)(c), Article 82(1)(d), Article 85(1), Article 87(2)(a) and Article 88(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) The Schengen Information System (SIS II) was established by Regulation (EC) No 1987/2006 of the European Parliament and of the Council ([2]) and by Council Decision 2007/533/JHA ([3]). Regulation (EC) No 1987/2006 and Decision 2007/533/JHA provide that the Commission is to be responsible, during a transitional period, for the operational management of the central system of SIS II (Central SIS II). After that transitional period, a Management Authority is to be responsible for the operational management of Central SIS II and certain aspects of the communication infrastructure.

(2) The Visa Information System (VIS) was established by Council Decision 2004/512/EC ([4]). Regulation (EC) No 767/2008 of the European Parliament and of the Council ([5]) provides that the Commission is to be responsible, during a transitional period, for the operational management of the VIS. After that transitional period, a Management Authority is to be responsible for the operational management of the central VIS and of the national interfaces and for certain aspects of the communication infrastructure.

([1]) Position of the European Parliament of 5 July 2018 (not yet published in the Official Journal) and Decision of the Council of 9 November 2018.

([2]) Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 381, 28.12.2006, p. 4).

([3]) Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63).

([4]) Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS) (OJ L 213, 15.6.2004, p. 5).

([5]) Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) (OJ L 218, 13.8.2008, p. 60).

(3) Eurodac was established by Council Regulation (EC) No 2725/2000 ([1]). Council Regulation (EC) No 407/2002 ([2]) laid down necessary implementing rules. Those legal acts were repealed and replaced by Regulation (EU) No 603/2013 of the European Parliament and of the Council ([3]) with effect from 20 July 2015.

(4) The European Agency for the operational management of large-scale IT (information technology) systems in the area of freedom, security and justice, commonly referred to as eu-LISA, was established by Regulation (EU) No 1077/2011 of the European Parliament and of the Council ([4]) in order to ensure the operational management of SIS, the VIS and Eurodac and of certain aspects of their communication infrastructures and potentially that of other large-scale IT systems in the area of freedom, security and justice, subject to the adoption of separate Union legal acts. Regulation (EU) No 1077/2011 was amended by Regulation (EU) No 603/2013 in order to reflect the changes introduced to Eurodac.

(5) Since the Management Authority required legal, administrative and financial autonomy, it was established in the form of a regulatory agency (the 'Agency') with legal personality. As was agreed, the seat of the Agency was established in Tallinn, Estonia. However, since the tasks relating to the technical development and the preparation for the operational management of SIS II and the VIS were already being carried out in Strasbourg, France, and a backup site for those systems had been installed in Sankt Johann im Pongau, Austria, in line also with the locations of SIS II and the VIS as established under the relevant Union legal acts, this should continue to be the case. Those two sites should also continue to be the locations, respectively, where the tasks relating to operational management of Eurodac are carried out and where a backup site for Eurodac is established. Those two sites should also be the locations, respectively, for the technical development and operational management of other large-scale IT systems in the area of freedom, security and justice and for a backup site capable of ensuring the operation of a large-scale IT system in the event of failure of that large-scale IT system. In order to maximise the possible use of the backup site, that site could also be used to operate systems simultaneously provided that it remains capable of ensuring their operation in the event of failure of one or more of the systems. Due to the high-security, high-availability and mission-critical nature of the systems, if the hosting capacity of the existing technical sites becomes insufficient, it should be possible for the Agency's Management Board (the Management Board), where justified on the basis of an independent impact assessment and cost-benefit analysis, to propose the establishment of a second separate technical site either in Strasbourg or in Sankt Johann im Pongau or in both locations, as required, in order to host the systems. The Management Board should consult the Commission and take its views into account before notifying the European Parliament and the Council (the 'budgetary authority') of its intention to implement any project related to property.

(6) Since taking up its responsibilities on 1 December 2012, the Agency took over the tasks conferred on the Management Authority in relation to the VIS by Regulation (EC) No 767/2008 and Council Decision 2008/633/JHA ([5]). In April 2013, the Agency also took over the tasks conferred on the Management Authority in relation to SIS II by Regulation (EC) No 1987/2006 and Decision 2007/533/JHA after SIS II went live and, in June 2013, it took over the tasks conferred on the Commission in relation to Eurodac in accordance with Regulations (EC) No 2725/2000 and (EC) No 407/2002.

(7) The first evaluation of the Agency's work, based on an independent external evaluation and carried out in the period 2015-2016 concluded that the Agency effectively ensures the operational management of the large-scale IT systems and other tasks entrusted to it but also that a number of changes to Regulation (EU) No 1077/2011 are necessary such as the transfer to the Agency of the communication infrastructure tasks retained by the Commission. Building

([1]) Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention (OJ L 316, 15.12.2000, p. 1).

([2]) Council Regulation (EC) No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention (OJ L 62, 5.3.2002, p. 1).

([3]) Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 180, 29.6.2013, p. 1).

([4]) Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 286, 1.11.2011, p. 1).

([5]) Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (OJ L 218, 13.8.2008, p. 129).

on that external evaluation, the Commission took into account policy, legal and factual developments and proposed, in particular in its report of 29 June 2017 on the functioning of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) (the evaluation report), that the mandate of the Agency be extended to carry out the tasks deriving from the adoption by the co-legislators of legislative proposals entrusting new systems to the Agency and the tasks referred to in the Commission's Communication of 6 April 2016 entitled 'Stronger and Smarter Information Systems for Borders and Security', in the High-Level Expert Group on Information Systems and Interoperability's final report of 11 May 2017 and in the Commission's Communication of 16 May 2017 entitled 'Seventh progress report towards an effective and genuine Security Union', subject to the adoption of the relevant Union legal acts, where required. In particular, the Agency should be tasked with the development of solutions regarding interoperability defined in the Communication of 6 April 2016 as the ability of information systems to exchange data and to enable the sharing of information.

Where relevant, any actions carried out with regard to interoperability should be guided by the Commission's Communication of 23 March 2017 entitled 'European Interoperability Framework — Implementation Strategy'. Annex 2 of that Communication provides the general guidelines, recommendations and best practices for achieving interoperability or for, at least, creating the environment to achieve better interoperability when designing, implementing and managing European public services.

(8) The evaluation report also concluded that the Agency's mandate should be extended to enable it to provide Member States with advice with regard to the connection of national systems to the central systems of the large-scale IT systems it manages (the 'systems') and with ad hoc assistance and support, where requested, and to provide the Commission services with assistance and support on technical issues related to new systems.

(9) The Agency should be entrusted with the preparation, development and operational management of the Entry/Exit System (EES), established by Regulation (EU) 2017/2226 of the European Parliament and of the Council ([1]).

(10) The Agency should also be entrusted with the operational management of DubliNet, a separate secure electronic transmission channel set up under Article 18 of Commission Regulation (EC) No 1560/2003 ([2]), which Member States' competent asylum authorities should use for the exchange of information on applicants for international protection.

(11) The Agency should further be entrusted with the preparation, development and operational management of the European Travel Information and Authorisation System (ETIAS), established by Regulation (EU) 2018/1240 of the European Parliament and of the Council ([3]).

(12) The core function of the Agency should continue to be the fulfilment of the operational management tasks for SIS II, the VIS, Eurodac, the EES, DubliNet, ETIAS and, if so decided, other large-scale IT systems in the area of freedom, security and justice. The Agency should also be responsible for technical measures required as a result of the non-normative tasks with which it is entrusted. Those responsibilities should be without prejudice to the normative tasks reserved for the Commission alone or for the Commission assisted by a Committee in the respective Union legal acts governing the systems.

(13) The Agency should be able to implement technical solutions in order to comply with the availability requirements laid down in the Union legal acts governing the systems, while fully respecting the specific provisions of those acts with regard to the technical architecture of the respective systems. Where those technical solutions require a duplication of a system or a duplication of components of a system, an independent impact assessment and cost-benefit analysis should be carried out and a decision should be taken by the Management Board following the

([1]) Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (OJ L 327, 9.12.2017, p. 20).

([2]) Commission Regulation (EC) No 1560/2003 of 2 September 2003 laying down detailed rules for the application of Council Regulation (EC) No 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national (OJ L 222, 5.9.2003, p. 3).

([3]) Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).

consultation of the Commission. That impact assessment should also include an examination of the hosting capacity needs of the existing technical sites related to the development of such technical solutions and the possible risks related to the current operational set up.

(14) It is no longer justified for the Commission to retain certain tasks related to the communication infrastructure of the systems and those tasks should therefore be transferred to the Agency in order to improve the coherence of the management of the communication infrastructure. However, for those systems that use EuroDomain, a secured communication infrastructure provided by TESTA-ng (Trans-European Services for Telematics between Administrations-new generation) and set up as part of the ISA Programme that was established by Decision No 922/2009/EC of the European Parliament and of the Council ([1]) and continued as part of the ISA2 Programme that was established by Decision (EU) 2015/2240 of the European Parliament and of the Council ([2]), the tasks in relation to the implementation of the budget, acquisition and renewal and contractual matters should be retained by the Commission.

(15) The Agency should be able to entrust tasks relating to the delivery, setting up, maintenance and monitoring of the communication infrastructure to external private-sector entities or bodies in accordance with Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council ([3]). The Agency should have sufficient budgetary and staff resources at its disposal in order to limit as much as possible the need to outsource its tasks and duties to external private-sector entities or bodies.

(16) The Agency should continue to perform tasks relating to training on the technical use of SIS II, the VIS and Eurodac and other systems entrusted to it in the future.

(17) In order to contribute to evidence-based Union migration and security policy-making and to the monitoring of the proper functioning of the systems, the Agency should compile and publish statistics and produce statistical reports and make them available to relevant actors in accordance with the Union legal acts governing the systems, for example in order to monitor the implementation of Council Regulation (EU) No 1053/2013 ([4]) and for the purposes of carrying out risk analysis and vulnerability assessment in accordance with Regulation (EU) 2016/1624 of the European Parliament and of the Council ([5]).

(18) It should be possible to make the Agency responsible for the preparation, development and operational management of additional large-scale IT systems pursuant to Articles 67 to 89 of the Treaty on the Functioning of the European Union (TFEU). Possible examples of such systems could be the centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons to supplement and support the European Criminal Records Information System (ECRIS-TCN system) or the computerised system for cross-border communication in civil and criminal proceedings (e-CODEX). However, the Agency should be entrusted with such systems only by means of subsequent and separate Union legal acts, preceded by an impact assessment.

(19) The mandate of the Agency with regard to research should be extended in order to increase its ability to be more proactive in suggesting relevant and necessary technical changes to the systems. The Agency should not only be able to monitor research activities relevant to the operational management of the systems but also be able to contribute to the implementation of relevant parts of the European Union Framework Programme for Research and Innovation, where the Commission delegates the relevant powers to the Agency. At least once a year, the Agency should provide information on such monitoring to the European Parliament, to the Council and, where the processing of personal data is concerned, to the European Data Protection Supervisor.

([1]) Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European Public Administrations (ISA) (OJ L 280, 3.10.2009, p. 20).

([2]) Decision (EU) 2015/2240 of the European Parliament and of the Council of 25 November 2015 establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA2 programme) as a means for modernising the public sector (OJ L 318, 4.12.2015, p. 1).

([3]) 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).

([4]) Council Regulation (EU) No 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen *acquis* and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen (OJ L 295, 6.11.2013, p. 27).

([5]) Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC (OJ L 251, 16.9.2016, p. 1).

(20) It should be possible for the Commission to entrust the Agency with responsibility for carrying out pilot projects of an experimental nature designed to test the feasibility of an action and its usefulness, which may be implemented without a basic act in accordance with Regulation (EU, Euratom) 2018/1046. In addition, it should be possible for the Commission to entrust the Agency with budget implementation tasks for proofs of concept funded under the instrument for financial support for external borders and visa established by Regulation (EU) No 515/2014 of the European Parliament and of the Council ([1]) in accordance with Regulation (EU, Euratom) 2018/1046, after informing the European Parliament. It should also be possible for the Agency to plan and implement testing activities on matters strictly covered by this Regulation and the Union legal acts governing the development, establishment, operation and use of the systems, such as testing virtualisation concepts. When tasked with carrying out a pilot project, the Agency should pay particular attention to the European Union Information Management Strategy.

(21) The Agency should, as regards the connection of national systems to the central systems provided for in the Union legal acts governing the systems, provide advice to Member States at their request.

(22) The Agency should also provide ad hoc support to Member States at their request, subject to the procedure set out in this Regulation, where required by extraordinary security or migratory challenges or needs. In particular, a Member State should be able to request and rely on operational and technical reinforcement where that Member State faces specific and disproportionate migratory challenges at particular areas of its external borders characterised by large inward migratory flows. Such reinforcement should be provided in hotspot areas by migration management support teams composed of experts from relevant Union agencies. Where the support of the Agency is required in this context with regard to issues related to the systems, the Member State concerned should transmit a request for support to the Commission, which, following its assessment that such support is effectively justified, should transmit the request for support without delay to the Agency. The Agency should, inform the Management Board of such requests. The Commission should also monitor whether the Agency provides a timely response to the request for ad hoc support. The Agency's annual activity report should report in detail on the actions the Agency has carried out to provide ad hoc support to Member States and on the costs incurred in that respect.

(23) The Agency should also support the Commission services on technical issues related to existing or new systems, where requested, in particular for the preparation of new proposals on large-scale IT systems to be entrusted to the Agency.

(24) It should be possible for a group of Member States to entrust the Agency with the development, management or hosting of a common IT component in order to assist them with the implementation of technical aspects of obligations deriving from Union legal acts regarding decentralised IT systems in the area of freedom, security and justice. This should be without prejudice to the obligations of those Member States under the applicable Union legal acts, in particular with regard to the architecture of those systems. This should require prior approval by the Commission, be subject to a positive decision of the Management Board, be reflected in a delegation agreement between the Member States concerned and the Agency and be financed fully by the Member States concerned. The Agency should inform the European Parliament and the Council of the approved delegation agreement and of any modifications thereto. Other Member States should be able to participate in such common IT solutions provided that this possibility is provided for in the delegation agreement and that the necessary amendments are made thereto. This task should not adversely affect the Agency's operational management of the systems.

(25) Entrusting the Agency with the operational management of large-scale IT systems in the area of freedom, security and justice should not affect the specific rules applicable to those systems. In particular, the specific rules governing the purpose, access rights, security measures and further data protection requirements for each such system are fully applicable.

(26) In order to monitor effectively the functioning of the Agency, the Member States and the Commission should be represented on the Management Board. The Management Board should be entrusted with the necessary functions, in particular to adopt the annual work programme, to carry out its functions relating to the Agency's budget, to adopt the financial rules applicable to the Agency and to establish procedures for taking decisions relating to the operational tasks of the Agency by the Executive Director. The Management Board should carry out those tasks in an

([1]) Regulation (EU) No 515/2014 of the European Parliament and of the Council of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for external borders and visa and repealing Decision No 574/2007/EC (OJ L 150, 20.5.2014, p. 143).

efficient and transparent way. Following the organisation of an appropriate selection procedure by the Commission, and following a hearing of the proposed candidates in the competent committee or committees of the European Parliament, the Management Board should also appoint an Executive Director.

(27) Considering that the number of large-scale IT systems entrusted to the Agency will have increased significantly by 2020 and that the tasks of the Agency are being considerably enhanced, there will be a corresponding large increase in staff of the Agency up until 2020. A position of Deputy Executive Director of the Agency should therefore be created, taking also into account the fact that the tasks relating to the development and operational management of the systems will require increased and dedicated oversight and that the headquarters and technical sites of the Agency are spread over three Member States. The Management Board should appoint the Deputy Executive Director.

(28) The Agency should be governed and operated taking into account the principles of the Common approach on Union decentralised agencies adopted on 19 July 2012 by the European Parliament, the Council and the Commission.

(29) As regards SIS II, the European Union Agency for Law Enforcement Cooperation (Europol) and the European Judicial Cooperation Unit (Eurojust), which both have the right to access and directly search data entered in SIS II pursuant to Decision 2007/533/JHA, should have observer status at the meetings of the Management Board when a question in relation to the application of that Decision is on the agenda. The European Border and Coast Guard Agency, which has the right to access and search SIS II pursuant to Regulation (EU) 2016/1624, should have observer status at the meetings of the Management Board when a question in relation to the application of that Regulation is on the agenda. Europol, Eurojust and the European Border and Coast Guard Agency should each be able to appoint a representative to the SIS II Advisory Group established under this Regulation.

(30) As regards the VIS, Europol should have observer status at the meetings of the Management Board, when a question in relation to the application of Decision 2008/633/JHA is on the agenda. Europol should be able to appoint a representative to the VIS Advisory Group established under this Regulation.

(31) As regards Eurodac, Europol should have observer status at the meetings of the Management Board, when a question in relation with the application of Regulation (EU) No 603/2013 is on the agenda. Europol should be able to appoint a representative to the Eurodac Advisory Group established under this Regulation.

(32) As regards the EES, Europol should have observer status at the meetings of the Management Board when a question concerning Regulation (EU) 2017/2226 is on the agenda.

(33) As regards ETIAS, Europol should have observer status at the meetings of the Management Board when a question concerning Regulation (EU) 2018/1240 is on the agenda. The European Border and Coast Guard Agency should also have observer status at the meetings of the Management Board when a question concerning ETIAS in relation with the application of that Regulation is on the agenda. Europol and the European Border and Coast Guard Agency should be able to appoint a representative to the EES-ETIAS Advisory Group established under this Regulation.

(34) Member States should have voting rights on the Management Board concerning a large-scale IT system, where they are bound under Union law by any Union legal act governing the development, establishment, operation and use of that particular system. Denmark should also have voting rights in relation to a large-scale IT system if it decides, under Article 4 of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union (TEU) and to the TFEU, to implement the Union legal act governing the development, establishment, operation and use of that particular system in its national law.

(35) Member States should appoint a member to the Advisory Group of a large-scale IT system if they are bound under Union law by any Union legal act governing the development, establishment, operation and use of that particular system. Denmark should, in addition, appoint a member to the Advisory Group of a large-scale IT system if it decides, under Article 4 of Protocol No 22, to implement the Union legal act governing the development, establishment, operation and use of that particular system in its national law. Advisory Groups should cooperate with each other when necessary.

(36) In order to guarantee its full autonomy and independence and to enable it to properly fulfil the objectives and to perform the tasks assigned to it by this Regulation, the Agency should be granted an adequate and autonomous budget with revenue from the general budget of the Union. The financing of the Agency should be subject to an

agreement between the European Parliament and the Council as set out in point 31 of the Interinstitutional Agreement of 2 December 2013 between the European Parliament, the Council and the Commission on budgetary discipline, on cooperation in budgetary matters and sound financial management ([1]). The Union budgetary and discharge procedures should apply. The auditing of accounts and of the legality and regularity of the underlying transactions should be undertaken by the Court of Auditors.

(37) For the purpose of fulfilling its mission and to the extent required for the accomplishment of its tasks, the Agency should be allowed to cooperate with Union institutions, bodies, offices and agencies, in particular those established in the area of freedom, security and justice, in matters covered by this Regulation and the Union legal acts governing the development, establishment, operation and use of the systems in the framework of working arrangements concluded in accordance with Union law and policy and within the framework of their respective competences. Where so provided by a Union legal act, the Agency should also be allowed to cooperate with international organisations and other relevant entities and should be able to conclude working arrangements for that purpose. Those working arrangements should receive the Commission's prior approval and be authorised by the Management Board. The Agency should also consult and follow up on the recommendations of the European Union Agency for Network and Information Security (ENISA), established by Regulation (EU) No 526/2013 of the European Parliament and of the Council ([2]), regarding network and information security, where appropriate.

(38) When ensuring the development and the operational management of the systems, the Agency should follow European and international standards, taking into account the highest professional requirements, in particular the European Union Information Management Strategy.

(39) Regulation (EU) 2018/1725 of the European Parliament and of the Council ([3]) should apply to the processing of personal data by the Agency, without prejudice to the provisions on data protection laid down in the Union legal acts governing the development, establishment, operation and use of the systems, which should be consistent with Regulation (EU) 2018/1725. In order to maintain security and to prevent processing in infringement of Regulation (EU) 2018/1725 and of the Union legal acts governing the systems, the Agency should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage. The European Data Protection Supervisor should be able to obtain from the Agency access to all information necessary for his or her enquiries. In accordance with Regulation (EC) No 45/2001 of the European Parliament and of the Council ([4]), the Commission consulted the European Data Protection Supervisor, who delivered an opinion on 10 October 2017.

(40) In order to ensure the transparent operation of the Agency, Regulation (EC) No 1049/2001 of the European Parliament and of the Council ([5]) should apply to the Agency. The Agency should be as transparent as possible with regard to its activities, without jeopardising the attainment of the objective of its operations. It should make public information on all of its activities. It should likewise ensure that the public and any interested party are promptly given information with regard to its work.

(41) The activities of the Agency should be subject to the scrutiny of the European Ombudsman in accordance with Article 228 TFEU.

([1]) OJ C 373, 20.12.2013, p. 1.

([2]) 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).

([3]) 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 (see page 39 of this Official Journal).

([4]) 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).

([5]) 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).

(42) Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council ([1]) should apply to the Agency, which should 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) ([2]).

(43) Council Regulation (EU) 2017/1939 ([3]), concerning the establishment of the European Public Prosecutor's Office, should apply to the Agency.

(44) In order to ensure open and transparent employment conditions and equal treatment of staff, the Staff Regulations of Officials of the European Union ('Staff Regulations of Officials') and the Conditions of Employment of Other Servants of the European Union ('Conditions of Employment of other Servants'), laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68 ([4]) (together referred to as the 'Staff Regulations'), should apply to the staff (including the Executive Director and the Deputy Executive Director of the Agency), including the rules of professional secrecy or other equivalent duties of confidentiality.

(45) Since the Agency is a body set up by the Union within the meaning of Regulation (EU, Euratom) 2018/1046, the Agency should adopt its financial rules accordingly.

(46) Commission Delegated Regulation (EU) No 1271/2013 ([5]) should apply to the Agency.

(47) The Agency, as established by this Regulation, replaces and succeeds the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, as established by Regulation (EU) No 1077/2011. It should therefore be the legal successor in respect of all contracts concluded by, liabilities incumbent upon, and properties acquired by, the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice as established by Regulation (EU) No 1077/2011. This Regulation should not affect the legal force of agreements, working arrangements and memoranda of understanding concluded by the Agency as established by Regulation (EU) No 1077/2011, without prejudice to any amendments thereto as required by this Regulation.

(48) To enable the Agency to continue to fulfil the tasks of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, as established by Regulation (EU) No 1077/2011, to the best of its abilities, transitional measures should be laid down, in particular with regard to the Management Board, the Advisory Groups, the Executive Director and the internal rules adopted by the Management Board.

(49) This Regulation aims to amend and expand the provisions of Regulation (EU) No 1077/2011. Since the amendments to be made by this Regulation are of a substantial number and nature, Regulation (EU) No 1077/2011 should, in the interests of clarity, be replaced in its entirety in relation to the Member States bound by this Regulation. The Agency, as established by this Regulation, should replace and assume the functions of the Agency, as established by Regulation (EU) No 1077/2011 and, as a consequence, that Regulation should be repealed.

(50) Since the objectives of this Regulation, namely the establishment of an Agency at Union level responsible for the operational management and, where appropriate, the development of large-scale IT systems in the area of freedom, security and justice, cannot be sufficiently achieved by the Member States, but can rather, by reason of the scale and effects of the action, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 TEU. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary to achieve those objectives.

([1]) Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the 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).

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

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

([4]) Regulation (EEC, Euratom, ECSC) No 259/68 of the Council of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities and instituting special measures temporarily applicable to officials of the Commission (OJ L 56, 4.3.1968, p. 1).

([5]) 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).

(51) In accordance with Articles 1 and 2 of Protocol No 22, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this Regulation, insofar as it relates to SIS II, the VIS, the EES and ETIAS builds upon the Schengen *acquis*, Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six months after the Council has decided on this Regulation whether it will implement it in its national law. In accordance with Article 3 of the Agreement between the European Community and the Kingdom of Denmark on the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in Denmark or any other Member State of the European Union and 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention ([1]), Denmark is to notify the Commission whether it will implement the contents of this Regulation, insofar as it relates to Eurodac and DubliNet.

(52) Insofar as its provisions relate to SIS II as governed by Decision 2007/533/JHA, the United Kingdom is taking part in this Regulation, in accordance with Article 5(1) of Protocol No 19 on the Schengen *acquis* integrated into the framework of the European Union, annexed to the TEU and to the TFEU, and Article 8(2) of Council Decision 2000/365/EC ([2]). Insofar as its provisions relate to SIS II as governed by Regulation (EC) No 1987/2006 and to the VIS, to the EES and to ETIAS, this Regulation constitutes a development of the provisions of the Schengen *acquis* in which the United Kingdom does not take part, in accordance with Decision 2000/365/EC; the United Kingdom requested, by its letter of 19 July 2018 to the President of the Council, to be authorised to take part in this Regulation, in accordance with Article 4 of Protocol No 19. By virtue of Article 1 of Council Decision (EU) 2018/1600 ([3]), the United Kingdom has been authorised to take part in this Regulation. Furthermore, insofar as its provisions relate to Eurodac and DubliNet, the United Kingdom notified its wish to take part in the adoption and application of this Regulation by its letter of 23 October 2017 to the President of the Council, in accordance with Article 3 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. The United Kingdom therefore takes part in the adoption of this Regulation, is bound by it and subject to its application.

(53) Insofar as its provisions relate to SIS II as governed by Decision 2007/533/JHA, Ireland could, in principle, take part in this Regulation, in accordance with Article 5(1) of Protocol No 19 and Article 6(2) of Council Decision 2002/192/EC ([4]). Insofar as its provisions relate to SIS II as governed by Regulation (EC) No 1987/2006 and to the VIS, to the EES and to ETIAS, this Regulation constitutes a development of the provisions of the Schengen *acquis* in which Ireland does not take part, in accordance with Decision 2002/192/EC; Ireland has not requested to take part in the adoption of this Regulation, in accordance with Article 4 of Protocol No 19. Ireland is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application to the extent that its measures develop provisions of the Schengen *acquis* as they relate to SIS II as governed by Regulation (EC) No 1987/2006, to the VIS, to the EES and to ETIAS. Furthermore, insofar as its provisions relate to Eurodac and DubliNet, in accordance with Articles 1 and 2 and Article 4a(1) of Protocol No 21, Ireland is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Since it is not possible, under these circumstances, to ensure that this Regulation is applicable in its entirety to Ireland, as required by Article 288 TFEU, Ireland is not taking part in the adoption of this Regulation and is not bound by it or subject to its application, without prejudice to its rights under Protocols No 19 and No 21.

(54) As regards Iceland and Norway, this Regulation constitutes, insofar as it relates to SIS II and the VIS, to the EES and to ETIAS, a development of the provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* ([5]) which fall within the area referred to in Article 1, points A, B and G of Council Decision 1999/437/EC ([6]). As regards

([1]) OJ L 66, 8.3.2006, p. 38.
([2]) Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis* (OJ L 131, 1.6.2000, p. 43).
([3]) Council Decision (EU) 2018/1600 of 28 September 2018 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis relating to the European Union Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) (OJ L 267, 25.10.2018, p. 3).
([4]) Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis* (OJ L 64, 7.3.2002, p. 20).
([5]) OJ L 176, 10.7.1999, p. 36.
([6]) Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* (OJ L 176, 10.7.1999, p. 31).

Eurodac and DubliNet, this Regulation constitutes a new measure within the meaning of the Agreement between the European Community and the Republic of Iceland and the Kingdom of Norway concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Iceland or Norway ([1]). Consequently, subject to their decision to implement it in their internal legal order, delegations of the Republic of Iceland and the Kingdom of Norway should participate in the Management Board of the Agency. In order to determine further detailed rules allowing for the participation of the Republic of Iceland and the Kingdom of Norway in the activities of the Agency, a further arrangement should be concluded between the Union and these States.

(55) As regards Switzerland, this Regulation constitutes, insofar as it relates to SIS II and the VIS, to the EES and to ETIAS, a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen *acquis* ([2]) which fall within the area referred to in Article 1, points A, B and G of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/146/EC ([3]). As regards Eurodac and DubliNet, this Regulation constitutes a new measure related to Eurodac within the meaning of the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland ([4]). Consequently, subject to its decision to implement it in their internal legal order, the delegation of the Swiss Confederation should participate in the Management Board of the Agency. In order to determine further detailed rules allowing for the participation of the Swiss Confederation in the activities of the Agency, a further arrangement should be concluded between the Union and the Swiss Confederation.

(56) As regards Liechtenstein, this Regulation constitutes, insofar as it relates to SIS II and the VIS, to the EES and to ETIAS, a development of the provisions of the Schengen *acquis* within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* ([5]) which fall within the area referred to in Article 1, points A, B and G of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU ([6]).

As regards Eurodac and DubliNet, this Regulation constitutes a new measure within the meaning of the Protocol between the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland ([7]). Consequently, subject to its decision to implement it in its internal legal order, the delegation of the Principality of Liechtenstein should participate in the Management Board of the Agency. In order to determine further detailed rules allowing for the participation of the Principality of Liechtenstein in the activities of the Agency, a further arrangement should be concluded between the Union and the Principality of Liechtenstein,

---

([1]) OJ L 93, 3.4.2001, p. 40.
([2]) OJ L 53, 27.2.2008, p. 52.
([3]) Council Decision 2008/146/EC of 28 January 2008 on the conclusion, on behalf of the European Community, of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 53, 27.2.2008, p. 1).
([4]) OJ L 53, 27.2.2008, p. 5.
([5]) OJ L 160, 18.6.2011, p. 21.
([6]) Council Decision 2011/350/EU of 7 March 2011 on the conclusion, on behalf of the European Union, of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*, relating to the abolition of checks at internal borders and movement of persons (OJ L 160, 18.6.2011, p. 19).
([7]) OJ L 160, 18.6.2011, p. 39.

HAVE ADOPTED THIS REGULATION:

CHAPTER I

SUBJECT MATTER AND OBJECTIVES

Article 1

Subject matter

1. A European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (the Agency) is hereby established.

2. The Agency, as established by this Regulation, shall replace and succeed the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, as established by Regulation (EU) No 1077/2011.

3. The Agency shall be responsible for the operational management of the Schengen Information System (SIS II), the Visa Information System (VIS) and Eurodac.

4. The Agency shall be responsible for the preparation, development or operational management of the Entry/Exit System (EES), DubliNet, and the European Travel Information and Authorisation System (ETIAS).

5. The Agency may be made responsible for the preparation, development or operational management of large-scale IT systems in the area of freedom, security and justice other than those referred to in paragraphs 3 and 4 of this Article, including existing systems, only if so provided by relevant Union legal acts governing those systems, based on Articles 67 to 89 TFEU, taking into account, where appropriate, the developments in research referred to in Article 14 of this Regulation and the results of pilot projects and proofs of concept referred to in Article 15 of this Regulation.

6. Operational management shall consist of all the tasks necessary to keep large-scale IT systems functioning in accordance with the specific provisions applicable to each of them, including responsibility for the communication infrastructure used by them. Those large-scale IT systems shall not exchange data or enable sharing of information or knowledge, unless so provided in a specific Union legal act.

7. The Agency shall also be responsible for the following tasks:

(a) ensuring data quality in accordance with Article 12;

(b) developing the necessary actions to enable interoperability in accordance with Article 13;

(c) carrying out research activities in accordance with Article 14;

(d) carrying out pilot projects, proofs of concept and testing activities in accordance with Article 15; and

(e) providing support to Member States and the Commission in accordance with Article 16.

Article 2

Objectives

Without prejudice to the respective responsibilities of the Commission and of the Member States under the Union legal acts governing large-scale IT systems, the Agency shall ensure:

(a) the development of large-scale IT systems using an adequate project management structure for efficiently developing such systems;

(b) the effective, secure and continuous operation of large-scale IT systems;

(c) the efficient and financially accountable management of large-scale IT systems;

(d) an adequately high quality of service for users of large-scale IT systems;

(e) continuity and uninterrupted service;

(f) a high level of data protection, in accordance with Union data protection law, including specific provisions for each large-scale IT system;

(g) an appropriate level of data and physical security, in accordance with the applicable rules, including specific provisions for each large-scale IT system.

CHAPTER II

TASKS OF THE AGENCY

Article 3

Tasks relating to SIS II

In relation to SIS II, the Agency shall perform:

(a) the tasks conferred on the Management Authority by Regulation (EC) No 1987/2006 and Decision 2007/533/JHA; and

(b) tasks relating to training on the technical use of SIS II, in particular for SIRENE staff (SIRENE — Supplementary Information Request at the National Entries), and training of experts on the technical aspects of SIS II in the framework of Schengen evaluation.

Article 4

Tasks relating to the VIS

In relation to the VIS, the Agency shall perform:

(a) the tasks conferred on the Management Authority by Regulation (EC) No 767/2008 and Decision 2008/633/JHA; and

(b) tasks relating to training on the technical use of the VIS and training of experts on the technical aspects of the VIS in the framework of Schengen evaluation.

Article 5

Tasks relating to Eurodac

In relation to Eurodac, the Agency shall perform:

(a) the tasks conferred on it by Regulation (EU) No 603/2013; and

(b) tasks relating to training on the technical use of Eurodac.

Article 6

Tasks relating to the EES

In relation to the EES, the Agency shall perform:

(a) the tasks conferred on it by Regulation (EU) 2017/2226; and

(b) tasks relating to training on the technical use of the EES and training of experts on the technical aspects of the EES in the framework of Schengen evaluation.

Article 7

Tasks relating to ETIAS

In relation to ETIAS, the Agency shall perform:

(a) the tasks conferred on it by Regulation (EU) 2018/1240; and

(b) tasks relating to training on the technical use of ETIAS and training of experts on the technical aspects of ETIAS in the framework of Schengen evaluation.

Article 8

Tasks relating to DubliNet

In relation to DubliNet, the Agency shall perform:

(a) the operational management of DubliNet, a separate secure electronic transmission channel between the authorities of Member States, set up under Article 18 of Regulation (EC) No 1560/2003, for the purposes of Articles 31, 32 and 34 of Regulation (EU) No 604/2013 of the European Parliament and of the Council ([1]); and

([1]) Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third country national or a stateless person (OJ L 180, 29.6.2013, p. 31).

(b) tasks relating to training on the technical use of DubliNet.

Article 9

Tasks relating to the preparation, development and operational management of other large-scale IT systems

When entrusted with the preparation, development or operational management of other large-scale IT systems referred to in Article 1(5), the Agency shall perform the tasks conferred on it pursuant to the Union legal act governing the relevant system, as well as tasks relating to training on the technical use of those systems, as appropriate.

Article 10

Technical solutions requiring specific conditions before implementation

Where the Union legal acts governing the systems require the Agency to keep those systems functioning 24 hours a day, 7 days a week and without prejudice to those Union legal acts, the Agency shall implement technical solutions to meet those requirements. Where those technical solutions require a duplication of a system or a duplication of components of a system, they shall only be implemented where an independent impact assessment and cost-benefit analysis to be commissioned by the Agency has been carried out and following the consultation of the Commission and the positive decision of the Management Board. The impact assessment shall also examine existing and future needs in terms of the hosting capacity of the existing technical sites related to the development of such technical solutions and the possible risks related to the current operational set up.

Article 11

Tasks relating to the communication infrastructure

1. The Agency shall carry out all the tasks relating to the communication infrastructure of the systems conferred on it by the Union legal acts governing the systems, with the exception of those systems that make use of the EuroDomain for their communication infrastructure. In the case of those systems that make such use of the EuroDomain, the Commission shall be responsible for the tasks of the implementation of the budget, acquisition and renewal, and contractual matters. In accordance with the Union legal acts governing the systems using the EuroDomain, the tasks regarding the communication infrastructure, including the operational management and security, are to be divided between the Agency and the Commission. In order to ensure coherence between the exercise of their respective responsibilities, operational working arrangements shall be concluded between the Agency and the Commission and reflected in a memorandum of understanding.

2. The communication infrastructure shall be adequately managed and controlled in such a way as to protect it from threats and to ensure its security and that of the systems, including that of data exchanged through the communication infrastructure.

3. The Agency shall adopt appropriate measures, including security plans, inter alia, to prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or transport of data media, in particular by means of appropriate encryption techniques. All system-related operational information circulating in the communication infrastructure shall be encrypted.

4. Tasks relating to the delivery, setting up, maintenance and monitoring of the communication infrastructure may be entrusted to external private-sector entities or bodies in accordance with Regulation (EU, Euratom) 2018/1046. Such tasks shall be carried out under the responsibility of the Agency and under its close supervision.

When carrying out the tasks referred to in the first subparagraph, all external private-sector entities or bodies, including network providers, shall be bound by the security measures referred to in paragraph 3 and shall have no access, by any means, to any operational data stored in the systems or transferred through the communication infrastructure or to the SIS II-related SIRENE exchange.

5. The management of the encryption keys shall remain within the competence of the Agency and shall not be outsourced to any external private-sector entity. This is without prejudice to the existing contracts on the communication infrastructures of SIS II, the VIS and Eurodac.

Article 12

Data quality

Without prejudice to Member States' responsibilities with regard to the data entered into the systems, the Agency, closely involving its Advisory Groups, together with the Commission, shall work towards establishing for all the systems automated data quality control mechanisms and common data quality indicators and towards developing a central repository containing only anonymised data for reporting and statistics, subject to specific provisions in the Union legal acts governing the development, establishment, operation and use of the systems.

Article 13

Interoperability

Where interoperability of large-scale IT systems has been stipulated in a relevant Union legal act, the Agency shall develop the necessary actions to enable that interoperability.

Article 14

Monitoring of research

1. The Agency shall monitor developments in research relevant for the operational management of SIS II, the VIS, Eurodac, the EES, ETIAS, DubliNet and other large-scale IT systems as referred to in Article 1(5).

2. The Agency may contribute to the implementation of the parts of the European Union Framework Programme for Research and Innovation that relate to large-scale IT systems in the area of freedom, security and justice. For that purpose, and where the Commission has delegated the relevant powers to it, the Agency shall have the following tasks:

(a) managing some stages of programme implementation and some phases in the lifetime of specific projects on the basis of the relevant work programmes adopted by the Commission;

(b) adopting the instruments of budget execution and for revenue and expenditure and carrying out all the operations necessary for the management of the programme; and

(c) providing support in programme implementation.

3. The Agency shall, on a regular basis and at least once a year, keep the European Parliament, the Council, the Commission, and, where processing of personal data is concerned, the European Data Protection Supervisor, informed on the developments referred to in this Article without prejudice to the reporting requirements in relation to the implementation of parts of the European Union Framework Programme for Research and Innovation referred to in paragraph 2.

Article 15

Pilot projects, proofs of concept and testing activities

1. Upon the specific and precise request of the Commission, which shall have informed the European Parliament and the Council at least three months in advance of making such a request, and after a positive decision of the Management Board, the Agency may, in accordance with point (u) of Article 19(1) of this Regulation and by way of a delegation agreement be entrusted with carrying out pilot projects as referred to in point (a) of Article 58(2) of Regulation (EU, Euratom) 2018/1046 for the development or the operational management of large-scale IT systems pursuant to Articles 67 to 89 TFEU in accordance with point (c) of Article 62(1) of Regulation (EU, Euratom) 2018/1046.

The Agency shall keep the European Parliament, the Council and, where the processing of personal data is concerned, the European Data Protection Supervisor informed on a regular basis of the evolution of the pilot projects carried out by the Agency under the first subparagraph.

2. Financial appropriations for pilot projects as referred to in point (a) of Article 58(2) of Regulation (EU, Euratom) 2018/1046, that have been requested by the Commission under paragraph 1, shall be entered in the budget for no more than two consecutive financial years.

3. At the request of the Commission or the Council, after having informed the European Parliament and after a positive decision of the Management Board, the Agency may be entrusted, by way of a delegation agreement, with budget implementation tasks for proofs of concept funded under the instrument for financial support for external borders and visa established by Regulation (EU) No 515/2014 in accordance with point (c) of Article 62(1) of Regulation (EU, Euratom) 2018/1046.

4. Following a positive decision of the Management Board, the Agency may plan and implement testing activities on matters covered by this Regulation and by any of the Union legal acts governing the development, establishment, operation and use of the systems.

Article 16

Support to Member States and the Commission

1. Any Member State may request the Agency to provide advice with regard to the connection of its national system to the central systems of the large-scale IT systems managed by the Agency.

2. Any Member State may submit a request for ad hoc support to the Commission, which, subject to its positive assessment that such support is required by virtue of extraordinary security or migratory needs, shall transmit it, without delay, to the Agency. The Agency shall inform the Management Board of such requests. The Member State shall be informed where the Commission's assessment is negative.

The Commission shall monitor whether the Agency has provided a timely response to the Member State's request. The Agency's annual activity report shall report in detail on the actions the Agency has carried out to provide ad hoc support to Member States and on the costs incurred in that respect.

3. The Agency may also be requested to provide advice or support to the Commission on technical issues related to existing or new systems, including by way of studies and testing. The Agency shall inform the Management Board of such requests.

4. A group of at least five Member States may entrust the Agency with the task of developing, managing or hosting a common IT component to assist them in implementing technical aspects of obligations deriving from Union law on decentralised systems in the area of freedom, security and justice. Those common IT solutions shall be without prejudice to the obligations of the requesting Member States under the applicable Union law, in particular with regard to the architecture of those systems.

In particular, the requesting Member States may entrust the Agency with the task of establishing a common component or router for advance passenger information and passenger name record data as a technical support tool to facilitate connectivity with air carriers in order to assist Member States in the implementation of Council Directive 2004/82/EC ([1]) and Directive (EU) 2016/681 of the European Parliament and of the Council ([2]). In such a case the Agency shall centrally collect the data from air carriers and transmit those data to the Member States via the common component or router. The requesting Member States shall adopt the necessary measures to ensure that air carriers transfer the data via the Agency.

The Agency shall be entrusted with the task of developing, managing or hosting a common IT component only after prior approval by the Commission and subject to a positive decision of the Management Board.

The requesting Member States shall entrust the Agency with the tasks referred to in the first and second subparagraphs by way of a delegation agreement setting out the conditions for the delegation of the tasks and the calculation of all relevant costs and the invoicing method. All relevant costs shall be covered by the participating Member States. The delegation agreement shall comply with the Union legal acts governing the systems in question. The Agency shall inform the European Parliament and the Council of the approved delegation agreement and of any modifications thereto.

Other Member States may request to participate in a common IT solution where this possibility is provided for in the delegation agreement setting out, in particular, the financial implications of such participation. The delegation agreement shall be modified accordingly following the prior approval by the Commission and after a positive decision of the Management Board.

CHAPTER III

STRUCTURE AND ORGANISATION

Article 17

Legal status and location

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

([1]) Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (OJ L 261, 6.8.2004, p. 24).

([2]) Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ L 119, 4.5.2016, p. 132).

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

3. The seat of the Agency shall be Tallinn, Estonia.

The tasks relating to development and operational management referred to in Article 1(4) and (5) and Articles 3, 4, 5, 6, 7, 8, 9 and 11 shall be carried out at the technical site in Strasbourg, France.

A backup site capable of ensuring the operation of a large-scale IT system in the event of failure of such a system shall be installed in Sankt Johann im Pongau, Austria.

4. Both technical sites may be used for the simultaneous operation of the systems, provided that the backup site remains capable of ensuring their operation in the event of the failure of one or more of the systems.

5. Due to the specific nature of the systems, should it become necessary for the Agency to establish a second separate technical site either in Strasbourg or in Sankt Johann im Pongau, or in both locations, as required, in order to host the systems, such need shall be justified on the basis of an independent impact assessment and cost-benefit analysis. The Management Board shall consult the Commission and take into account its views before notifying the budgetary authority of its intention to implement any project related to property in accordance with Article 45(9).

Article 18

Structure

1. The administrative and management structure of the Agency shall comprise:

(a) a Management Board;

(b) an Executive Director;

(c) Advisory Groups.

2. The structure of the Agency shall include:

(a) a data protection officer;

(b) a security officer;

(c) an accounting officer.

Article 19

Functions of the Management Board

1. The Management Board shall:

(a) provide the general orientation for the Agency's activities;

(b) adopt, by a majority of two-thirds of members entitled to vote, the annual budget of the Agency and exercise other functions in respect of the Agency's budget pursuant to Chapter V;

(c) appoint the Executive Director and the Deputy Executive Director and, where relevant, extend their respective terms of office or remove them from office in accordance with Articles 25 and 26 respectively;

(d) exercise disciplinary authority over the Executive Director and oversee his or her performance, including the implementation of the Management Board's decisions, and exercise disciplinary authority over the Deputy Executive Director in agreement with the Executive Director;

(e) take all decisions on the establishment of the Agency's organisational structure and, where necessary, its modification, taking into consideration the Agency's activity needs and having regard to sound budgetary management;

(f) adopt the Agency's staff policy;

(g) establish the Agency's rules of procedure;

(h) adopt an anti-fraud strategy, proportionate to the risk of fraud, taking into account the costs and benefits of the measures to be implemented;

(i) adopt rules for the prevention and management of conflicts of interest in respect of its members and publish them on the Agency's website;

(j) adopt detailed internal rules and procedures for the protection of whistleblowers, including appropriate channels of communication for reporting misconduct;

(k) authorise the conclusion of working arrangements in accordance with Articles 41 and 43;

(l) approve, following a proposal by the Executive Director, the Headquarters Agreement concerning the seat of the Agency and the agreements concerning the technical and backup sites, set up in accordance with Article 17(3), to be signed by the Executive Director and the host Member States;

(m) exercise, in accordance with paragraph 2, with respect to the staff of the Agency, the powers conferred by the Staff Regulations of Officials on the Appointing Authority and by the Conditions of Employment of Other Servants on the Authority Empowered to Conclude a Contract of Employment ('the appointing authority powers');

(n) adopt, in agreement with the Commission, the necessary implementing rules for giving effect to the Staff Regulations in accordance with Article 110 of the Staff Regulations of Officials;

(o) adopt the necessary rules on the secondment of national experts to the Agency;

(p) adopt a draft estimate of the Agency's revenue and expenditure, including the draft establishment plan, and submit them by 31 January each year to the Commission;

(q) adopt the draft single programming document, containing the Agency's multiannual programming and its work programme for the following year and a provisional draft estimate of the Agency's revenue and expenditure, including the draft establishment plan, and submit it by 31 January each year, as well as any updated version of that document, to the European Parliament, to the Council and to the Commission;

(r) adopt, before 30 November each year, by a two-thirds majority of its members with the right to vote, and in accordance with the annual budgetary procedure, the single programming document taking into account the opinion of the Commission and ensure that the definitive version of this single programming document is transmitted to the European Parliament, to the Council and to the Commission and is published;

(s) adopt an interim report by the end of August of each year on the progress of the implementation of the planned activities for the current year and submit it to the European Parliament, to the Council and to the Commission;

(t) assess and adopt the consolidated annual activity report of the Agency's activities for the previous year, comparing, in particular, the results achieved with the objectives of the annual work programme, and send both the report and its assessment by 1 July of each year to the European Parliament, to the Council, to the Commission and to the Court of Auditors and ensure that the annual activity report is published;

(u) carry out its functions relating to the Agency's budget, including the implementation of pilot projects and proofs of concept as referred to in Article 15;

(v) adopt the financial rules applicable to the Agency in accordance with Article 49;

(w) appoint an accounting officer, who may be the Commission's accounting officer, subject to the Staff Regulations, who shall be completely independent in the performance of his or her duties;

(x) ensure adequate follow-up to the findings and recommendations stemming from the various internal or external audit reports and evaluations as well as from investigations by the European Anti-Fraud Office (OLAF) and the European Public Prosecutor's Office (EPPO);

(y) adopt the communication and dissemination plans referred to in Article 34(4) and regularly update them;

(z) adopt the necessary security measures, including a security plan and a business continuity and disaster recovery plan, taking into account the possible recommendations of the security experts present in the Advisory Groups;

(aa) adopt the security rules on the protection of classified information and non-classified sensitive information following approval by the Commission;

(bb) appoint a security officer;

(cc) appoint a data protection officer in accordance with Regulation (EU) 2018/1725;

(dd) adopt the detailed rules for implementing Regulation (EC) No 1049/2001;

(ee) adopt the reports on the development of the EES pursuant to Article 72(2) of Regulation (EU) 2017/2226 and the reports on the development of ETIAS pursuant to Article 92(2) of Regulation (EU) 2018/1240;

(ff) adopt the reports on the technical functioning of SIS II pursuant to Article 50(4) of Regulation (EC) No 1987/2006 and Article 66(4) of Decision 2007/533/JHA respectively, of the VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and Article 17(3) of Decision 2008/633/JHA, of the EES pursuant to Article 72(4) of Regulation (EU) 2017/2226 and of ETIAS pursuant to Article 92(4) of Regulation (EU) 2018/1240;

(gg) adopt the annual report on the activities of the Central System of Eurodac pursuant to Article 40(1) of Regulation (EU) No 603/2013;

(hh) adopt formal comments on the European Data Protection Supervisor's reports on the audits carried out pursuant to Article 45(2) of Regulation (EC) No 1987/2006, Article 42(2) of Regulation (EC) No 767/2008 and Article 31(2) of Regulation (EU) No 603/2013, Article 56(2) of Regulation (EU) 2017/2226 and Article 67 of Regulation (EU) 2018/1240 and ensure appropriate follow-up of those audits;

(ii) publish statistics related to SIS II pursuant to Article 50(3) of Regulation (EC) No 1987/2006 and Article 66(3) of Decision 2007/533/JHA respectively;

(jj) compile and publish statistics on the work of the Central System of Eurodac pursuant to Article 8(2) of Regulation (EU) No 603/2013;

(kk) publish statistics related to the EES pursuant to Article 63 of Regulation (EU) 2017/2226;

(ll) publish statistics related to ETIAS pursuant to Article 84 of Regulation (EU) 2018/1240;

(mm) ensure annual publication of the list of competent authorities authorised to search directly the data contained in SIS II pursuant to Article 31(8) of Regulation (EC) No 1987/2006 and Article 46(8) of Decision 2007/533/JHA, together with the list of Offices of the national systems of SIS II (N.SIS II Offices) and SIRENE Bureaux pursuant to Article 7(3) of Regulation (EC) No 1987/2006 and Article 7(3) of Decision 2007/533/JHA respectively as well as the list of competent authorities pursuant to Article 65(2) of Regulation (EU) 2017/2226 and the list of competent authorities pursuant to Article 87(2) of Regulation (EU) 2018/1240;

(nn) ensure annual publication of the list of units pursuant to Article 27(2) of Regulation (EU) No 603/2013;

(oo) ensure that all decisions and actions of the Agency affecting large-scale IT systems in the area of freedom, security and justice respect the principle of independence of the judiciary;

(pp) perform any other tasks conferred on it in accordance with this Regulation.

Without prejudice to the provisions on publication of the lists of relevant authorities provided for in the Union legal acts referred to in point (mm) of the first subparagraph and where an obligation to publish and continuously update those lists on the Agency's website is not provided for in those legal acts, the Management Board shall ensure such publication and continuous update.

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

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

3. The Management Board may advise the Executive Director on any matter strictly related to the development or operational management of large-scale IT systems and on activities related to research, pilot projects, proofs of concept and testing activities.

Article 20

Composition of the Management Board

1. The Management Board shall be composed of one representative of each Member State and two representatives of the Commission. Each representative shall have a right to vote in accordance with Article 23.

2. Each member of the Management Board shall have an alternate. The alternate shall represent the member in his or her absence or in the event that the member is elected Chairperson or Deputy Chairperson of the Management Board and is chairing the Management Board meeting. The members of the Management Board and their alternates shall be appointed on the basis of the high level of their relevant experience and expertise in the field of large-scale IT systems in the area of freedom, security and justice, and their knowledge with respect to data protection, taking into account their relevant managerial, administrative and budgetary skills. All parties represented on the Management Board shall make efforts to limit the turnover of their representatives in order to ensure continuity of the Management Board's work. All parties shall aim to achieve a balanced representation between men and women on the Management Board.

3. The term of office of the members and their alternates shall be four years and shall be renewable. Upon expiry of their terms of office or in the event of their resignation, members shall remain in office until their appointments are renewed or until they are replaced.

4. Countries associated with the implementation, application and development of the Schengen *acquis* and with Dublin- and Eurodac-related measures shall participate in the activities of the Agency. They shall each appoint one representative and an alternate to the Management Board.

Article 21

Chairperson of the Management Board

1. The Management Board shall elect a Chairperson and a Deputy Chairperson from among those members of the Management Board that are appointed by Member States which are fully bound under Union law by all the Union legal acts governing the development, establishment, operation and use of all the large-scale IT systems managed by the Agency. The Chairperson and the Deputy Chairperson shall be elected by a majority of two-thirds of the members of the Management Board with the right to vote.

The Deputy Chairperson shall automatically replace the Chairperson if he or she is prevented from attending to his or her duties.

2. The term of office of the Chairperson and the Deputy Chairperson shall be four years. Their terms of office may be renewed once. Where 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.

Article 22

Meetings of the Management Board

1. The Chairperson shall convene the meetings of the Management Board.

2. The Executive Director shall take part in the deliberations, without the right to vote.

3. The Management Board shall hold at least two ordinary meetings a year. In addition, it shall meet on the initiative of its Chairperson, at the request of the Commission, at the request of the Executive Director or at the request of at least one third of the members of the Management Board with the right to vote.

4. Europol and Eurojust may attend the meetings of the Management Board as observers when a question concerning SIS II in relation to the application of Decision 2007/533/JHA is on the agenda. The European Border and Coast Guard Agency may attend the meetings of the Management Board as observer when a question concerning SIS II in relation to the application of Regulation (EU) 2016/1624 is on the agenda.

Europol may attend the meetings of the Management Board as observer when a question concerning the VIS in relation to the application of Decision 2008/633/JHA or a question concerning Eurodac in relation to the application of Regulation (EU) No 603/2013 is on the agenda.

Europol may attend the meetings of the Management Board as observer when a question concerning the EES in relation to the application of Regulation (EC) No 2017/2226 is on the agenda or when a question concerning ETIAS in relation to Regulation (EU) 2018/1240 is on the agenda. The European Border and Coast Guard Agency may also attend the meetings of the Management Board as observer when a question concerning ETIAS in relation with the application of Regulation (EU) 2018/1240 is on the agenda.

The Management Board may invite any other person whose opinion may be of interest to attend its meetings as an observer.

5. The members of the Management Board and their alternates may be assisted by advisers or experts, subject to the rules of procedure for the Management Board, in particular those that are members of the Advisory Groups.

6. The Agency shall provide the secretariat for the Management Board.

Article 23

Voting rules of the Management Board

1. Without prejudice to paragraph 5 of this Article, and to points (b) and (r) of Article 19(1), Article 21(1) and Article 25 (8), decisions of the Management Board shall be taken by a majority of its members with the right to vote.

2. Without prejudice to paragraphs 3 and 4, each member of the Management Board shall have one vote. In the absence of a member with the right to vote, his or her alternate shall be entitled to exercise his or her right to vote.

3. Each member appointed by a Member State which is bound under Union law by any Union legal act governing the development, establishment, operation and use of a large-scale IT system managed by the Agency may vote on a question which concerns that large-scale IT system.

Denmark may vote on a question which concerns a large-scale IT system if it decides under Article 4 of the Protocol No 22 to implement the Union legal act governing the development, establishment, operation and use of that particular large-scale IT system in its national law.

4. Article 42 shall apply as regards the voting rights of the representatives of countries that have entered into agreements with the Union on their association with the implementation, application and development of the Schengen *acquis* and with Dublin- and Eurodac-related measures.

5. In the event of a disagreement among members about whether a vote concerns a specific large-scale IT system, any decision which finds that this vote does not concern that specific large-scale IT system shall be taken by a two-thirds majority of the members of the Management Board with the right to vote.

6. The Chairperson, or the Deputy Chairperson when he or she is replacing the Chairperson, shall not vote. The right to vote of the Chairperson, or of the Deputy Chairperson when he or she is replacing the Chairperson, shall be exercised by his or her alternate member.

7. The Executive Director shall not vote.

8. The rules of procedure for the Management Board shall establish more detailed voting arrangements, in particular the conditions under which a member may act on behalf of another member and any quorum requirements, where appropriate.

Article 24

Responsibilities of the Executive Director

1. The Executive Director shall manage the Agency. The Executive Director shall assist and be accountable to the Management Board. 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.

2. The Executive Director shall be the legal representative of the Agency.

3. The Executive Director shall be responsible for the implementation of tasks assigned to the Agency by this Regulation. In particular, the Executive Director shall be responsible for:

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

(b) the operation of the Agency in accordance with this Regulation;

(c) preparing and implementing the procedures, decisions, strategies, programmes and activities adopted by the Management Board, within the limits set out by this Regulation, its implementing rules and the applicable Union law;

(d) preparing the single programming document and submitting it to the Management Board after consulting the Commission and the Advisory Groups;

(e) implementing the single programming document and reporting to the Management Board on its implementation;

(f) preparing the interim report on the progress of the implementation of the planned activities for the current year and, after consulting the Advisory Groups, submitting it to the Management Board for adoption by the end of August of each year;

(g) preparing the consolidated annual report of the Agency's activities and, after consulting the Advisory Groups, submitting it to the Management Board for assessment and adoption;

(h) preparing an action plan following up on the conclusions of internal or external audit reports and evaluations, as well as on investigations by OLAF and by the EPPO, and reporting on progress twice a year to the Commission and regularly to the Management Board;

(i) protecting the financial interests of the Union by applying preventive measures against fraud, corruption and any other illegal activities, without prejudicing the investigative competence of the EPPO and OLAF, by effective checks and, if irregularities are detected, by recovering amounts wrongly paid and, where appropriate, by imposing effective, proportionate and dissuasive administrative, including financial, penalties;

(j) preparing an anti-fraud strategy for the Agency and submitting it to the Management Board for approval as well as monitoring the proper and timely implementation of that strategy;

(k) preparing draft financial rules applicable to the Agency and submitting them to the Management Board for adoption after consulting the Commission;

(l) preparing the draft budget for the following year, established on the basis of activity-based budgeting;

(m) preparing the Agency's draft statement of estimates of revenue and expenditure;

(n) implementing the budget of the Agency;

(o) establishing and implementing an effective system to enable the regular monitoring and evaluation of:

(i) large-scale IT systems, including statistics, and

(ii) the Agency, including the effective and efficient achievement of its objectives;

(p) establishing, without prejudice to Article 17 of the Staff Regulations of Officials, confidentiality requirements in order to comply with Article 17 of Regulation (EC) No 1987/2006, Article 17 of Decision 2007/533/JHA, Article 26(9) of Regulation (EC) No 767/2008, Article 4(4) of Regulation (EU) No 603/2013; Article 37(4) of Regulation (EC) No 2017/2226 and Article 74(2) of Regulation (EU) 2018/1240;

(q) negotiating and, after approval by the Management Board, signing a Headquarters Agreement concerning the seat of the Agency and agreements concerning the technical and backup sites with the host Member States;

(r) preparing the practical arrangements for implementing Regulation (EC) No 1049/2001 and submitting them to the Management Board for adoption;

(s) preparing the necessary security measures, including a security plan and a business continuity and disaster recovery plan, and, after consulting the relevant Advisory Group, submitting them to the Management Board for adoption;

(t) preparing the reports on the technical functioning of each large-scale IT system referred to in point (ff) of Article 19(1) and the annual report on the activities of the Central System of Eurodac referred to in point (gg) of Article 19(1) on the basis of the results of monitoring and evaluation and, after consulting the relevant Advisory Group, submitting them to the Management Board for adoption;

(u) preparing the reports on the development of the EES referred to in Article 72(2) of Regulation (EC) No 2017/2226 and on the development of ETIAS referred to in Article 92(2) of Regulation (EU) 2018/1240 and submitting them to the Management Board for adoption;

(v) preparing the annual list for publication of competent authorities authorised to search directly the data contained in SIS II, including the list of N.SIS II Offices and SIRENE Bureaux, and the list of competent authorities authorised to search directly the data contained in the EES and ETIAS referred to in point (mm) of Article 19(1) and the list of units referred to in point (nn) of Article 19(1), and submitting them to the Management Board for adoption.

4. The Executive Director shall perform any other tasks in accordance with this Regulation.

5. The Executive Director shall decide whether it is necessary to locate one or more staff members in one or more Member States in order to carry out the Agency's tasks in an efficient and effective manner and to establish a local office for that purpose. Before adopting such a decision, the Executive Director shall obtain the prior consent of the Commission, the Management Board and the Member State or Member States concerned. The decision of the Executive Director 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 the Agency. Activities carried out in technical sites shall not be carried out in a local office.

Article 25

Appointment of the Executive Director

1. The Management Board shall appoint the Executive Director from a list of at least three candidates proposed by the Commission following an open and transparent selection procedure. The selection procedure shall provide for publication in the *Official Journal of the European Union* and in other appropriate media of a call for expressions of interest. The Management Board shall appoint the Executive Director on the grounds of merit, proven experience in the field of large-scale IT systems, administrative, financial and management skills and knowledge with respect to data protection.

2. Before appointment, the candidates proposed by the Commission shall be invited to make a statement before the competent committee or committees of the European Parliament and answer questions from the committee members. After hearing the statement and the responses, the European Parliament shall adopt an opinion setting out its view and may indicate a preferred candidate.

3. The Management Board shall appoint the Executive Director taking those views into account.

4. If the Management Board takes a decision to appoint a candidate other than the candidate whom the European Parliament indicated as its preferred candidate, the Management Board shall inform the European Parliament and the Council in writing of the manner in which the opinion of the European Parliament was taken into account.

5. The term of office of the Executive Director shall be five years. By the end of that period, the Commission shall undertake an assessment that takes into account its evaluation of the Executive Director's performance and the Agency's future tasks and challenges.

6. The Management Board, acting on a proposal from the Commission that takes into account the assessment referred to in paragraph 5, may extend the term of office of the Executive Director once for no more than five years.

7. The Management Board shall inform the European Parliament if it intends to extend the Executive Director's term of office. Within the one-month period before any such extension, the Executive Director shall be invited to make a statement before the competent committee or committees of the European Parliament and answer questions from the committee members.

8. An Executive Director whose term of office has been extended may not participate in another selection procedure for the same post at the end of the overall period.

9. The Executive Director may be removed from office only upon a decision of the Management Board, acting on a proposal from a majority of its members with the right to vote or from the Commission.

10. The Management Board shall reach decisions on appointment, extension of the term of office or removal from office of the Executive Director on the basis of a two-thirds majority of votes of its members with the right to vote.

11. For the purpose of concluding the employment contract with the Executive Director, the Agency shall be represented by the Chairperson of the Management Board. The Executive Director shall be engaged as a temporary agent of the Agency under Article 2(a) of the Conditions of Employment of other Servants.

Article 26

Deputy Executive Director

1. A Deputy Executive Director shall assist the Executive Director. The Deputy Executive Director shall also replace the Executive Director in his or her absence. The Executive Director shall set out the duties of the Deputy Executive Director.

2. On the proposal of the Executive Director, the Management Board shall appoint the Deputy Executive Director. The Deputy Executive Director shall be appointed on the grounds of merit and appropriate administrative and management skills, including relevant professional experience. The Executive Director shall propose at least three candidates for the post of Deputy Executive Director. The Management Board shall take its decision by a two-thirds majority of its members with a right to vote. The Management Board shall have the power to dismiss the Deputy Executive Director by means of a decision adopted by a two-thirds majority of its members with a right to vote.

3. The term of office of the Deputy Executive Director shall be five years. The Management Board may extend that term once, for a period of no more than five years. The Management Board shall adopt such a decision by a two-thirds majority of its members with the right to vote.

Article 27

Advisory Groups

1. The following Advisory Groups shall provide the Management Board with expertise relating to large-scale IT systems and, in particular, in the context of the preparation of the annual work programme and the annual activity report:

(a) SIS II Advisory Group;

(b) VIS Advisory Group;

(c) Eurodac Advisory Group;

(d) EES-ETIAS Advisory Group;

(e) any other advisory group relating to a large-scale IT system when so provided in the relevant Union legal act governing the development, establishment, operation and use of that large-scale IT system.

2. Each Member State that is bound under Union law by any Union legal act governing the development, establishment, operation and use of a particular large-scale IT system, and the Commission shall appoint one member to the Advisory Group relating to that large-scale IT system for a four-year term, which may be renewed.

Denmark shall also appoint a member to an Advisory Group relating to a large-scale IT system if it decides under Article 4 of the Protocol No 22 to implement the Union legal act governing the development, establishment, operation and use of that particular large-scale IT system in its national law.

Each country associated with the implementation, application and development of the Schengen *acquis* and with Dublin- and Eurodac-related measures that participates in a particular large-scale IT system shall appoint a member to the Advisory Group relating to that large-scale IT system.

3. Europol, Eurojust and the European Border and Coast Guard Agency may each appoint a representative to the SIS II Advisory Group. Europol may also appoint a representative to the VIS, Eurodac and EES-ETIAS Advisory Groups. The European Border and Coast Guard Agency may also appoint a representative to the EES-ETIAS Advisory Group.

4. Members of the Management Board and their alternates shall not be members of any of the Advisory Groups. The Executive Director or a representative of the Executive Director shall be entitled to attend all the meetings of the Advisory Groups as an observer

5. Advisory Groups shall cooperate with each other as necessary. The procedures for the operation and cooperation of the Advisory Groups shall be laid down in the Agency's rules of procedure.

6. When preparing an opinion, the members of each Advisory Group shall do their best to reach consensus. If consensus is not reached, the reasoned position of the majority of members shall be considered the opinion of the Advisory Group. The minority reasoned position or positions shall also be recorded. Article 23(3) and (5) shall apply accordingly. The members representing the countries associated with the implementation, application and development of the Schengen *acquis* and with Dublin- and Eurodac-related measures shall be allowed to express opinions on issues on which they are not entitled to vote.

7. Each Member State and each country associated with the implementation, application and development of the Schengen *acquis* and with Dublin- and Eurodac-related measures shall facilitate the activities of the Advisory Groups.

8. Article 21 shall apply *mutatis mutandis* as regards the chair of the Advisory Groups.

CHAPTER IV

GENERAL PROVISIONS

Article 28

Staff

1. The Staff Regulations and the rules adopted by agreement between the institutions of the Union for giving effect to the Staff Regulations shall apply to the staff of the Agency, including the Executive Director.

2. For the purpose of implementing the Staff Regulations, the Agency shall be considered an agency within the meaning of Article 1a(2) of the Staff Regulations of Officials.

3. The staff of the Agency shall consist of officials, temporary staff and contract staff. The Management Board shall, on an annual basis, give its consent in the case of contracts that the Executive Director plans to renew where, following renewal, those contracts would be of an indefinite period pursuant to the Conditions of Employment of Other Servants.

4. The Agency shall not recruit interim staff to perform what are deemed to be sensitive financial duties.

5. The Commission and the Member States may second officials or national experts to the Agency on a temporary basis. The Management Board shall adopt a decision laying down rules on the secondment of national experts to the Agency.

6. Without prejudice to Article 17 of the Staff Regulations of Officials, the Agency shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality.

7. The Management Board shall, in agreement with the Commission, adopt the necessary implementing measures referred to in Article 110 of the Staff Regulations of Officials.

Article 29

Public interest

The members of the Management Board, the Executive Director, the Deputy Executive Director and the members of the Advisory Groups shall undertake to act in the public interest. For that purpose, they shall issue an annual, written, public statement of commitment which shall be published on the Agency's website.

The list of members of the Management Board and of members of the Advisory Groups shall be published on the Agency's website.

Article 30

Headquarters Agreement and agreements concerning the technical sites

1. The necessary arrangements concerning the accommodation to be provided for the Agency in the host Member States and the facilities to be made available by those Member States, together with the specific rules applicable in the host Member States to the members of the Management Board, to the Executive Director, to the other members of staff of the Agency and to the members of their families, shall be laid down in a Headquarters Agreement concerning the seat of the Agency and in agreements concerning the technical sites. Such agreements shall be concluded between the Agency and the host Member States, following approval by the Management Board.

2. The Agency's host Member States shall provide the necessary conditions to ensure the proper functioning of the Agency, including, inter alia, multilingual, European-oriented schooling and appropriate transport connections.

Article 31

Privileges and immunities

The Protocol on the Privileges and Immunities of the European Union shall apply to the Agency.

Article 32

Liability

1. The contractual liability of the Agency 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 the Agency.

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

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

5. The personal liability of the Agency's staff towards the Agency shall be governed by the provisions laid down in the Staff Regulations of Officials or Conditions of Employment of Other Servants applicable to them.

Article 33

Language arrangements

1. Council Regulation No 1 ([1]) shall apply to the Agency.

2. Without prejudice to decisions taken pursuant to Article 342 TFEU, the single programming document referred to in point (r) of Article 19(1) and the annual activity report referred to in point (t) of Article 19(1) shall be produced in all official languages of the institutions of the Union.

3. The Management Board may adopt a decision on working languages without prejudice to the obligations set out in paragraphs 1 and 2.

4. The translation services necessary for the activities of the Agency shall be provided by the Translation Centre for the Bodies of the European Union.

Article 34

Transparency and communication

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

2. On the basis of a proposal by the Executive Director, the Management Board shall adopt the detailed rules for applying Regulation (EC) No 1049/2001 without delay.

3. Decisions taken by the Agency pursuant to Article 8 of Regulation (EC) No 1049/2001 may form the subject of a complaint to the European Ombudsman or of an action before the Court of Justice of the European Union, under the conditions laid down in Articles 228 and 263 TFEU respectively.

4. The Agency shall communicate in accordance with the Union legal acts governing the development, establishment, operation and use of large-scale IT-systems and may engage in communication activities on its own initiative within its field of competence. The Agency shall ensure, in particular, that in addition to the publications specified in points (r), (t), (ii), (jj), (kk) and (ll) of Article 19(1) and Article 47(9), the public and any interested party are promptly given objective, accurate, reliable comprehensive and easily understandable information with regard to its work. The allocation of resources to communication activities shall not be detrimental to the effective exercise of the Agency's tasks as referred to in Articles 3 to 16. Communication activities shall be carried out in accordance with the relevant communication and dissemination plans adopted by the Management Board.

5. Any natural or legal person shall be entitled to address written correspondence to the Agency in any of the official languages of the Union. The person concerned shall have the right to receive an answer in the same language.

Article 35

Data protection

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

2. The Management Board shall adopt measures for the application of Regulation (EU) 2018/1725 by the Agency, including measures concerning the data protection officer. Those measures shall be adopted after consulting the European Data Protection Supervisor.

([1]) Council Regulation No 1 of 15 April 1958 determining the languages to be used by the European Economic Community (OJ 17, 6.10.1958, p. 385).

Article 36

Purposes of processing personal data

1. The Agency may process personal data only for the following purposes:

(a) where necessary for the performance of its tasks related to the operational management of large-scale IT systems entrusted to it under Union law;

(b) where necessary for its administrative tasks.

2. Where the Agency processes personal data for the purpose referred to in point (a) of paragraph 1 of this Article, Regulation (EU) 2018/1725 shall apply without prejudice to the specific provisions concerning data protection and data security of the Union legal acts governing the development, establishment, operation and use of the systems.

Article 37

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

1. The Agency shall adopt its own security rules based on the principles and rules laid down in the Commission's security rules for protecting European Union Classified Information (EUCI) and sensitive non-classified information, including, inter alia, provisions for the exchange with third states, processing and storage of such information as set out in Commission Decisions (EU, Euratom) 2015/443 ([1]) and 2015/444 ([2]). Any administrative arrangement on the exchange of classified information with the relevant authorities of a third state or, in the absence of such arrangement, any exceptional ad hoc release of EUCI to such authorities shall have received the Commission's prior approval.

2. The Management Board shall adopt the security rules referred to in paragraph 1 of this Article following approval by the Commission. The Agency may take all necessary measures to facilitate the exchange of information relevant to its tasks with the Commission and the Member States and, where appropriate, the relevant Union agencies. The Agency shall develop and operate an information system capable of exchanging classified information with the Commission, the Member States and relevant Union agencies in accordance with Decision (EU, Euratom) 2015/444. The Management Board shall, pursuant to Article 2 and point (z) of Article 19(1) of this Regulation, decide on the Agency's internal structure necessary to comply with the appropriate security principles.

Article 38

Security of the Agency

1. The Agency shall be responsible for the security and the maintenance of order within the buildings, premises and land used by it. The Agency shall apply the security principles and relevant provisions of the Union legal acts governing the development, establishment, operation and use of large-scale IT systems.

2. The host Member States shall take all effective and adequate measures to maintain order and security in the immediate vicinity of the buildings, premises and land used by the Agency and shall provide the Agency with the appropriate protection in accordance with the Headquarters Agreement concerning the seat of the Agency and the agreements concerning the technical and backup sites, whilst guaranteeing the free access of persons authorised by the Agency to those buildings, premises and land.

Article 39

Evaluation

1. By 12 December 2023, and every five years thereafter, the Commission, after consulting the Management Board, shall evaluate, in accordance with the Commission's guidelines, the performance of the Agency in relation to its objectives, mandate, locations and tasks. That evaluation shall also include an examination of the implementation of this Regulation and the way and extent to which the Agency effectively contributes to the operational management of large-scale IT systems and to the establishment of a coordinated, cost-effective and coherent IT environment at Union level in the area of freedom, security and justice. That evaluation shall, in particular, assess the possible need to modify the mandate of the Agency and the financial implications of any such modification. The Management Board may issue recommendations regarding amendments to this Regulation to the Commission.

([1]) Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41).
([2]) Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

2. Where the Commission considers that the continuation of the Agency is no longer justified with regard to its assigned objectives, mandate and tasks, it may propose that this Regulation be amended accordingly or repealed.

3. The Commission shall report to the European Parliament, to the Council and to the Management Board on the findings of the evaluation referred to in paragraph 1. The findings of the evaluation shall be made public.

Article 40

Administrative inquiries

The activities of the Agency shall be subject to the inquiries of the European Ombudsman in accordance with Article 228 TFEU.

Article 41

Cooperation with Union institutions, bodies, offices and agencies

1. The Agency shall cooperate with the Commission, with other Union institutions and with other Union bodies, offices and agencies, in particular those established in the area of freedom, security and justice, and in particular the European Union Agency for Fundamental Rights, in matters covered by this Regulation, in order to achieve, inter alia, coordination and financial savings, to avoid duplication and to promote synergy and complementarity as regards their respective activities.

2. The Agency shall cooperate with the Commission within the framework of a working arrangement laying down operational working methods.

3. The Agency shall consult and follow the recommendations of the European Network and Information Security Agency regarding network and information security, where appropriate.

4. Cooperation with Union bodies, offices and agencies shall take place within the framework of working arrangements. The Management Board shall authorise such working arrangements, taking into account the opinion of the Commission. Where the Agency does not follow the Commission's opinion, it shall justify its reasons. Such working arrangements may provide for the sharing of services between agencies, where appropriate, either by proximity of locations or by policy area within the limits of the respective mandates and without prejudice to their core tasks. Such working arrangements may establish a mechanism for cost recovery.

5. Union institutions, bodies, offices and agencies shall use information received from the Agency only within the limits of their competences and insofar as they respect fundamental rights, including data protection requirements. Onward transmission or other communication of personal data processed by the Agency to Union institutions, bodies, offices or agencies shall be subject to specific working arrangements regarding the exchange of personal data and subject to the prior approval by the European Data Protection Supervisor. Any transfer of personal data by the Agency shall be in accordance with Articles 35 and 36. As regards the handling of classified information, such working arrangements shall provide that the Union institution, body, office or agency concerned comply with security rules and standards equivalent to those applied by the Agency.

Article 42

Participation by countries associated with the implementation, application and development of the Schengen acquis and with Dublin- and Eurodac-related measures

1. The Agency shall be open to the participation of countries that have entered into agreements with the Union on their association with the implementation, application and development of the Schengen *acquis* and with Dublin- and Eurodac-related measures.

2. Under the relevant provisions of the agreements referred to in paragraph 1, arrangements shall be made specifying, in particular, the nature and extent of, and the detailed rules for, the participation of countries as referred to in paragraph 1 in the work of the Agency, including provisions on financial contributions, staff and voting rights.

Article 43

Cooperation with international organisations and other relevant entities

1. Where so provided by a Union legal act, in so far as it is necessary for the performance of its tasks, the Agency may, by means of the conclusion of working arrangements, establish and maintain relations with international organisations and their subordinate bodies, governed by public international law, or other relevant entities or bodies, which are set up by, or on the basis of, an agreement between two or more countries.

2. In accordance with paragraph 1, working arrangements may be concluded specifying, in particular, the scope, nature, purpose and extent of such cooperation. Such working arrangements may be concluded only with the authorisation of the Management Board after having received the Commission's prior approval.

CHAPTER V

ESTABLISHMENT AND STRUCTURE OF THE BUDGET

SECTION 1

Single programming document

Article 44

Single programming document

1. Each year the Executive Director shall draw up a draft single programming document for the following year, as set out in Article 32 of Delegated Regulation (EU) No 1271/2013 and in the relevant provision of the Agency's financial rules adopted pursuant to Article 49 of this Regulation and taking into account guidelines set by the Commission.

The single programming document shall contain a multiannual programme, an annual work programme and the Agency's budget and information on its resources, as set out in detail in the Agency's financial rules adopted pursuant to Article 49.

2. The Management Board shall adopt the draft single programming document after consulting the Advisory Groups and shall send it to the European Parliament, to the Council and to the Commission by 31 January each year, as well as any updated version of that document.

3. Before 30 November each year, the Management Board shall adopt, by a two-thirds majority of its members with the right to vote, and in accordance with the annual budgetary procedure, the single programming document, taking into account the opinion of the Commission. The Management Board shall ensure that the definitive version of this single programming document is sent to the European Parliament, to the Council and to the Commission and is published.

4. The single programming document shall become definitive after the final adoption of the general budget of the Union and, if necessary, shall be adjusted accordingly. The adopted single programming document shall then be sent to the European Parliament, the Council and the Commission and shall be published.

5. The annual work programme for the following year 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 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 6. It shall clearly indicate tasks that have been added, changed or deleted in comparison with the previous financial year. The Management Board shall amend the adopted annual work programme when a new task is given to the Agency. Any substantial amendment to the annual work programme shall be adopted by the same procedure as 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.

6. The multiannual programme shall set out the overall strategic programming, including objectives, expected results and performance indicators. It shall also set out resource programming, including multiannual budget and staff. The resource programming shall be updated annually. The strategic programming shall be updated where appropriate and in particular to address the outcome of the evaluation referred to in Article 39.

Article 45

Establishment of the budget

1. Each year the Executive Director shall draw up, taking into account the activities carried out by the Agency, a draft statement of estimates of the Agency's revenue and expenditure for the following financial year, including a draft establishment plan, and shall submit it to the Management Board.

2. The Management Board shall, on the basis of the draft statement of estimates drawn up by the Executive Director, adopt a draft estimate of the revenue and expenditure of the Agency for the following financial year, including the draft establishment plan. By 31 January each year, the Management Board shall send it to the Commission and to the countries associated with the implementation, application and development of the Schengen *acquis* and with Dublin- and Eurodac-related measures, as a part of the single programming document.

3. The Commission shall send the draft estimate to the budgetary authority together with the preliminary draft general budget of the Union.

4. On the basis of the draft estimate, the Commission shall enter in the draft general budget of the Union the estimates it deems necessary for the establishment plan and the amount of the subsidy to be charged to the general budget, which it shall place before the budgetary authority in accordance with Articles 313 and 314 TFEU.

5. The budgetary authority shall authorise the appropriations for the contribution to the Agency.

6. The budgetary authority shall adopt the establishment plan for the Agency.

7. The Management Board shall adopt the Agency's budget. It shall become final following the final adoption of the general budget of the Union. Where appropriate, the Agency's budget shall be adjusted accordingly.

8. Any modification to the Agency's budget, including the establishment plan, shall follow the same procedure as that applicable to the establishment of the initial budget.

9. Without prejudice to Article 17(5), the Management Board shall, as soon as possible, notify the budgetary authority of its intention to implement any project which may have significant financial implications for the funding of its budget, in particular any projects relating to property, such as the rental or purchase of buildings. The Management Board shall inform the Commission thereof. If either branch of the budgetary authority intends to issue an opinion, it shall, within two weeks of the receipt of the information on the project, notify the Management Board of its intention to issue such an opinion. In the absence of a reply, the Agency may proceed with the planned operation. Delegated Regulation (EU) No 1271/2013 shall apply to any building project likely to have any significant implications for the Agency's budget.

SECTION 2

Presentation, implementation and control of the budgET

Article 46

Structure of the budget

1. Estimates of all revenue and expenditure for the Agency shall be prepared each financial year, corresponding to the calendar year, and shall be shown in the Agency's budget.

2. The Agency's budget shall be balanced in terms of revenue and of expenditure.

3. Without prejudice to other types of income, the revenue of the Agency shall consist of:

(a) a contribution from the Union entered in the general budget of the Union (Commission section);

(b) a contribution from the countries associated with the implementation, application and development of the Schengen *acquis* and with Dublin- and Eurodac-related measures that participate in the work of the Agency, as established in the respective association agreements and in the arrangements referred to in Article 42 that specify their financial contribution;

(c) Union funding in the form of delegation agreements in accordance with the Agency's financial rules adopted pursuant to Article 49 and with the provisions of the relevant instruments supporting the policies of the Union;

(d) contributions paid by Member States for the services provided to them in accordance with the delegation agreement referred to in Article 16;

(e) cost recovery paid by Union bodies, offices and agencies for services provided to them in accordance with the working arrangements referred to in Article 41; and

(f) any voluntary financial contribution from the Member States.

4. The expenditure of the Agency shall include staff remuneration, administrative and infrastructure expenses and operational expenditure.

Article 47

Implementation and control of the budget

1. The Executive Director shall implement the Agency's budget.

2. Each year the Executive Director shall forward to the budgetary authority all information relevant to the findings of evaluation procedures.

3. By 1 March of a financial year N+1, the Agency's accounting officer shall communicate the provisional accounts for financial year N to the Commission's accounting officer and the Court of Auditors. The Commission's accounting officer shall consolidate the provisional accounts of the institutions and decentralised bodies in accordance with Article 245 of Regulation (EU, Euratom) 2018/1046.

4. The Executive Director shall send a report on the budgetary and financial management for year N to the European Parliament, to the Council, to the Commission and to the Court of Auditors by 31 March of year N+1.

5. The Commission's accounting officer shall send the Agency's provisional accounts for year N, consolidated with the Commission's accounts, to the Court of Auditors by 31 March of year N+1.

6. On receipt of the Court of Auditors' observations on the Agency's provisional accounts, pursuant to Article 246 of Regulation (EU, Euratom) 2018/1046, the Executive Director shall draw up the Agency's final accounts under his or her own responsibility and forward them to the Management Board for an opinion.

7. The Management Board shall deliver an opinion on the Agency's final accounts for year N.

8. By 1 July of year N+1, the Executive Director shall send the final accounts, together with the opinion of the Management Board, to the European Parliament, to the Council, to the Commission and to the Court of Auditors as well as to the countries associated with the implementation, application and development of the Schengen *acquis* and with Dublin- and Eurodac-related measures.

9. The final accounts for year N shall be published in the *Official Journal of the European Union* by 15 November of year N +1.

10. The Executive Director shall send the Court of Auditors a reply to its observations by 30 September of year N+1. The Executive Director shall also send that reply to the Management Board.

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 year N, in accordance with Article 261(3) of Regulation (EU, Euratom) 2018/1046.

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

Article 48

Prevention of conflicts of interest

The Agency shall adopt internal rules requiring the members of its Management Board and its Advisory Groups and its staff members to avoid any situation liable to give rise to a conflict of interest during their employment or term of office and to report such situations. Those internal rules shall be published on the website of the Agency.

Article 49

Financial rules

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

Article 50

Combating fraud

1. In order to combat fraud, corruption and other unlawful activities, Regulation (EU, Euratom) No 883/2013 and Regulation (EU) 2017/1939 shall apply.

2. The Agency shall accede to the Interinstitutional Agreement of 25 May 1999 concerning internal investigations by OLAF and shall adopt, without delay, the appropriate provisions applicable to all the employees of the Agency using the template set out in the Annex to that Agreement.

3. 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 the Agency.

4. 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 ([1]), 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 the Agency.

5. Without prejudice to paragraphs 1, 2, 3 and 4, contracts, grant agreements and grant decisions of the Agency shall contain provisions expressly empowering the Court of Auditors, OLAF and the EPPO to conduct audits and investigations, in accordance with their respective competences.

CHAPTER VI

AMENDMENTS TO OTHER UNION LEGAL ACTS

Article 51

Amendment to Regulation (EC) No 1987/2006

In Regulation (EC) No 1987/2006, Article 15(2) and (3) are replaced by the following:

'2. The Management Authority shall be responsible for all tasks relating to the Communication Infrastructure, in particular:

(a) supervision;

(b) security;

(c) the coordination of relations between the Member States and the provider;

(d) tasks relating to implementation of the budget;

(e) acquisition and renewal, and

(f) contractual matters.'.

Article 52

Amendment to Decision 2007/533/JHA

In Decision 2007/533/JHA, Article 15(2) and (3) are replaced by the following:

'2. The Management Authority shall also be responsible for all tasks relating to the Communication Infrastructure, in particular:

(a) supervision;

(b) security;

(c) the coordination of relations between the Member States and the provider;

(d) tasks relating to implementation of the budget;

(e) acquisition and renewal, and

(f) contractual matters.'.

CHAPTER VII

TRANSITIONAL PROVISIONS

Article 53

Legal succession

1. The Agency, as established by this Regulation, shall be the legal successor in respect of all contracts concluded by, liabilities incumbent on, and properties acquired by the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice as established by Regulation (EU) No 1077/2011.

([1]) 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).

2. This Regulation shall not affect the legal force of agreements, working arrangements and memoranda of understanding concluded by the Agency as established by Regulation (EU) No 1077/2011, without prejudice to any amendments thereto required by this Regulation.

Article 54

Transitional arrangements concerning the Management Board and the Advisory Groups

1. The members and the Chairperson and Deputy Chairperson of the Management Board, appointed on the basis of Articles 13 and 14 of Regulation (EU) No 1077/2011 respectively, shall continue to exercise their functions for the remaining terms of their office.

2. The members, Chairpersons and deputy Chairpersons of the Advisory groups, appointed on the basis of Article 19 of Regulation (EU) No 1077/2011, shall continue to exercise their functions for their remaining terms of office.

Article 55

Maintenance in force of the internal rules adopted by the Management Board

Internal rules and measures adopted by the Management Board on the basis of Regulation (EU) No 1077/2011 shall remain in force after 11 December 2018, without prejudice to any amendments thereto required by this Regulation.

Article 56

Transitional arrangements concerning the Executive Director

The Executive Director of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, appointed on the basis of Article 18 of Regulation (EU) No 1077/2011, shall, for his or her remaining term of office, be assigned the responsibilities of the Executive Director of the Agency, as provided for in Article 24 of this Regulation. The other conditions of his or her contract shall remain unchanged. If a decision extending the mandate of the Executive Director in accordance with Article 18(4) of Regulation (EU) No 1077/2011 is adopted prior to 11 December 2018, the term of office shall be extended automatically until 31 October 2022.

CHAPTER VIII

FINAL PROVISIONS

Article 57

Replacement and repeal

Regulation (EU) No 1077/2011 is hereby replaced with regard to the Member States bound by this Regulation.

Therefore, Regulation (EU) No 1077/2011 is repealed.

With regard to the Member States bound by this Regulation, references to the repealed Regulation shall be construed as references to this Regulation and shall be read in accordance with the correlation table in the Annex to this Regulation.

Article 58

Entry into force and applicability

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

This Regulation shall apply from 11 December 2018. However point (x) of Article 19(1), points (h) and (i) of Article 24(3) and Article 50(5) of this Regulation, insofar as they refer to the EPPO, and Article 50(1) of this Regulation, insofar as it refers to Regulation (EU) 2017/1939, shall apply from the date determined by the Commission decision provided for in the second subparagraph of Article 120(2) of Regulation (EU) 2017/1939.

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

Done at Strasbourg, 14 November 2018.

For the European Parliament	*For the Council*
The President	*The President*
A. TAJANI	K. EDTSTADLER

ANNEX

CORRELATION TABLE

Regulation (EU) No 1077/2011	This Regulation
Article 1(1)	Article 1(1)
—	Article 1(2)
Article 1(2)	Article 1(3) and (4)
Article 1(3)	Article 1(5)
Article 1(4)	Article 1(6)
Article 2	Article 2
Article 3	Article 3
Article 4	Article 4
Article 5	Article 5
Article 5a	Article 6
—	Article 7
—	Article 8
Article 6	Article 9
—	Article 10
Article 7(1) and (2)	Article 11(1)
Article 7(3)	Article 11(2)
Article 7(4)	Article 11(3)
Article 7(5)	Article 11(4)
Article 7(6)	Article 11(5)
—	Article 12
—	Article 13
Article 8(1)	Article 14(1)
—	Article 14(2)
Article 8(2)	Article 14(3)
Article 9(1) and (2)	Article 15(1) and (2)
—	Article 15(3)
—	Article 15(4)
—	Article 16
Article 10(1) and (2)	Article 17(1) and (2)
Article 10(3)	Article 24(2)
Article 10(4)	Article 17(3)
—	Article 17(4)
—	Article 17(5)
Article 11	Article 18
Article 12(1)	Article 19(1)
—	Article 19(1)(a)

Regulation (EU) No 1077/2011	This Regulation
—	Article 19((1)(b)
Article 12(1)(a)	Article 19(1)(c)
Article 12(1)(b)	Article 19(1)(d)
Article 12(1)(c)	Article 19(1)(e)
—	Article 19(1)(f)
Article 12(1)(d)	Article 19(1)(g)
—	Article 19(1)(h)
—	Article 19(1)(i)
—	Article 19(1)(j)
—	Article 19(1)(k)
Article 12(1)(e)	Article 19(1)(l)
—	Article 19(1)(m)
Article 12(1)(f)	Article 19(1)(n)
Article 12(1)(g)	Article 19(1)(o)
—	Article 19(1)(p)
Article 12(1)(h)	Article 19(1)(q)
Article 12(1)(i)	Article 19(1)(q)
Article 12(1)(j)	Article 19(1)(r)
—	Article 19(1)(s)
Article 12(1)(k)	Article 19(1)(t)
Article 12(1)(l)	Article 19(1)(u)
Article 12(1)(m)	Article 19(1)(v)
Article 12(1)(n)	Article 19(1)(w)
Article 12(1)(o)	Article 19(1)(x)
—	Article 19(1)(y)
Article 12(1)(p)	Article 19(1)(z)
Article 12(1)(q)	Article 19(1)(bb)
Article 12(1)(r)	Article 19(1)(cc)
Article 12(1)(s)	Article 19(1)(dd)
Article 12(1)(t)	Article 19(1)(ff)
Article 12(1)(u))	Article 19(1)(gg)
Article 12(1)(v)	Article 19(1)(hh)
Article 12(1)(w)	Article 19(1)(ii)
Article 12(1)(x)	Article 19(1)(jj)
—	Article 19(1)(ll)
Article 12(1)(y)	Article 19(1)(mm)
Article 12(1)(z)	Article 19(1)(nn)
—	Article 19(1)(oo)
Article 12(1)(aa)	Article 19(1)(pp)
Article 12(1)(sa)	Article 19(1)(ee)

Regulation (EU) No 1077/2011	This Regulation
Article 12(1)(xa)	Article 19(1)(kk)
Article 12(1)(za)	Article 19(1)(mm)
—	Article 19(1) second subparagraph
—	Article 19(2)
Article 12(2)	Article 19(3)
Article 13(1)	Article 20(1)
Article 13(2) and (3)	Article 20(2)
Article 13(4)	Article 20(3)
Article 13(5)	Article 20(4)
Article 14(1) and (3)	Article 21(1)
Article 14(2)	Article 21(2)
Article 15(1)	Article 22(1) and (3)
Article 15(2)	Article 22(2)
Article 15(3)	Article 22(5)
Article 15(4) and (5)	Article 22(4)
Article 15(6)	Article 22(6)
Article 16(1) to (5)	Article 23(1) to (5)
—	Article 23(6)
Article 16(6)	Article 23(7)
Article 16(7)	Article 23(8)
Article 17(1) and (4)	Article 24(1)
Article 17(2)	—
Article 17(3)	—
Article 17(5) and (6)	Article 24(3)
Article 17(5)(a)	Article 24(3)(a)
Article 17(5)(b)	Article 24(3)(b)
Article 17(5)(c)	Article 24(3)(c)
Article 17(5)(d)	Article 24(3)(o)
Article 17(5)(e)	Article 22(2)
Article 17(5)(f)	Article 19(2)
Article 17(5)(g)	Article 24(3)(p)
Article 17(5)(h)	Article 24(3)(q)
Article 17(6)(a)	Article 24(3)(d) and (g)
Article 17(6)(b)	Article 24(3)(k)
Article 17(6)(c)	Article 24(3)(d)
Article 17(6)(d)	Article 24(3)(l)
Article 17(6)(e)	—
Article 17(6)(f)	—
Article 17(6)(g)	Article 24(3)(r)
Article 17(6)(h)	Article 24(3)(s)

Regulation (EU) No 1077/2011	This Regulation
Article 17(6)(i)	Article 24(3)(t)
Article 17(6)(j)	Article 24(3)(v)
Article 17(6)(k)	Article 24(3)(u)
Article 17(7)	Article 24(4)
—	Article 24(5)
Article 18	Article 25
Article 18(1)	Article 25(1) and (10)
Article 18(2)	Article 25(2), (3) and (4)
Article 18(3)	Article 25(5)
Article 18(4)	Article 25(6)
Article 18(5)	Article 25(7)
Article 18(6)	Article 24(1)
—	Article 25(8)
Article 18(7)	Article 25(9) and (10)
—	Article 25(11)
—	Article 26
Article 19	Article 27
Article 20	Article 28
Article 20(1) and (2)	Article 28(1) and (2)
Article 20(3)	—
Article 20(4)	Article 28(3)
Article 20(5)	Article 28(4)
Article 20(6)	Article 28(5)
Article 20(7)	Article 28(6)
Article 20(8)	Article 28(7)
Article 21	Article 29
Article 22	Article 30
Article 23	Article 31
Article 24	Article 32
Article 25(1) and (2)	Article 33(1) and (2)
—	Article 33(3)
Article 25(3)	Article 33(4)
Articles 26 and 27	Article 34
Article 28(1)	Article 35(1) and Article 36(2)
Article 28(2)	Article 35(2)
—	Article 36(1)
Article 29(1) and (2)	Article 37(1)
Article 29(3)	Article 37(2)
Article 30	Article 38

Regulation (EU) No 1077/2011	This Regulation
Article 31(1)	Article 39(1)
Article 31(2)	Article 39(1) and (3)
—	Article 39(2)
—	Article 40
—	Article 41
—	Article 43
—	Article 44
Article 32(1)	Article 46(3)
Article 32(2)	Article 46(4)
Article 32(3)	Article 46(2)
Article 32(4)	Article 45(2)
Article 32(5)	Article 45(2)
Article 32(6)	Article 44(2)
Article 32(7)	Article 45(3)
Article 32(8)	Article 45(4)
Article 32(9)	Article 45(5) and (6)
Article 32(10)	Article 45(7)
Article 32(11)	Article 45(8)
Article 32(12)	Article 45(9)
Article 33(1) to (4)	Article 47(1) to (4)
—	Article 47(5)
Article 33(5)	Article 47(6)
Article 33(6)	Article 47(7)
Article 33(7)	Article 47(8)
Article 33(8)	Article 47(9)
Article 33(9)	Article 47(10)
Article 33(10)	Article 47(11)
Article 33(11)	Article 47(12)
—	Article 48
Article 34	Article 49
Article 35(1) and (2)	Article 50(1) and (2)
—	Article 50(3)
Article 35(3)	Article 50(4) and (5)
Article 36	—
Article 37	Article 42
—	Article 51
—	Article 52
—	Article 53
—	Article 54

Regulation (EU) No 1077/2011	This Regulation
—	Article 55
—	Article 56
—	Article 57
Article 38	Article 58
—	Annex

REGULATION (EU) 2018/1727 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 November 2018

on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/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 85 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) Eurojust was set up by Council Decision 2002/187/JHA ([2]) as a Union body with legal personality, to stimulate and to improve coordination and cooperation between competent judicial authorities of the Member States, particularly in relation to serious organised crime. Eurojust's legal framework has been amended by Council Decisions 2003/659/JHA ([3]) and 2009/426/JHA ([4]).

(2) Article 85 of the Treaty on the Functioning of the European Union (TFEU) provides for Eurojust to be governed by a regulation, adopted in accordance with the ordinary legislative procedure. It also requires determining arrangements for involving the European Parliament and national parliaments in the evaluation of Eurojust's activities.

(3) Article 85 TFEU also provides that Eurojust's mission is to support and strengthen coordination and cooperation between national investigating and prosecuting authorities in relation to serious crime affecting two or more Member States or requiring prosecution on common bases, on the basis of operations conducted and information supplied by the Member States' authorities and by the European Union Agency for Law Enforcement Cooperation (Europol).

(4) This Regulation aims to amend and expand the provisions of Decision 2002/187/JHA. Since the amendments to be made are of substantial number and nature, Decision 2002/187/JHA should in the interests of clarity be replaced in its entirety in relation to the Member States bound by this Regulation.

(5) As the European Public Prosecutor's Office (EPPO) has been established by means of enhanced cooperation, Council Regulation (EU) 2017/1939 ([5]) is binding in its entirety and directly applicable only to Member States that participate in enhanced cooperation. Therefore, for those Member States which do not participate in the EPPO, Eurojust remains fully competent for forms of serious crime listed in Annex I to this Regulation.

(6) Article 4(3) of the Treaty on European Union (TEU) recalls the principle of sincere cooperation by virtue of which the Union and the Member States are, in full mutual respect, to assist each other in carrying out tasks which flow from the TEU and the TFEU.

(7) In order to facilitate cooperation between Eurojust and the EPPO, Eurojust should address issues of relevance to the EPPO whenever necessary.

(8) In light of the establishment of the EPPO by means of enhanced cooperation, the division of competences between the EPPO and Eurojust with respect to crimes affecting the financial interests of the Union needs to be clearly established. From the date on which the EPPO assumes its tasks, Eurojust should be able to exercise its competence in cases which concern crimes for which the EPPO is competent, where those crimes involve both Member States which participate in enhanced cooperation on the establishment of the EPPO and Member States which do not

([1]) Position of the European Parliament of 4 October 2018 (not yet published in the Official Journal) and decision of the Council of 6 November 2018.

([2]) Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 63, 6.3.2002, p. 1).

([3]) Council Decision 2003/659/JHA of 18 June 2003 amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 245, 29.9.2003, p. 44).

([4]) Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 138, 4.6.2009, p. 14).

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

participate in such enhanced cooperation. In such cases, Eurojust should act at the request of the non-participating Member States or at the request of the EPPO. Eurojust should in any case remain competent for offences affecting the financial interests of the Union whenever the EPPO is not competent or where, although the EPPO is competent, it does not exercise its competence. The Members States which do not participate in enhanced cooperation on the establishment of the EPPO may continue to request Eurojust's support in all cases regarding offences affecting the financial interests of the Union. The EPPO and Eurojust should develop close operational cooperation in line with their respective mandates.

(9) In order for Eurojust to fulfil its mission and develop its full potential in the fight against serious cross-border crime, its operational functions should be strengthened by reducing the administrative workload of national members, and its European dimension enhanced through the Commission's participation in the Executive Board and the increased involvement of the European Parliament and national parliaments in the evaluation of its activities.

(10) Therefore, this Regulation should determine the arrangements for parliamentary involvement, modernising Eurojust's structure and simplifying its current legal framework, while maintaining those elements that have proven to be efficient in its operation.

(11) The forms of serious crime affecting two or more Member States for which Eurojust is competent should be clearly laid down. In addition, cases which do not involve two or more Member States, but which require a prosecution on common bases, should be defined. Such cases may include investigations and prosecutions affecting only one Member State and a third country where an agreement has been concluded with that third country or where there may be a specific need for Eurojust's involvement. Such prosecution may also refer to cases which affect one Member State and have repercussions at Union level.

(12) When exercising its operational functions in relation to concrete criminal cases, at the request of the competent authorities of Member States or on its own initiative, Eurojust should act either through one or more of the national members or as a College. By acting on its own initiative, Eurojust may take a more proactive role in coordinating cases, such as by supporting the national authorities in their investigations and prosecutions. This may include involving Member States that might not initially have been included in the case and discovering links between cases based on the information it receives from Europol, the European Anti-Fraud Office (OLAF), the EPPO and national authorities. This also allows Eurojust to produce guidelines, policy documents and casework-related analyses as part of its strategic work.

(13) At the request of a Member State's competent authority or of the Commission, it should also be possible for Eurojust to assist with investigations involving only that Member State but which have repercussions at Union level. Examples of such investigations include cases where a member of a Union institution or body is involved. Such investigations also cover cases which involve a significant number of Member States and could potentially require a coordinated European response.

(14) The written opinions of Eurojust are not binding on Member States, but should be responded to in accordance with this Regulation.

(15) To ensure Eurojust can support and coordinate cross-border investigations appropriately, it is necessary that all national members have the necessary operational powers with respect to their Member State and in accordance with the law of that Member State in order to cooperate between themselves and with national authorities in a more coherent and effective way. National members should be granted those powers that allow Eurojust to appropriately achieve its mission. Those powers should include accessing relevant information in national public registers, directly contacting and exchanging information with competent authorities and participating in joint investigation teams. National members may, in accordance with their national law, retain the powers which are derived from their capacity as national authorities. In agreement with the competent national authority or in urgent cases, national members may also order investigative measures and controlled deliveries, and issue and execute requests for mutual legal assistance or mutual recognition. Since those powers are to be exercised in accordance with national law, the courts of Member States should be competent to review those measures, in accordance with the requirements and procedures laid down by national law.

(16) It is necessary to provide Eurojust with an administrative and management structure that allows it to perform its tasks more effectively, complies with the principles applicable to Union agencies, and fully respects fundamental rights and freedoms, while maintaining Eurojust's special characteristics and safeguarding its independence in the exercise of its operational functions. To that end, the functions of the national members, the College and the Administrative Director should be clarified and an Executive Board established.

(17) Provisions should be laid down to clearly distinguish between the operational and the management functions of the College, thus reducing the administrative burden on national members to a minimum so that the focus is put on Eurojust's operational work. The management tasks of the College should include in particular the adoption of

Eurojust's work programmes, budget, annual activity report, and working arrangements with partners. The College should exercise the power of appointing authority with respect to the Administrative Director. The College should also adopt Eurojust's rules of procedure. Since those rules of procedure may have an impact on the judicial activities of the Member States, implementing powers should be conferred on the Council to approve those rules.

(18) To improve Eurojust's governance and streamline procedures, an Executive Board should be established to assist the College in its management functions and to allow for streamlined decision-making on non-operational and strategic issues.

(19) The Commission should be represented in the College when the College exercises its management functions. The Commission's representative in the College should be also its representative on the Executive Board, to ensure non-operational supervision of Eurojust and to provide it with strategic guidance.

(20) In order to ensure the efficient day-to-day administration of Eurojust, the Administrative Director should be its legal representative and manager, accountable to the College. The Administrative Director should prepare and implement the decisions of the College and the Executive Board. The Administrative Director should be appointed on the basis of merit, and of his or her documented administrative and managerial skills, as well as relevant competence and experience.

(21) A President and two Vice-Presidents of Eurojust should be elected by the College from among the national members for a term of office of four years. When a national member is elected President, the Member State concerned should be able to second another suitably qualified person to the national desk and to apply for compensation from Eurojust's budget.

(22) Suitably qualified persons are persons who have the necessary qualifications and experience to perform the tasks required to ensure that the national desk functions effectively. They may have the status of a deputy or Assistant to the national member who has been elected President or they may have a more administrative or technical function. Each Member State should be able to decide on its own requirements in this regard.

(23) Quorum and voting procedures should be regulated in Eurojust's rules of procedure. In exceptional cases, where a national member and his or her deputy are absent, the Assistant of the national member concerned should be entitled to vote in the College if the Assistant has the status of a magistrate, i.e. a prosecutor, judge or representative of a judicial authority.

(24) Since the compensation mechanism has a budgetary impact, this Regulation should confer implementing powers to determine that mechanism on the Council.

(25) The setting up of an on-call coordination mechanism within Eurojust is necessary to make Eurojust more efficient and enable it to be available around the clock to intervene in urgent cases. Each Member State should ensure that their representatives in the on-call coordination mechanism are available to act 24 hours a day, seven days a week.

(26) Eurojust national coordination systems should be set up in the Member States to coordinate the work carried out by the national correspondents for Eurojust, the national correspondent for terrorism matters, any national correspondent for issues relating to the competence of the EPPO, the national correspondent for the European Judicial Network and up to three other contact points, as well as representatives in the network for joint investigation teams and representatives in the networks set up by Council Decisions 2002/494/JHA ([1]), 2007/845/JHA ([2]) and 2008/852/JHA ([3]). Member States may decide that one or more of those tasks are to be performed by the same national correspondent.

(27) For the purposes of stimulating and strengthening coordination and cooperation between national investigating and prosecuting authorities, it is crucial that Eurojust receive information from national authorities that is necessary for

([1]) Council Decision 2002/494/JHA of 13 June 2002 setting up a European network of contact points in respect of persons responsible for genocide, crimes against humanity and war crimes (OJ L 167, 26.6.2002, p. 1).

([2]) Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime (OJ L 332, 18.12.2007, p. 103).

([3]) Council Decision 2008/852/JHA of 24 October 2008 on a contact-point network against corruption (OJ L 301, 12.11.2008, p. 38).

the performance of its tasks. To that end, competent national authorities should inform their national members of the setting up and results of joint investigation teams without undue delay. Competent national authorities should also inform national members without undue delay of cases falling under the competence of Eurojust that directly involve at least three Member States and for which requests or decisions on judicial cooperation have been transmitted to at least two Member States. Under certain circumstances, they should also inform national members of conflicts of jurisdiction, controlled deliveries and repeated difficulties in judicial cooperation.

(28) Directive (EU) 2016/680 of the European Parliament and of the Council ([1]) sets out harmonised rules for the protection and the free movement of personal data processed for the purposes of the 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. In order to ensure the same level of protection for natural persons through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between Eurojust and competent authorities in Member States, the rules for the protection and the free movement of operational personal data processed by Eurojust should be consistent with Directive (EU) 2016/680.

(29) The general rules of the distinct Chapter of Regulation (EU) 2018/1725 of the European Parliament and of the Council ([2]) on the processing of operational personal data should apply without prejudice to the specific data protection rules of this Regulation. Such specific rules should be regarded as *lex specialis* to the provisions in that Chapter of Regulation (EU) 2018/1725 (*lex specialis derogat legi generali*). In order to reduce legal fragmentation, specific data protection rules in this Regulation should be consistent with the principles underpinning that Chapter of Regulation (EU) 2018/1725, as well as with the provisions of that Regulation relating to independent supervision, remedies, liability and penalties.

(30) The protection of the rights and freedoms of data subjects requires a clear attribution of responsibilities for data protection under this Regulation. Member States should be responsible for the accuracy of data they have transmitted to Eurojust and which have been processed unaltered by Eurojust, for keeping such data up to date and for the legality of transmitting those data to Eurojust. Eurojust should be responsible for the accuracy of data provided by other data suppliers or resulting from Eurojust's own analyses or data collection and for keeping such data up to date. Eurojust should ensure that data are processed fairly and lawfully, and are collected and processed for a specific purpose. Eurojust should also ensure that the data are adequate, relevant, not excessive in relation to the purpose for which they are processed, stored no longer than is necessary for that purpose, and processed in a manner that ensures appropriate security of personal data and confidentiality of data processing.

(31) Appropriate safeguards for the storage of operational personal data for archiving purposes in the public interest or statistical purposes should be included in Eurojust's rules of procedure.

(32) A data subject should be able to exercise the right of access referred to in Regulation (EU) 2018/1725 to operational personal data relating to him or her which are processed by Eurojust. The data subject may make such a request at reasonable intervals, free of charge, to Eurojust or to the national supervisory authority in the Member State of the data subject's choice.

(33) The data protection provisions of this Regulation are without prejudice to the applicable rules on the admissibility of personal data as evidence in criminal pre-trial and court proceedings.

(34) All processing of personal data by Eurojust, within the framework of its competence, for the fulfilment of its tasks should be considered as processing of operational personal data.

(35) As Eurojust also processes administrative personal data unrelated to criminal investigations, the processing of such data should be subject to the general rules of Regulation (EU) 2018/1725.

([1]) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

([2]) 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 (see page 39 of this Official Journal).

(36) Where operational personal data are transmitted or supplied to Eurojust by the Member State, the competent authority, the national member or the national correspondent for Eurojust should have the right to request rectification or erasure of those operational personal data.

(37) In order to demonstrate compliance with this Regulation, Eurojust or the authorised processor should maintain records regarding all categories of processing activities under its responsibility. Eurojust and each authorised processor should be obliged to cooperate with the European Data Protection Supervisor (the 'EDPS') and to make those records available to it on request, so that they might serve for monitoring those processing operations. Eurojust or its authorised processor, when processing personal data in non-automated processing systems, should have in place effective methods of demonstrating the lawfulness of the processing, of enabling self-monitoring and of ensuring data integrity and data security, such as logs or other forms of records.

(38) The Executive Board of Eurojust should designate a Data Protection Officer who should be a member of the existing staff. The person designated as Data Protection Officer of Eurojust should have received specialised training in data protection law and practice for acquiring expert knowledge in that field. The necessary level of expert knowledge should be determined in relation to the data processing carried out and the protection required for the personal data processed by Eurojust.

(39) The EDPS should be responsible for monitoring and ensuring the complete application of the data protection provisions of this Regulation with regard to processing of operational personal data by Eurojust. The EDPS should be granted powers allowing him or her to fulfil this duty effectively. The EDPS should have the right to consult Eurojust regarding submitted requests, to refer matters to Eurojust for the purpose of addressing concerns that have emerged regarding its processing of operational personal data, to make proposals for improving the protection of the data subjects, and to order Eurojust to carry out specific operations with regard to processing of operational personal data. As a result, the EDPS requires the means to have the orders complied with and executed. He or she should therefore also have the power to warn Eurojust. To warn means to issue an oral or written reminder of Eurojust's obligation to execute the EDPS' orders or to comply with the proposals of the EDPS and a reminder of the measures to be applied upon any non-compliance or refusal by Eurojust.

(40) The duties and powers of the EDPS, including the power to order Eurojust to carry out the rectification, restriction of processing or erasure of operational personal data which have been processed in breach of the data protection provisions contained in this Regulation, should not extend to the personal data contained in national case files.

(41) In order to facilitate cooperation between the EDPS and the national supervisory authorities, but without prejudice to the independence of the EDPS or to his or her responsibility for supervision of Eurojust with regard to data protection, the EDPS and national supervisory authorities should regularly meet within the European Data Protection Board, in line with the rules on coordinated supervision laid down in Regulation (EU) 2018/1725.

(42) As the first recipient on the territory of the Union of data provided by or retrieved from third countries or international organisations, Eurojust should be responsible for the accuracy of such data. Eurojust should take measures to verify as far as possible the accuracy of the data upon receiving the data or when making data available to other authorities.

(43) Eurojust should be subject to the general rules on contractual and non-contractual liability applicable to Union institutions, bodies, offices and agencies.

(44) Eurojust should be able to exchange relevant personal data and maintain cooperative relations with other Union institutions, bodies, offices or agencies to the extent necessary for the fulfilment of its or their tasks.

(45) To guarantee purpose limitation, it is important to ensure that personal data can be transferred by Eurojust to third countries and international organisations only if necessary for preventing and combating crime that falls within Eurojust's tasks. To this end, it is necessary to ensure that, when personal data are transferred, the recipient gives an undertaking that the data will be used by the recipient or transferred onward to a competent authority of a third country solely for the purpose for which they were originally transferred. Further onward transfer of the data should take place in compliance with this Regulation.

(46) All Member States are affiliated to the International Criminal Police Organisation (Interpol). To fulfil its mission, Interpol receives, stores and circulates personal data to assist competent authorities in preventing and combating international crime. It is therefore appropriate to strengthen cooperation between the Union and Interpol by promoting an efficient exchange of personal data while ensuring respect for fundamental rights and freedoms regarding the automatic processing of personal data. Where operational personal data are transferred from Eurojust to Interpol, and to countries which have delegated members to Interpol, this Regulation, in particular the provisions on international transfers, should apply. This Regulation should be without prejudice to the specific rules laid down in Council Common Position 2005/69/JHA ([1]) and Council Decision 2007/533/JHA ([2]).

(47) When Eurojust transfers operational personal data to an authority of a third country or to an international organisation by virtue of an international agreement concluded pursuant to Article 218 TFEU, adequate safeguards should be provided for with respect to the protection of privacy and fundamental rights and freedoms of individuals to ensure that the applicable data protection rules are complied with.

(48) Eurojust should ensure that a transfer to a third country or to an international organisation takes place only if necessary for the 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, and that the controller in the third country or international organisation is an authority competent within the meaning of this Regulation. A transfer should be carried out only by Eurojust acting as controller. Such a transfer may take place in cases where the Commission has decided that the third country or international organisation in question ensures an adequate level of protection, where appropriate safeguards have been provided, or where derogations for specific situations apply.

(49) Eurojust should be able to transfer personal data to an authority of a third country or an international organisation on the basis of a Commission decision finding that the country or international organisation in question ensures an adequate level of data protection ('adequacy decision'), or, in the absence of an adequacy decision, an international agreement concluded by the Union pursuant to Article 218 TFEU, or a cooperation agreement allowing for the exchange of personal data concluded between Eurojust and the third country prior to the date of application of this Regulation.

(50) Where the College identifies an operational need for cooperation with a third country or an international organisation, it should be able to suggest that the Council draw the attention of the Commission to the need for an adequacy decision or for a recommendation for the opening of negotiations on an international agreement pursuant to Article 218 TFEU.

(51) Transfers not based on an adequacy decision should be allowed only where appropriate safeguards have been provided in a legally binding instrument which ensures the protection of personal data or where Eurojust has assessed all the circumstances surrounding the data transfer and, on the basis of that assessment, considers that appropriate safeguards with regard to the protection of personal data exist. Such legally binding instruments could, for example, be legally binding bilateral agreements which have been concluded by the Member States and implemented in their legal order and which could be enforced by their data subjects, ensuring compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress. Eurojust should be able to take into account cooperation agreements concluded between Eurojust and third countries which allow for the exchange of personal data when carrying out the assessment of all the circumstances surrounding the data transfer. Eurojust should be able to also take into account the fact that the transfer of personal data will be subject to confidentiality obligations and the principle of specificity, ensuring that the data will not be processed for other purposes than for the purposes of the transfer. In addition, Eurojust should take into account that the personal data will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment. While those conditions could be considered to be appropriate safeguards allowing the transfer of data, Eurojust should be able to require additional safeguards.

(52) Where no adequacy decision or appropriate safeguards exist, a transfer or a category of transfers could take place only in specific situations, if necessary to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so

([1]) Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol (OJ L 27, 29.1.2005, p. 61).
([2]) Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63).

provides; for the prevention of an immediate and serious threat to the public security of a Member State or a third country; in an individual case for the purposes of the 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; or in an individual case for the establishment, exercise or defence of legal claims. Those derogations should be interpreted restrictively and should not allow frequent, massive and structural transfers of personal data, or large-scale transfers of data, but should be limited to data strictly necessary. Such transfers should be documented and should be made available to the EDPS on request in order to monitor the lawfulness of the transfer.

(53) In exceptional cases, Eurojust should be able to extend the deadlines for the storage of operational personal data in order to achieve its objectives, subject to observance of the purpose limitation principle applicable to processing of personal data in the context of all its activities. Such decisions should be taken following careful consideration of all interests at stake, including those of the data subjects. Any extension of a deadline for processing personal data in cases where prosecution is time-barred in all Member States concerned should be decided only where there is a specific need to provide assistance under this Regulation.

(54) Eurojust should maintain privileged relations with the European Judicial Network based on consultation and complementarity. This Regulation should help clarify the respective roles of Eurojust and the European Judicial Network and their mutual relations, while maintaining the specificity of the European Judicial Network.

(55) Eurojust should maintain cooperative relations with other Union institutions, bodies, offices and agencies, with the EPPO, with the competent authorities of third countries and with international organisations, to the extent required for the fulfilment of its tasks.

(56) To enhance operational cooperation between Eurojust and Europol, and particularly to establish links between data already in the possession of either agency, Eurojust should enable Europol to have access, on the basis of a hit/no-hit system, to data held by Eurojust. Eurojust and Europol should ensure that the necessary arrangements are established to optimise their operational cooperation, taking due account of their respective mandates and any restrictions provided by the Member States. These working arrangements should ensure access to, and the possibility of searching, all information that has been provided to Europol for the purpose of cross-checking in accordance with the specific safeguards and data protection guarantees provided for in this Regulation. Any access by Europol to data held by Eurojust should be limited by technical means to information falling within the respective mandates of those Union agencies.

(57) Eurojust and Europol should keep each other informed of any activity involving the financing of joint investigation teams.

(58) Eurojust should be able to exchange personal data with Union institutions, bodies, offices and agencies to the extent necessary for the fulfilment of its tasks, with full respect for the protection of privacy and other fundamental rights and freedoms.

(59) Eurojust should enhance its cooperation with competent authorities of third countries and international organisations on the basis of a strategy drawn up in consultation with the Commission. For that purpose, provision should be made for Eurojust to post liaison magistrates to third countries in order to achieve objectives similar to those assigned to liaison magistrates seconded by the Member States on the basis of Council Joint Action 96/277/JHA ([1]).

(60) Provision should be made for Eurojust to coordinate the execution of requests for judicial cooperation issued by a third country, where those requests require execution in at least two Member States as part of the same investigation. Eurojust should only undertake such coordination with the agreement of the Member States concerned.

(61) To guarantee the full autonomy and independence of Eurojust, it should be granted an autonomous budget sufficient to properly carry out its work, with revenue coming essentially from a contribution from the budget of the Union, except as regards the salaries and emoluments of the national members, deputies and Assistants, which are borne by their Member State. The Union budgetary procedure should be applicable as far as the Union contribution and other subsidies chargeable to the general budget of the Union are concerned. The auditing of accounts should be undertaken by the Court of Auditors and approved by the Committee on Budgetary Control of the European Parliament.

([1]) Council Joint Action 96/277/JHA of 22 April 1996 concerning a framework for the exchange of liaison magistrates to improve judicial cooperation between the Member States of the European Union (OJ L 105, 27.4.1996, p. 1).

(62) In order to increase the transparency and democratic oversight of Eurojust, it is necessary to provide a mechanism pursuant to Article 85(1) TFEU for the joint evaluation of Eurojust's activities by the European Parliament and national parliaments. The evaluation should take place in the framework of an inter-parliamentary committee meeting in the premises of the European Parliament in Brussels, with the participation of members of the competent committees of the European Parliament and of the national parliaments. The interparliamentary committee meeting should fully respect Eurojust's independence as regards actions to be taken in specific operational cases and as regards the obligation of discretion and confidentiality.

(63) It is appropriate to evaluate the application of this Regulation regularly.

(64) Eurojust's functioning should be transparent in accordance with Article 15(3) TFEU. Specific provisions on how the right of public access to documents is ensured should be adopted by the College. Nothing in this Regulation is intended to restrict the right of public access to documents in so far as it is guaranteed in the Union and in the Member States, in particular under Article 42 of the Charter of Fundamental Rights of the European Union (the 'Charter'). The general rules on transparency that apply to Union agencies should also apply to Eurojust in a way that does not jeopardise in any manner the obligation of confidentiality in its operational work. Administrative inquiries conducted by the European Ombudsman should respect the obligation of confidentiality of Eurojust.

(65) In order to increase Eurojust's transparency vis-à-vis Union citizens and its accountability, Eurojust should publish a list of its Executive Board members on its website and, where appropriate, summaries of the outcome of the meetings of the Executive Board, while respecting data protection requirements.

(66) Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council ([1]) should apply to Eurojust.

(67) Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council ([2]) should apply to Eurojust.

(68) The necessary provisions regarding accommodation for Eurojust in the Member State in which it has its headquarters, that is to say in the Netherlands, and the specific rules applicable to all Eurojust's staff and members of their families should be laid down in a headquarters agreement. The host Member State should provide the best possible conditions to ensure the functioning of Eurojust, including multilingual, European-oriented schooling and appropriate transport connections, so as to attract high-quality human resources from as wide a geographical area as possible.

(69) Eurojust as established by this Regulation should be the legal successor of Eurojust as established by Decision 2002/187/JHA with respect to all its contractual obligations, including employment contracts, liabilities and properties acquired. International agreements concluded by Eurojust as established by that Decision should remain in force.

(70) Since the objective of this Regulation, namely the setting up of an entity responsible for supporting and strengthening coordination and cooperation between judicial authorities of the Member States in relation to serious crime affecting two or more Member States or requiring a prosecution on common bases, cannot be sufficiently achieved by the Member States but can rather, by reason of the scale and effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 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 that objective.

(71) 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, those Member States are not taking part in the adoption of this Regulation and are not bound by it or subject to its application.

([1]) 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).

([2]) 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).

(72) In accordance with Articles 1 and 2 of the Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(73) The EDPS was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council ([1]) and delivered an opinion on 5 March 2014.

(74) This Regulation fully respects the fundamental rights and safeguards and observes the principles recognised in particular by the Charter,

HAVE ADOPTED THIS REGULATION:

CHAPTER I

ESTABLISHMENT, OBJECTIVES AND TASKS OF EUROJUST

Article 1

Establishment of the European Union Agency for Criminal Justice Cooperation

1. The European Union Agency for Criminal Justice Cooperation (Eurojust) is hereby established.

2. Eurojust as established by this Regulation shall replace and succeed Eurojust as established by Decision 2002/187/JHA.

3. Eurojust shall have legal personality.

Article 2

Tasks

1. Eurojust shall support and strengthen coordination and cooperation between national investigating and prosecuting authorities in relation to serious crime which Eurojust is competent to deal with in accordance with Article 3(1) and (3), where that crime affects two or more Member States, or requires prosecution on common bases, on the basis of operations conducted and information supplied by the Member States' authorities, by Europol, by the EPPO and by OLAF.

2. In carrying out its tasks, Eurojust shall:

(a) take into account any request emanating from a competent authority of a Member State, any information provided by Union authorities, institutions, bodies, offices and agencies competent by virtue of provisions adopted within the framework of the Treaties and any information collected by Eurojust itself;

(b) facilitate the execution of requests for, and decisions on, judicial cooperation, including requests and decisions based on instruments that give effect to the principle of mutual recognition.

3. Eurojust shall carry out its tasks at the request of the competent authorities of the Member States, on its own initiative or at the request of the EPPO within the limits of the EPPO's competence.

Article 3

Competence of Eurojust

1. Eurojust shall be competent with respect to the forms of serious crime listed in Annex I. However, as of the date on which the EPPO assumes its investigative and prosecutorial tasks in accordance with Article 120(2) of Regulation (EU) 2017/1939, Eurojust shall not exercise its competence with regard to crimes for which the EPPO exercises its competence, except in those cases where Member States which do not participate in enhanced cooperation on the establishment of the EPPO are also involved and at the request of those Member States or at the request of the EPPO.

2. Eurojust shall exercise its competence for crimes affecting the financial interests of the Union in cases involving Member States which participate in enhanced cooperation on the establishment of the EPPO but in respect of which the EPPO does not have competence or decides not to exercise its competence.

([1]) 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).

Eurojust, the EPPO and the Member States concerned shall consult and cooperate with each other to facilitate Eurojust's exercise of competence under this paragraph. The practical details of its exercise of competence under this paragraph shall be governed by a working arrangement as referred to in Article 47(3).

3. As regards forms of crime other than those listed in Annex I, Eurojust may also, in accordance with its tasks, assist with investigations and prosecutions where requested by a competent authority of a Member State.

4. Eurojust's competence shall cover criminal offences related to the criminal offences listed in Annex I. The following categories of offences shall be regarded as related criminal offences:

(a) criminal offences committed in order to procure the means of committing the serious crimes listed in Annex I;

(b) criminal offences committed in order to facilitate or commit the serious crimes listed in Annex I;

(c) criminal offences committed in order to ensure the impunity of those committing the serious crimes listed in Annex I.

5. At the request of a Member State's competent authority, Eurojust may also assist with investigations and prosecutions that only affect that Member State and a third country, provided that a cooperation agreement or arrangement establishing cooperation pursuant to Article 52 has been concluded with that third country or provided that in a specific case there is an essential interest in providing such assistance.

6. At the request of either the competent authority of a Member State or the Commission, Eurojust may assist in investigations and prosecutions that only affect that Member State but which have repercussions at Union level. Before acting at the request of the Commission, Eurojust shall consult the competent authority of the Member State concerned. That competent authority may, within a deadline set by Eurojust, oppose the execution of the request by Eurojust, justifying its position in every case.

Article 4

Operational functions of Eurojust

1. Eurojust shall:

(a) inform the competent authorities of the Member States of investigations and prosecutions of which it has been informed which have repercussions at Union level or which might affect Member States other than those directly concerned;

(b) assist the competent authorities of the Member States in ensuring the best possible coordination of investigations and prosecutions;

(c) assist in improving cooperation between the competent authorities of the Member States, in particular on the basis of Europol's analyses;

(d) cooperate and consult with the European Judicial Network in criminal matters, including by making use of and contributing to the improvement of the documentary database of the European Judicial Network;

(e) cooperate closely with the EPPO on matters relating to its competence;

(f) provide operational, technical and financial support to Member States' cross-border operations and investigations, including to joint investigation teams;

(g) support, and where appropriate participate in, the Union centres of specialised expertise developed by Europol and other Union institutions, bodies, offices and agencies;

(h) cooperate with Union institutions, bodies, offices and agencies, as well as networks established in the area of freedom, security and justice regulated under Title V of the TFEU;

(i) support Member States' action in combating forms of serious crime listed in Annex I.

2. In carrying out its tasks, Eurojust may ask the competent authorities of the Member States concerned, giving its reasons, to:

(a) undertake an investigation or prosecution of specific acts;

(b) accept that one of them may be in a better position to undertake an investigation or to prosecute specific acts;

(c) coordinate between the competent authorities of the Member States concerned;

(d) set up a joint investigation team in accordance with the relevant cooperation instruments;

(e) provide it with any information that is necessary for carrying out its tasks;

(f) take special investigative measures;

(g) take any other measure justified for the investigation or prosecution.

3. Eurojust may also:

(a) provide Europol with opinions based on analyses carried out by Europol;

(b) supply logistical support, including translation, interpretation and the organisation of coordination meetings.

4. Where two or more Member States cannot agree as to which of them should undertake an investigation or prosecution following a request under points (a) or (b) of paragraph 2, Eurojust shall issue a written opinion on the case. Eurojust shall send the opinion to the Member States concerned immediately.

5. At the request of a competent authority, or on its own initiative, Eurojust shall issue a written opinion on recurrent refusals or difficulties concerning the execution of requests for, and decisions on, judicial cooperation, including requests and decisions based on instruments giving effect to the principle of mutual recognition, provided that it is not possible to resolve such cases through mutual agreement between the competent national authorities or through the involvement of the national members concerned. Eurojust shall send the opinion to the Member States concerned immediately.

6. The competent authorities of the Member States concerned shall respond to requests from Eurojust under paragraph 2 and to the written opinions referred to in paragraph 4 or 5 without undue delay. The competent authorities of the Member States may refuse to comply with such requests or to follow the written opinion if doing so would harm essential national security interests, would jeopardise the success of an ongoing investigation or would jeopardise the safety of an individual.

Article 5

Exercise of operational and other functions

1. Eurojust shall act through one or more of the national members concerned when taking any of the actions referred to in Article 4(1) or (2). Without prejudice to paragraph 2 of this Article, the College shall focus on operational issues and any other issues that are directly linked to operational matters. The College shall only be involved in administrative matters to the extent necessary to ensure that its operational functions are fulfilled.

2. Eurojust shall act as a College:

(a) when taking any of the actions referred to in Article 4(1) or (2):

(i) at the request of one or more of the national members concerned by a case dealt with by Eurojust;

(ii) where the case involves investigations or prosecutions which have repercussions at Union level or which might affect Member States other than those directly concerned;

(b) when taking any of the actions referred to in Article 4(3), (4) or (5);

(c) where a general question relating to the achievement of its operational objectives is involved;

(d) when adopting Eurojust's annual budget, in which case the decision shall be taken by a majority of two thirds of its members;

(e) when adopting the programming document referred to in Article 15 or the annual report on Eurojust's activities, in which cases the decision shall be taken by a majority of two thirds of its members;

(f) when electing or dismissing the President and Vice-Presidents under Article 11;

(g) when appointing the Administrative Director or, where relevant, extending his or her term of office or removing him or her from office under Article 17;

(h) when adopting working arrangements under Articles 47(3) and 52;

(i) when adopting rules for the prevention and management of conflicts of interest in respect of its members, including in relation to their declaration of interests;

(j) when adopting reports, policy papers, guidelines for the benefit of national authorities and opinions pertaining to the operational work of Eurojust, whenever those documents are of a strategic nature;

(k) when appointing liaison magistrates in accordance with Article 53;

(l) when taking any decision which is not expressly attributed to the Executive Board by this Regulation or which is not under the responsibility of the Administrative Director in accordance with Article 18;

(m) when otherwise provided for in this Regulation.

3. When it fulfils its tasks, Eurojust shall indicate whether it is acting through one or more of the national members or as a College.

4. The College may assign additional administrative tasks to the Administrative Director and the Executive Board beyond those provided for in Articles 16 and 18, in accordance with its operational needs.

Where exceptional circumstances so require, the College may decide to suspend temporarily the delegation of the appointing authority powers to the Administrative Director and of those powers that have been sub-delegated by the latter, and to exercise them itself or to delegate them to one of its members or to a staff member other than the Administrative Director.

5. The College shall adopt Eurojust's rules of procedure on the basis of a two-thirds majority of its members. In the event that agreement cannot be reached by a two-thirds majority, the decision shall be taken by simple majority. Eurojust's rules of procedure shall be approved by the Council by means of implementing acts.

CHAPTER II

STRUCTURE AND ORGANISATION OF EUROJUST

SECTION I

Structure

Article 6

Structure of Eurojust

Eurojust shall comprise:

(a) the national members;

(b) the College;

(c) the Executive Board;

(d) the Administrative Director.

SECTION II

National members

Article 7

Status of national members

1. Eurojust shall have one national member seconded by each Member State in accordance with its legal system. That national member shall have his or her regular place of work at the seat of Eurojust.

2. Each national member shall be assisted by one deputy and by one Assistant. In principle, the deputy and the Assistant shall have their regular place of work at the seat of Eurojust. Each Member State may decide that the deputy or Assistant or both will have their regular place of work in their Member State. If a Member State takes such a decision, it shall notify the College. If the operational needs of Eurojust so require, the College may request the Member State to assign the deputy or Assistant or both to work at the seat of Eurojust for a specified period. The Member State shall comply with such a request from the College without undue delay.

3. Additional deputies or Assistants may assist the national member and, if necessary and with the agreement of the College, may have their regular place of work at Eurojust. Member States shall notify Eurojust and the Commission of the appointment of national members, deputies and Assistants.

4. National members and deputies shall have the status of a prosecutor, a judge or a representative of a judicial authority with competences equivalent to those of a prosecutor or judge under their national law. The Member States shall grant them at least the powers referred to in this Regulation in order to be able to fulfil their tasks.

5. The terms of office of the national members and their deputies shall be five years, renewable once. In cases where a deputy is unable to act on behalf of a national member or is unable to substitute for a national member, the national member shall remain in office upon expiry of his or her term of office until the renewal of his or her term or his or her replacement, subject to the consent of their Member State.

6. Member States shall appoint national members and deputies on the basis of a proven high level of relevant, practical experience in the field of criminal justice.

7. The deputy shall be able to act on behalf of or to substitute for the national member. An Assistant may also act on behalf of or substitute for the national member if he or she has a status referred to in paragraph 4.

8. Operational information exchange between Eurojust and Member States shall take place through the national members.

9. The salaries and emoluments of the national members, deputies and Assistants shall be borne by their Member State without prejudice to Article 12.

10. Where national members, deputies and Assistants act within the framework of Eurojust's tasks, the relevant expenditure related to those activities shall be regarded as operational expenditure.

Article 8

Powers of national members

1. The national members shall have the power to:

(a) facilitate or otherwise support the issuing or execution of any request for mutual legal assistance or mutual recognition;

(b) directly contact and exchange information with any competent national authority of the Member State or any other competent Union body, office or agency, including the EPPO;

(c) directly contact and exchange information with any competent international authority, in accordance with the international commitments of their Member State;

(d) participate in joint investigation teams including in setting them up.

2. Without prejudice to paragraph 1, Member States may grant additional powers to national members in accordance with their national law. Those Member States shall notify the Commission and the College of these powers.

3. With the agreement of the competent national authority, national members may, in accordance with their national law:

(a) issue or execute any request for mutual legal assistance or mutual recognition;

(b) order, request or execute investigative measures, as provided for in Directive 2014/41/EU of the European Parliament and of the Council ([1]).

4. In urgent cases where it is not possible to identify or to contact the competent national authority in a timely manner, national members shall be competent to take the measures referred to in paragraph 3 in accordance with their national law, provided that they inform the competent national authority as soon as possible.

5. The national member may submit a proposal to the competent national authority to carry out the measures referred to in paragraphs 3 and 4 where the exercise of the powers referred to in paragraphs 3 and 4 by that national member would be in conflict with:

(a) a Member State's constitutional rules; or

(b) fundamental aspects of that Member State's national criminal justice system regarding:

(i) the division of powers between the police, prosecutors and judges;

([1]) Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130, 1.5.2014, p. 1).

(ii) the functional division of tasks between prosecution authorities; or

(iii) the federal structure of the Member State concerned.

6. Member States shall ensure that, in cases referred to in paragraph 5, the proposal submitted by their national member is handled without undue delay by the competent national authority.

Article 9

Access to national registers

National members shall have access to, or at least be able to obtain the information contained in, the following types of registers of their Member State, in accordance with their national law:

(a) criminal records;

(b) registers of arrested persons;

(c) investigation registers;

(d) DNA registers;

(e) other registers of public authorities of their Member State where such information is necessary to fulfil their tasks.

SECTION III

The College

Article 10

Composition of the College

1. The College shall be composed of:

(a) all the national members; and

(b) one representative of the Commission when the College exercises its management functions.

The representative of the Commission nominated under point (b) of the first subparagraph should be the same person as the Commission's representative on the Executive Board under Article 16(4).

2. The Administrative Director shall attend the management meetings of the College, without the right to vote.

3. The College may invite any person whose opinion may be of interest to attend its meetings as an observer.

4. The members of the College may, subject to the provisions of Eurojust's rules of procedure, be assisted by advisers or experts.

Article 11

The President and Vice-President of Eurojust

1. The College shall elect a President and two Vice-Presidents from among the national members by a two-thirds majority of its members. In the event that a two-thirds majority cannot be reached after the second round of election, the Vice-Presidents shall be elected by a simple majority of the members of the College, while a two-thirds majority shall continue to be necessary for the election of the President.

2. The President shall exercise his or her functions on behalf of the College. The President shall:

(a) represent Eurojust;

(b) call and preside over the meetings of the College and the Executive Board and keep the College informed of any matters that are of interest to it;

(c) direct the work of the College and monitor Eurojust's daily management by the Administrative Director;

(d) exercise any other functions set out in Eurojust's rules of procedure.

3. The Vice-Presidents shall exercise the functions set out in paragraph 2 which the President entrusts to them. They shall replace the President if he or she is prevented from attending to his or her duties. The President and Vice-Presidents shall be assisted in the performance of their specific duties by the administrative staff of Eurojust.

4. The term of office of the President and the Vice-Presidents shall be four years. They may be re-elected once.

5. When a national member is elected President or Vice-President of Eurojust, his or her term of office shall be extended to ensure that he or she can fulfil his or her function as President or Vice-President.

6. If the President or Vice-President no longer fulfils the conditions required for the performance of his or her duties, he or she may be dismissed by the College acting on a proposal from one third of its members. The decision shall be adopted on the basis of a two-thirds majority of the members of the College, excluding the President or Vice-President concerned.

7. When a national member is elected President of Eurojust, the Member State concerned may second another suitably qualified person to reinforce the national desk for the duration of the former's mandate as President.

A Member State which decides to second such a person shall be entitled to apply for compensation in accordance with Article 12.

Article 12

Compensation mechanism for the election to the position of President

1. By 12 December 2019, the Council shall, acting on a proposal by the Commission and by means of implementing acts, determine a mechanism for compensation, for the purpose of Article 11(7), to be made available to Member States whose national member is elected President.

2. The compensation shall be available to any Member State if:

(a) its national member has been elected President; and

(b) it requests compensation from the College and provides justification for the need to reinforce its national desk on grounds of an increased workload.

3. The compensation provided shall equate to 50 % of the national salary of the seconded person. Compensation for living costs and other associated expenses shall be provided on a comparable basis to that provided to Union officials or other servants seconded abroad.

4. The costs of the compensation mechanism shall be borne by Eurojust's budget.

Article 13

Meetings of the College

1. The President shall convene the meetings of the College.

2. The College shall hold at least one meeting per month. In addition, it shall meet on the initiative of the President, at the request of the Commission to discuss the administrative tasks of the College, or at the request of at least one third of its members.

3. Eurojust shall send the EPPO the agenda of College meetings whenever issues are discussed which are of relevance for the exercise of the tasks of the EPPO. Eurojust shall invite the EPPO to participate in such meetings, without the right to vote. When the EPPO is invited to a College meeting, Eurojust shall provide it with the relevant documents supporting the agenda.

Article 14

Voting rules of the College

1. Unless stated otherwise, and where a consensus cannot be reached, the College shall take its decisions by a majority of its members.

2. Each member shall have one vote. In the absence of a voting member, the deputy shall be entitled to exercise the right to vote subject to the conditions set out in Article 7(7). In the absence of the deputy, the Assistant shall also be entitled to exercise the right to vote subject to the conditions set out in Article 7(7).

Article 15

Annual and multi-annual programming

1. By 30 November each year, the College shall adopt a programming document containing annual and multi-annual programming, based on a draft prepared by the Administrative Director, taking into account the opinion of the Commission. The College shall forward the programming document to the European Parliament, the Council, the Commission and the EPPO. The programming document shall become definitive after final adoption of the general budget of the Union and shall be adjusted accordingly, if necessary.

2. 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 multi-annual work programme referred to in paragraph 4. It shall clearly indicate which tasks have been added, changed or deleted in comparison with the previous financial year.

3. The College shall amend the adopted annual work programme when a new task is given to Eurojust. Any substantial amendment to the annual work programme shall be adopted by the same procedure as the initial annual work programme. The College may delegate to the Administrative Director the power to make non-substantial amendments to the annual work programme.

4. The multi-annual work programme shall set out overall strategic programming including objectives, the strategy for cooperation with the authorities of third countries and international organisations referred to in Article 52, expected results and performance indicators. It shall also set out resource programming including multi-annual budget and staff. The resource programming shall be updated annually. The strategic programming shall be updated where appropriate, and in particular to address the outcome of the evaluation referred to in Article 69.

SECTION IV

The executive board

Article 16

Functioning of the Executive Board

1. The College shall be assisted by an Executive Board. The Executive Board shall be responsible for taking administrative decisions to ensure the proper functioning of Eurojust. It shall oversee the necessary preparatory work of the Administrative Director on other administrative matters for adoption by the College. It shall not be involved in the operational functions of Eurojust referred to in Articles 4 and 5.

2. The Executive Board may consult the College when carrying out its tasks.

3. The Executive Board shall also:

(a) review Eurojust's programming document referred to in Article 15 based on the draft prepared by the Administrative Director and forward it to the College for adoption;

(b) adopt an anti-fraud strategy for Eurojust, proportionate to the fraud risks, taking into account the costs and benefits of the measures to be implemented and based on a draft prepared by the Administrative Director;

(c) adopt appropriate implementing rules giving effect to the Staff Regulations of Officials of the European Union (the 'Staff Regulations of Officials') and the Conditions of Employment of Other Servants of the European Union ('Conditions of Employment of Other Servants'), laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68 ([1]) in accordance with Article 110 of the Staff Regulations of Officials;

(d) ensure adequate follow-up to the findings and recommendations stemming from the internal or external audit reports, evaluations and investigations, including those of the EDPS and OLAF;

(e) take all decisions on the establishment and, where necessary, the modification of Eurojust's internal administrative structures;

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

(f) without prejudice to the responsibilities of the Administrative Director set out in Article 18, assist and advise him or her on the implementation of the decisions of the College, with a view to reinforcing supervision of administrative and budgetary management;

(g) undertake any additional administrative tasks assigned to it by the College under Article 5(4);

(h) adopt the financial rules applicable to Eurojust in accordance with Article 64;

(i) adopt, in accordance with Article 110 of the Staff Regulations of Officials, a decision based on Article 2(1) of the Staff Regulations of Officials and on Article 6 of the Conditions of Employment of Other Servants delegating the relevant appointing authority powers to the Administrative Director and establishing the conditions under which this delegation of powers can be suspended; the Administrative Director shall be authorised to sub-delegate those powers;

(j) review Eurojust's draft annual budget for adoption by the College;

(k) review the draft annual report on Eurojust's activities and forward it to the College for adoption;

(l) appoint an accounting officer and a Data Protection Officer who are functionally independent in the performance of their duties.

4. The Executive Board shall be composed of the President and Vice-Presidents of Eurojust, one representative of the Commission and two other members of the College designated on a two-year rotation system in accordance with Eurojust's rules of procedure. The Administrative Director shall attend the meetings of the Executive Board without the right to vote.

5. The President of Eurojust shall be the chairperson of the Executive Board. The Executive Board shall take its decisions by a majority of its members. Each member shall have one vote. In the event of a tied vote, the President of Eurojust shall have a casting vote.

6. The term of office of members of the Executive Board shall end when their term as national members, President or Vice-President ends.

7. The Executive Board shall meet at least once a month. In addition, it shall meet on the initiative of its chairperson or at the request of the Commission or of at least two of its other members.

8. Eurojust shall send to the EPPO the agenda of the Executive Board meetings and consult with the EPPO on the need to participate in those meetings. Eurojust shall invite the EPPO to participate, without the right to vote, whenever issues are discussed which are of relevance for the functioning of the EPPO.

When the EPPO is invited to an Executive Board meeting, Eurojust shall provide it with the relevant documents supporting the agenda.

SECTION V

The Administrative Director

Article 17

Status of the Administrative Director

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

2. The Administrative Director shall be appointed by the College from a list of candidates proposed by the Executive Board, following an open and transparent selection procedure in accordance with Eurojust's rules of procedure. For the purpose of concluding the employment contract with the Administrative Director, Eurojust shall be represented by the President of Eurojust.

3. The term of office of the Administrative Director shall be four years. By the end of that period, the Executive Board shall undertake an assessment that takes into account an evaluation of the performance of the Administrative Director.

4. The College, acting on a proposal from the Executive Board that takes into account the assessment referred to in paragraph 3, may extend the term of office of the Administrative Director once and for no more than four years.

5. An Administrative Director whose term of office has been extended shall not participate in another selection procedure for the same post at the end of the overall period.

6. The Administrative Director shall be accountable to the College.

7. The Administrative Director may be removed from the office only pursuant to a decision of the College acting on a proposal from the Executive Board.

Article 18

Responsibilities of the Administrative Director

1. For administrative purposes, Eurojust shall be managed by its Administrative Director.

2. Without prejudice to the powers of the College or the Executive Board, the Administrative Director shall be independent in the performance of his or her duties and shall neither seek nor take instructions from any government or any other body.

3. The Administrative Director shall be the legal representative of Eurojust.

4. The Administrative Director shall be responsible for the implementation of the administrative tasks assigned to Eurojust, in particular:

(a) the day-to-day administration of Eurojust and staff management;

(b) implementing the decisions adopted by the College and the Executive Board;

(c) preparing the programming document referred to in Article 15 and submitting it to the Executive Board for review;

(d) implementing the programming document referred to in Article 15 and reporting to the Executive Board and College on its implementation;

(e) preparing the annual report on Eurojust's activities and presenting it to the Executive Board for review and to the College for adoption;

(f) preparing an action plan following up on conclusions of internal or external audit reports, evaluations and investigations, including those of the EDPS and OLAF and reporting on progress twice a year to the College, to the Executive Board, to the Commission and to the EDPS;

(g) preparing an anti-fraud strategy for Eurojust and presenting it to the Executive Board for adoption;

(h) preparing draft financial rules applicable to Eurojust;

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

(j) exercising, with respect to the staff of Eurojust, the powers conferred by the Staff Regulations of Officials on the appointing authority and by the Conditions of Employment of Other Servants on the authority empowered to conclude contracts of employment of other servants ('the appointing authority powers');

(k) ensuring that the necessary administrative support is provided to facilitate the operational work of Eurojust;

(l) ensuring that support is provided to the President and Vice-Presidents as they carry out their duties;

(m) preparing a draft proposal for Eurojust's annual budget, which shall be reviewed by the Executive Board before adoption by the College.

CHAPTER III

OPERATIONAL MATTERS

Article 19

On-call coordination mechanism

1. In order to fulfil its tasks in urgent cases, Eurojust shall operate an on-call coordination mechanism ('OCC') able to receive and process at all times the requests referred to it. The OCC shall be contactable 24 hours a day, seven days a week.

2. The OCC shall rely on one OCC representative per Member State who may be either the national member, his or her deputy, an Assistant entitled to replace the national member, or a seconded national expert. The OCC representative shall be available to act 24 hours a day, seven days a week.

3. The OCC representatives shall act efficiently and without delay in relation to the execution of a request in their Member State.

Article 20

Eurojust national coordination system

1. Each Member State shall appoint one or more national correspondents for Eurojust.

2. All national correspondents appointed by the Member States under paragraph 1 shall have the skills and experience necessary for them to carry out their duties.

3. Each Member State shall set up a Eurojust national coordination system to ensure coordination of the work carried out by:

(a) the national correspondents for Eurojust;

(b) any national correspondents for issues relating to the competence of the EPPO;

(c) the national correspondent for Eurojust for terrorism matters;

(d) the national correspondent for the European Judicial Network in criminal matters and up to three other contact points of the European Judicial Network;

(e) national members or contact points of the Network for joint investigation teams, and national members or contact points of the networks set up by Decisions 2002/494/JHA, 2007/845/JHA and 2008/852/JHA;

(f) where applicable, any other relevant judicial authority.

4. The persons referred to in paragraphs 1 and 3 shall retain their position and status under national law, without this having a significant impact on the performance of their duties under this Regulation.

5. The national correspondents for Eurojust shall be responsible for the functioning of their Eurojust national coordination system. Where several correspondents for Eurojust are appointed, one of them shall be responsible for the functioning of their Eurojust national coordination system.

6. The national members shall be informed of all meetings of their Eurojust national coordination system where casework-related matters are discussed. The national members may attend such meetings as necessary.

7. Each Eurojust national coordination system shall facilitate the carrying out of Eurojust's tasks within the Member State concerned, in particular by:

(a) ensuring that the case management system referred to in Article 23 receives information related to the Member State concerned in an efficient and reliable manner;

(b) assisting in determining whether a request should be handled with the assistance of Eurojust or of the European Judicial Network;

(c) assisting the national member in identifying relevant authorities for the execution of requests for, and decisions on, judicial cooperation, including requests and decisions based on instruments giving effect to the principle of mutual recognition;

(d) maintaining close relations with the Europol national unit, other contact points of the European Judicial Network and other relevant competent national authorities.

8. In order to meet the objectives referred to in paragraph 7, the persons referred to in paragraph 1 and in points (a), (b) and (c) of paragraph 3 shall, and the persons or authorities referred to in points (d) and (e) of paragraph 3 may be connected to the case management system in accordance with this Article and with Articles 23, 24, 25 and 34. The cost of connection to the case management system shall be borne by the general budget of the Union.

9. The setting up of the Eurojust national coordination system and the appointment of national correspondents shall not prevent direct contacts between the national member and the competent authorities of his or her Member State.

Article 21

Exchanges of information with the Member States and between national members

1. The competent authorities of the Member States shall exchange with Eurojust all information necessary for the performance of its tasks under Articles 2 and 4 in accordance with the applicable data protection rules. This shall at least include the information referred to in paragraphs 4, 5 and 6 of this Article.

2. The transmission of information to Eurojust shall only be interpreted as a request for the assistance of Eurojust in the case concerned if so specified by a competent authority.

3. The national members shall exchange all information necessary for the performance of Eurojust's tasks among themselves or with their competent national authorities, without prior authorisation. In particular, the competent national authorities shall promptly inform their national members of a case which concerns them.

4. The competent national authorities shall inform their national members of the setting up of joint investigation teams and of the results of the work of such teams.

5. The competent national authorities shall inform their national members without undue delay of any case affecting at least three Member States for which requests for or decisions on judicial cooperation, including requests and decisions based on instruments giving effect to the principle of mutual recognition, have been transmitted to at least two Member States, where one or more of the following apply:

(a) the offence involved is punishable in the requesting or issuing Member State by a custodial sentence or a detention order, the maximum period of which is at least five or six years, to be decided by the Member State concerned, and is included in the following list:

  (i) trafficking in human beings;

  (ii) sexual abuse or sexual exploitation including child pornography and solicitation of children for sexual purposes;

  (iii) drug trafficking;

  (iv) illicit trafficking in firearms, their parts or components or ammunition or explosives;

  (v) corruption;

  (vi) crime against the financial interests of the Union;

  (vii) forgery of money or means of payment;

  (viii) money laundering activities;

  (ix) computer crime;

(b) there are factual indications that a criminal organisation is involved;

(c) there are indications that the case may have a serious cross-border dimension or may have repercussions at Union level, or that it may affect Member States other than those directly involved.

6. The competent national authorities shall inform their national members of:

(a) cases in which conflicts of jurisdiction have arisen or are likely to arise;

(b) controlled deliveries affecting at least three countries, at least two of which are Member States;

(c) repeated difficulties or refusals regarding the execution of requests for, or decisions on, judicial cooperation, including requests and decisions based on instruments giving effect to the principle of mutual recognition.

7. The competent national authorities shall not be obliged to supply information in a particular case if doing so would harm essential national security interests or jeopardise the safety of individuals.

8. This Article is without prejudice to conditions set out in bilateral or multilateral agreements or arrangements between Member States and third countries, including any conditions set by third countries concerning the use of information once supplied.

9. This Article is without prejudice to other obligations regarding the transmission of information to Eurojust, including Council Decision 2005/671/JHA ([1]).

10. Information referred to in this Article shall be provided in a structured way determined by Eurojust. The competent national authority shall not be obliged to provide such information where it has already been transmitted to Eurojust in accordance with other provisions of this Regulation.

Article 22

Information provided by Eurojust to competent national authorities

1. Eurojust shall provide competent national authorities with information on the results of the processing of information, including the existence of links with cases already stored in the case management system, without undue delay. That information may include personal data.

2. Where a competent national authority requests that Eurojust provide it with information within a certain timeframe, Eurojust shall transmit that information within that timeframe.

Article 23

Case management system, index and temporary work files

1. Eurojust shall establish a case management system composed of temporary work files and of an index which contain the personal data referred to in Annex II and non-personal data.

2. The purpose of the case management system shall be to:

(a) support the management and coordination of investigations and prosecutions for which Eurojust is providing assistance, in particular by cross-referencing information;

(b) facilitate access to information on on-going investigations and prosecutions;

(c) facilitate the monitoring of the lawfulness of Eurojust's processing of personal data and its compliance with the applicable data protection rules.

3. The case management system may be linked to the secure telecommunications connection referred to in Article 9 of Council Decision 2008/976/JHA ([2]).

4. The index shall contain references to temporary work files processed within the framework of Eurojust and may not contain any personal data other than those referred to in points (1)(a) to (i), (k) and (m) and (2) of Annex II.

5. In the performance of their duties, national members may process data on the individual cases on which they are working in a temporary work file. They shall allow the Data Protection Officer to have access to the temporary work file. The Data Protection Officer shall be informed by the national member concerned of the opening of each new temporary work file that contains personal data.

6. For the processing of operational personal data, Eurojust may not establish any automated data file other than the case management system. The national member may, however, temporarily store and analyse personal data for the purpose of determining whether such data are relevant to Eurojust's tasks and can be included in the case management system. That data may be held for up to three months.

Article 24

Functioning of temporary work files and the index

1. A temporary work file shall be opened by the national member concerned for every case with respect to which information is transmitted to him or her in so far as that transmission is in accordance with this Regulation or other applicable legal instruments. The national member shall be responsible for the management of the temporary work files opened by that national member.

([1]) Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences (OJ L 253, 29.9.2005, p. 22).

([2]) Council Decision 2008/976/JHA of 16 December 2008 on the European Judicial Network (OJ L 348, 24.12.2008, p. 130).

2. The national member who has opened a temporary work file shall decide, on a case-by-case basis, whether to keep the temporary work file restricted or to give access to it or to parts of it to other national members, to authorised Eurojust staff or to any other person working on behalf of Eurojust who has received the necessary authorisation from the Administrative Director.

3. The national member who has opened a temporary work file shall decide which information related to that temporary work file shall be introduced in the index in accordance with Article 23(4).

Article 25

Access to the case management system at national level

1. In so far as they are connected to the case management system, persons referred to in Article 20(3) shall only have access to:

(a) the index, unless the national member who has decided to introduce the data in the index expressly denied such access;

(b) temporary work files opened by the national member of their Member State;

(c) temporary work files opened by national members of other Member States and to which the national member of their Member States has received access, unless the national member who opened the temporary work file expressly denied such access.

2. The national member shall, within the limitations provided for in paragraph 1 of this Article, decide on the extent of access to the temporary work files which is granted in his or her Member State to the persons referred to in Article 20(3) in so far as they are connected to the case management system.

3. Each Member State shall decide, after consultation with its national member, on the extent of access to the index which is granted in that Member State to the persons referred to in Article 20(3) in so far as they are connected to the case management system. Member States shall notify Eurojust and the Commission of their decision regarding the implementation of this paragraph. The Commission shall inform the other Member States thereof.

4. Persons who have been granted access in accordance with paragraph 2 shall at least have access to the index to the extent necessary to access the temporary work files to which they have been granted access.

CHAPTER IV

PROCESSING OF INFORMATION

Article 26

Processing of personal data by Eurojust

1. This Regulation and Article 3 and Chapter IX of Regulation (EU) 2018/1725 shall apply to the processing of operational personal data by Eurojust. Regulation (EU) 2018/1725 shall apply to the processing of administrative personal data by Eurojust, with the exception of Chapter IX of that Regulation.

2. References to 'applicable data protection rules' in this Regulation shall be understood as references to the provisions on data protection set out in this Regulation and in Regulation (EU) 2018/1725.

3. The data protection rules on processing of operational personal data contained in this Regulation shall be considered as specific data protection rules to the general rules laid down in Article 3 and Chapter IX of Regulation (EU) 2018/1725.

4. Eurojust shall determine the time limits for the storage of administrative personal data in the data protection provisions of its rules of procedure.

Article 27

Processing of operational personal data

1. In so far as it is necessary to perform its tasks, Eurojust may, within the framework of its competence and in order to carry out its operational functions, process by automated means or in structured manual files in accordance with this Regulation only the operational personal data listed in point 1 of Annex II of persons who, under the national law of the Member States concerned, are persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence in respect of which Eurojust is competent or who have been convicted of such an offence.

2. Eurojust may process only the operational personal data listed in point 2 of Annex II of persons who, under the national law of the Member States concerned, are regarded as victims or other parties to a criminal offence, such as persons who might be called to testify in a criminal investigation or prosecution regarding one or more of the types of crime and the criminal offences referred to in Article 3, persons who are able to provide information on criminal offences, or contacts or associates of a person referred to in paragraph 1. The processing of such operational personal data may only take place if it is necessary for the fulfilment of the tasks of Eurojust, within the framework of its competence and in order to carry out its operational functions.

3. In exceptional cases, for a limited period of time which shall not exceed the time needed for the conclusion of the case in relation to which the data are processed, Eurojust may also process operational personal data other than the personal data referred to in Annex II relating to the circumstances of an offence, where such data are immediately relevant to and are included in ongoing investigations which Eurojust is coordinating or helping to coordinate and when their processing is necessary for the purposes specified in paragraph 1. The Data Protection Officer referred to in Article 36 shall be informed immediately when such operational personal data are processed, and shall be informed of the specific circumstances which justify the necessity of the processing of those operational personal data. Where such other data refer to witnesses or victims within the meaning of paragraph 2 of this Article, the decision to process them shall be taken jointly by the national members concerned.

4. Eurojust may process special categories of operational personal data in accordance with Article 76 of Regulation (EU) 2018/1725. Such data may not be processed in the index referred to in Article 23(4) of this Regulation. Where such other data refer to witnesses or victims within the meaning of paragraph 2 of this Article, the decision to process them shall be taken by the national members concerned.

Article 28

Processing under the authority of Eurojust or processor

The processor and any person acting under the authority of Eurojust or of the processor who has access to operational personal data shall not process those data except on instructions from Eurojust, unless required to do so by Union law or Member State law.

Article 29

Time limits for the storage of operational personal data

1. Operational personal data processed by Eurojust shall be stored by Eurojust for only as long as is necessary for the performance of its tasks. In particular, without prejudice to paragraph 3 of this Article, the operational personal data referred to in Article 27 may not be stored beyond the first applicable date among the following dates:

(a) the date on which prosecution is barred under the statute of limitations of all the Member States concerned by the investigation and prosecutions;

(b) the date on which Eurojust is informed that the person has been acquitted and the judicial decision became final, in which case the Member State concerned shall inform Eurojust without delay;

(c) three years after the date on which the judicial decision of the last of the Member States concerned by the investigation or prosecution became final;

(d) the date on which Eurojust and the Member States concerned mutually established or agreed that it was no longer necessary for Eurojust to coordinate the investigation and prosecutions, unless there is an obligation to provide Eurojust with this information in accordance with Article 21(5) or (6);

(e) three years after the date on which operational personal data were transmitted in accordance with Article 21(5) or (6).

2. Observance of the storage deadlines referred to in paragraph 1 of this Article shall be reviewed constantly by appropriate automated processing conducted by Eurojust, particularly from the moment in which the case is closed by Eurojust. A review of the need to store the data shall also be carried out every three years after they were entered; the results of such reviews shall apply to the case as a whole. If operational personal data referred to in Article 27(4) are stored for a period exceeding five years, the EDPS shall be informed.

3. Before one of the storage deadlines referred to in paragraph 1 expires, Eurojust shall review the need for the continued storage of the operational personal data where and as long as this is necessary to perform its tasks. It may decide by way of derogation to store those data until the following review. The reasons for the continued storage shall be justified and recorded. If no decision is taken on the continued storage of operational personal data at the time of the review, those data shall be deleted automatically.

4. Where, in accordance with paragraph 3, operational personal data have been stored beyond the storage deadlines referred to in paragraph 1, the EDPS shall also carry out a review of the need to store those data every three years.

5. Once the deadline for the storage of the last item of automated data from the file has expired, all documents in the file shall be destroyed with the exception of any original documents which Eurojust has received from national authorities and which need to be returned to their provider.

6. Where Eurojust has coordinated an investigation or prosecutions, the national members concerned shall inform each other whenever they receive information that the case has been dismissed or that all judicial decisions related to the case have become final.

7. Paragraph 5 shall not apply where:

(a) this would damage the interests of a data subject who requires protection; in such cases, the operational personal data shall be used only with the express and written consent of the data subject;

(b) the accuracy of the operational personal data is contested by the data subject; in such cases paragraph 5 shall not apply for a period enabling Member States or Eurojust, as appropriate, to verify the accuracy of such data;

(c) the operational personal data are to be maintained for purposes of proof or for the establishment, exercise or defence of legal claims;

(d) the data subject opposes the erasure of the operational personal data and requests the restriction of their use instead; or

(e) the operational personal data are further needed for archiving purposes in the public interest or statistical purposes.

Article 30

Security of operational personal data

Eurojust and Member States shall define mechanisms to ensure that the security measures referred to in Article 91 of Regulation (EU) 2018/1725 are addressed across information system boundaries.

Article 31

Right of access by the data subject

1. Any data subject who wishes to exercise the right of access referred to in Article 80 of Regulation (EU) 2018/1725 to operational personal data that relate to the data subject and which have been processed by Eurojust may make a request to Eurojust or to the national supervisory authority in the Member State of the data subject's choice. That authority shall refer the request to Eurojust without delay, and in any case within one month of its receipt.

2. The request shall be answered by Eurojust without undue delay and in any case within three months of its receipt by Eurojust.

3. The competent authorities of the Member States concerned shall be consulted by Eurojust on the decision to be taken in response to a request. The decision on access to data shall only be taken by Eurojust in close cooperation with the Member States directly concerned by the communication of such data. Where a Member State objects to Eurojust's proposed decision, it shall notify Eurojust of the reasons for its objection. Eurojust shall comply with any such objection. The national members concerned shall subsequently notify the competent authorities of the content of Eurojust's decision.

4. The national members concerned shall deal with the request and reach a decision on Eurojust's behalf. Where the national members concerned are not in agreement, they shall refer the matter to the College, which shall take its decision on the request by a two-thirds majority.

Article 32

Limitations to the right of access

In the cases referred to in Article 81 of Regulation (EU) 2018/1725, Eurojust shall inform the data subject after consulting the competent authorities of the Member States concerned in accordance with Article 31(3) of this Regulation.

Article 33

Right to restriction of processing

Without prejudice to the exceptions set out in Article 29(7) of this Regulation, where the processing of operational personal data has been restricted under Article 82(3) of Regulation (EU) 2018/1725, such operational personal data shall only be processed for the protection of the rights of the data subject or another natural or legal person who is a party to the proceedings to which Eurojust is a party, or for the purposes laid down in Article 82(3) of Regulation (EU) 2018/1725.

Article 34

Authorised access to operational personal data within Eurojust

Only national members, their deputies, their Assistants and authorised seconded national experts, the persons referred to in Article 20(3) in so far as those persons are connected to the case management system and authorised Eurojust staff may, for the purpose of achieving Eurojust's tasks, have access to operational personal data processed by Eurojust within the limits provided for in Articles 23, 24 and 25.

Article 35

Records of categories of processing activities

1. Eurojust shall maintain a record of all categories of processing activities under its responsibility. That record shall contain all of the following information:

(a) Eurojust's contact details and the name and the contact details of its Data Protection Officer;

(b) the purposes of the processing;

(c) the description of the categories of data subjects and of the categories of operational personal data;

(d) the categories of recipients to whom the operational personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of operational personal data to a third country or an international organisation, including the identification of that third country or international organisation;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 91 of Regulation (EU) 2018/1725.

2. The records referred to in paragraph 1 shall be in writing, including in electronic form.

3. Eurojust shall make the record available to the EDPS on request.

Article 36

Designation of the Data Protection Officer

1. The Executive Board shall designate a Data Protection Officer. The Data Protection Officer shall be a member of staff specifically appointed for this purpose. In the performance of his or her duties, the Data Protection Officer shall act independently and may not receive any instructions.

2. The Data Protection Officer shall be selected on the basis of his or her professional qualities and, in particular, expert knowledge of data protection law and practice, and ability to fulfil his or her tasks under this Regulation, in particular those referred to in Article 38.

3. The selection of the Data Protection Officer shall not be liable to result in a conflict of interests between his or her duty as Data Protection Officer and any other official duties he or she may have, in particular in relation to the application of this Regulation.

4. The Data Protection Officer shall be appointed for a term of four years and shall be eligible for reappointment up to a maximum total term of eight years. The Data Protection Officer may be dismissed from his or her post by the Executive Board only with the agreement of the EDPS, if he or she no longer fulfils the conditions required for the performance of his or her duties.

5. Eurojust shall publish the contact details of the Data Protection Officer and communicate them to the EDPS.

Article 37

Position of the Data Protection Officer

1. Eurojust shall ensure that the Data Protection Officer is involved properly and in a timely manner in all issues which relate to the protection of personal data.

2. Eurojust shall support the Data Protection Officer in performing the tasks referred to in Article 38 by providing the resources and staff necessary to carry out those tasks and by providing access to personal data and processing operations, and to maintain his or her expert knowledge.

3. Eurojust shall ensure that the Data Protection Officer does not receive any instructions regarding the carrying out of his or her tasks. The Data Protection Officer shall not be dismissed or penalised by the Executive Board for performing his or her tasks. The Data Protection Officer shall report directly to the College in relation to operational personal data and report to the Executive Board in relation to administrative personal data.

4. Data subjects may contact the Data Protection Officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation and under Regulation (EU) 2018/1725.

5. The Executive Board shall adopt implementing rules concerning the Data Protection Officer. Those implementing rules shall in particular concern the selection procedure for the position of the Data Protection Officer, his or her dismissal, tasks, duties and powers, and safeguards for the independence of the Data Protection Officer.

6. The Data Protection Officer and his or her staff shall be bound by the obligation of confidentiality in accordance with Article 72.

7. The Data Protection Officer may be consulted by the controller and the processor, by the staff committee concerned and by any individual on any matter concerning the interpretation or application of this Regulation and Regulation (EU) 2018/1725 without them going through the official channels. No one shall suffer prejudice on account of a matter brought to the attention of the Data Protection Officer alleging that a breach of this Regulation or Regulation (EU) 2018/1725 has taken place.

8. After his or her designation the Data Protection Officer shall be registered with the EDPS by Eurojust.

Article 38

Tasks of the Data Protection Officer

1. The Data Protection Officer shall in particular have the following tasks regarding the processing of personal data:

(a) ensuring in an independent manner the compliance of Eurojust with the data protection provisions of this Regulation and Regulation (EU) 2018/1725 and with the relevant data protection provisions in Eurojust's rules of procedure; this includes monitoring compliance with this Regulation, with Regulation (EU) 2018/1725, with other Union or national data protection provisions and with the policies of Eurojust in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and related audits;

(b) informing and advising Eurojust and staff who process personal data of their obligations pursuant to this Regulation, to Regulation (EU) 2018/1725 and to other Union or national data protection provisions;

(c) providing advice where requested as regards the data protection impact assessment and monitoring its performance pursuant to Article 89 of Regulation (EU) 2018/1725;

(d) ensuring that a record of the transfer and receipt of personal data is kept in accordance with the provisions to be laid down in Eurojust's rules of procedure;

(e) cooperating with the staff of Eurojust who are responsible for procedures, training and advice concerning data processing;

(f) cooperating with the EDPS;

(g) ensuring that data subjects are informed of their rights under this Regulation and Regulation (EU) 2018/1725;

(h) acting as the contact point for the EDPS on issues relating to processing, including the prior consultation referred to in Article 90 of Regulation (EU) 2018/1725, and consulting where appropriate, with regard to any other matter;

(i) providing advice where requested as regards the necessity of a notification or communication of a personal data breach pursuant to Articles 92 and 93 of Regulation (EU) 2018/1725;

(j) preparing an annual report and communicating that report to the Executive Board, to the College and to the EDPS.

2. The Data Protection Officer shall carry out the functions provided for in Regulation (EU) 2018/1725 with regard to administrative personal data.

3. The Data Protection Officer and the staff members of Eurojust assisting the Data Protection Officer in the performance of his or her duties shall have access to the personal data processed by Eurojust and to its premises, to the extent necessary for the performance of their tasks.

4. If the Data Protection Officer considers that the provisions of Regulation (EU) 2018/1725 related to the processing of administrative personal data or that the provisions of this Regulation or of Article 3 and of Chapter IX of Regulation (EU) 2018/1725 related to the processing of operational personal data have not been complied with, he or she shall inform the Executive Board, requesting that it resolve the non-compliance within a specified time. If the Executive Board does not resolve the non-compliance within the specified time, the Data Protection Officer shall refer the matter to the EDPS.

Article 39

Notification of a personal data breach to the authorities concerned

1. In the event of a personal data breach, Eurojust shall without undue delay notify the competent authorities of the Member States concerned of that breach.

2. The notification referred to in paragraph 1 shall, as a minimum:

(a) describe the nature of the personal data breach including, where possible and appropriate, the categories and number of data subjects concerned and the categories and number of data records concerned;

(b) describe the likely consequences of the personal data breach;

(c) describe the measures proposed or taken by Eurojust to address the personal data breach; and

(d) where appropriate, recommend measures to mitigate the possible adverse effects of the personal data breach.

Article 40

Supervision by the EDPS

1. The EDPS shall be responsible for monitoring and ensuring the application of the provisions of this Regulation and Regulation (EU) 2018/1725 relating to the protection of fundamental rights and freedoms of natural persons with regard to processing of operational personal data by Eurojust, and for advising Eurojust and data subjects on all matters concerning the processing of operational personal data. To that end, the EDPS shall fulfil the duties set out in paragraph 2 of this Article, shall exercise the powers granted in paragraph 3 of this Article and shall cooperate with the national supervisory authorities in accordance with Article 42.

2. The EDPS shall have the following duties under this Regulation and Regulation (EU) 2018/1725:

(a) hearing and investigating complaints, and informing the data subject of the outcome within a reasonable period;

(b) conducting inquiries either on his or her own initiative or on the basis of a complaint, and informing the data subjects of the outcome within a reasonable period;

(c) monitoring and ensuring the application of the provisions of this Regulation and Regulation (EU) 2018/1725 relating to the protection of natural persons with regard to the processing of operational personal data by Eurojust;

(d) advising Eurojust, either on his or her own initiative or in response to a consultation, on all matters concerning the processing of operational personal data, in particular before Eurojust draws up internal rules relating to the protection of fundamental rights and freedoms with regard to the processing of operational personal data.

3. The EDPS may under this Regulation and Regulation (EU) 2018/1725, taking into account the implications for investigations and prosecutions in the Member States:

(a) give advice to data subjects on the exercise of their rights;

(b) refer a matter to Eurojust in the event of an alleged breach of the provisions governing the processing of operational personal data, and, where appropriate, make proposals for remedying that breach and for improving the protection of the data subjects;

(c) consult Eurojust where requests to exercise certain rights in relation to operational personal data have been refused in breach of Article 31, 32 or 33 of this Regulation or Articles 77 to 82 or Article 84 of Regulation (EU) 2018/1725;

(d) warn Eurojust;

(e) order Eurojust to carry out the rectification, restriction or erasure of operational personal data which have been processed by Eurojust in breach of the provisions governing the processing of operational personal data and to notify such actions to third parties to whom such data have been disclosed, provided that this does not interfere with the tasks of Eurojust set out in Article 2;

(f) refer the matter to the Court of Justice of the European Union (the 'Court') under the conditions set out in the TFEU;

(g) intervene in actions brought before the Court.

4. The EDPS shall have access to the operational personal data processed by Eurojust and to its premises to the extent necessary for the performance of his or her tasks.

5. The EDPS shall draw up an annual report on his or her supervisory activities in relation to Eurojust. That report shall be part of the annual report of the EDPS referred to in Article 60 of Regulation (EU) 2018/1725. The national supervisory authorities shall be invited to make observations on this report before it becomes part of the annual report of the EDPS referred to in Article 60 of Regulation (EU) 2018/1725. The EDPS shall take utmost account of the observations made by national supervisory authorities and, in any case, shall refer to them in the annual report.

6. Eurojust shall cooperate with the EDPS in the performance of his or her tasks at his or her request.

Article 41

Professional secrecy of the EDPS

1. The EDPS and his or her staff shall, both during and after their term of office, be subject to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of their performance of official duties.

2. The EDPS shall, in the exercise of his or her supervision powers, take into utmost account the secrecy of judicial inquiries and criminal proceedings, in accordance with Union or Member State law.

Article 42

Cooperation between the EDPS and national supervisory authorities

1. The EDPS shall act in close cooperation with national supervisory authorities with respect to specific issues requiring national involvement, in particular if the EDPS or a national supervisory authority finds major discrepancies between practices of the Member States or potentially unlawful transfers using Eurojust's communication channels, or in the context of questions raised by one or more national supervisory authorities on the implementation and interpretation of this Regulation.

2. In the cases referred to in paragraph 1, coordinated supervision shall be ensured in accordance with Article 62 of Regulation (EU) 2018/1725.

3. The EDPS shall keep national supervisory authorities fully informed of all issues that directly affect them or are otherwise relevant to them. Upon a request from one or more national supervisory authorities, the EDPS shall inform them on specific issues.

4. In cases relating to data originating from one or several Member States, including cases referred to in Article 43(3), the EDPS shall consult the national supervisory authorities concerned. The EDPS shall not decide on further action to be taken before those national supervisory authorities have informed the EDPS of their position, within a deadline specified by the EDPS. That deadline shall not be shorter than one month or longer than three months. The EDPS shall take utmost account of the position of the national supervisory authorities concerned. In cases where the EDPS intends not to follow their position, he or she shall inform them, provide a justification, and submit the matter to the European Data Protection Board.

In cases which the EDPS considers to be extremely urgent, he or she may decide to take immediate action. In such cases, the EDPS shall immediately inform the national supervisory authorities concerned and substantiate the urgent nature of the situation and justify the action he or she has taken.

5. National supervisory authorities shall keep the EDPS informed of any actions they take with respect to the transfer, retrieval, or any other communication of operational personal data under this Regulation by the Member States.

Article 43

Right to lodge a complaint with the EDPS with respect to operational personal data

1. Any data subject shall have the right to lodge a complaint with the EDPS, if he or she considers that the processing by Eurojust of operational personal data relating to him or her does not comply with this Regulation or Regulation (EU) 2018/1725.

2. Where a complaint relates to a decision referred to in Article 31, 32 or 33 of this Regulation or Article 80, 81 or 82 of Regulation (EU) 2018/1725, the EDPS shall consult the national supervisory authorities or the competent judicial body of the Member State that provided the data or the Member State directly concerned. In adopting his or her decision, which may extend to a refusal to communicate any information, the EDPS shall take into account the opinion of the national supervisory authority or of the competent judicial body.

3. Where a complaint relates to the processing of data provided by a Member State to Eurojust, the EDPS and the national supervisory authority of the Member State that provided the data, each acting within the scope of their respective competences shall ensure that the necessary checks on the lawfulness of the processing of the data have been carried out correctly.

4. Where a complaint relates to the processing of data provided to Eurojust by Union bodies, offices or agencies, by third countries or by international organisations or to the processing of data retrieved by Eurojust from publicly available sources, the EDPS shall ensure that Eurojust has correctly carried out the necessary checks on the lawfulness of the processing of the data.

5. The EDPS shall inform the data subject of the progress and outcome of the complaint, as well as the possibility of a judicial remedy pursuant to Article 44.

Article 44

Right to judicial review against the EDPS

Actions against the decisions of the EDPS concerning operational personal data shall be brought before the Court.

Article 45

Responsibility in data protection matters

1. Eurojust shall process operational personal data in such a way that it can be established which authority provided the data or from where the data were retrieved.

2. Responsibility for the accuracy of operational personal data shall lie with:

(a) Eurojust for operational personal data provided by a Member State, or by a Union institution, body, office or agency where the data provided has been altered in the course of processing by Eurojust;

(b) the Member State or the Union institution, office, body or agency which provided the data to Eurojust, where the data provided has not been altered in the course of processing by Eurojust;

(c) Eurojust for operational personal data provided by third countries or by international organisations, as well for operational personal data retrieved by Eurojust from publicly available sources.

3. Responsibility for compliance with Regulation (EU) 2018/1725 in relation to administrative personal data and for compliance with this Regulation and with Article 3 and Chapter IX of Regulation (EU) 2018/1725 in relation to operational personal data shall lie with Eurojust.

Responsibility for the legality of a transfer of operational personal data shall lie:

(a) where a Member State has provided the operational personal data concerned to Eurojust, with that Member State;

(b) with Eurojust, where it has provided the operational personal data concerned to Member States, to Union institutions, bodies, offices or agencies, to third countries or to international organisations.

4. Subject to other provisions of this Regulation, Eurojust shall be responsible for all data processed by it.

Article 46

Liability for unauthorised or incorrect processing of data

1. Eurojust shall be liable, in accordance with Article 340 TFEU, for any damage caused to an individual which results from the unauthorised or incorrect processing of data carried out by it.

2. Complaints against Eurojust on grounds of the liability referred to in paragraph 1 of this Article shall be heard by the Court in accordance with Article 268 TFEU.

3. Each Member State shall be liable, in accordance with its national law, for any damage caused to an individual which results from the unauthorised or incorrect processing carried out by it of data which were communicated to Eurojust.

CHAPTER V

RELATIONS WITH PARTNERS

SECTION I

Common provisions

Article 47

Common provisions

1. In so far as necessary for the performance of its tasks, Eurojust may establish and maintain cooperative relations with Union institutions, bodies, offices and agencies in accordance with their respective objectives, and with the competent authorities of third countries and international organisations in accordance with the cooperation strategy referred to in Article 52.

2. In so far as relevant to the performance of its tasks and subject to any restrictions pursuant to Article 21(8) and Article 76, Eurojust may exchange any information with the entities referred to in paragraph 1 of this Article directly, with the exception of personal data.

3. For the purposes set out in paragraphs 1 and 2, Eurojust may conclude working arrangements with the entities referred to in paragraph 1. Such working arrangements shall not form the basis for allowing the exchange of personal data and shall not bind the Union or its Member States.

4. Eurojust may receive and process personal data received from the entities referred to in paragraph 1 in so far as necessary for the performance of its tasks, subject to the applicable data protection rules.

5. Personal data shall only be transferred by Eurojust to Union institutions, bodies, offices or agencies, to third countries or to international organisations if this is necessary for the performance of its tasks and is in accordance with Articles 55 and 56. If the data to be transferred have been provided by a Member State, Eurojust shall obtain the consent of the relevant competent authority in that Member State, unless the Member State has granted its prior authorisation to such onward transfer, either in general terms or subject to specific conditions. Such consent may be withdrawn at any time.

6. Where Member States, Union institutions, bodies, offices or agencies, third countries or international organisations have received personal data from Eurojust, onward transfers of such data to third parties shall be prohibited unless all of the following conditions have been met:

(a) Eurojust has obtained prior consent from the Member State that provided the data;

(b) Eurojust has given its explicit consent after considering the circumstances of the case at hand;

(c) the onward transfer is only for a specific purpose that is not incompatible with the purpose for which the data were transmitted.

SECTION II

Relations with partners within the Union

Article 48

Cooperation with the European Judicial Network and other Union networks involved in judicial cooperation in criminal matters

1. Eurojust and the European Judicial Network in criminal matters shall maintain privileged relations with each other, based on consultation and complementarity, especially between the national member, contact points of the European Judicial Network in the same Member State as the national member, and the national correspondents for Eurojust and the European Judicial Network. In order to ensure efficient cooperation, the following measures shall be taken:

(a) on a case-by-case basis national members shall inform the contact points of the European Judicial Network of all cases which they consider the Network to be in a better position to deal with;

(b) the Secretariat of the European Judicial Network shall form part of the staff of Eurojust; it shall function as a separate unit; it may draw on the administrative resources of Eurojust which are necessary for the performance of the European Judicial Network's tasks, including for covering the costs of the plenary meetings of the Network;

(c) contact points of the European Judicial Network may be invited on a case-by-case basis to attend Eurojust meetings;

(d) Eurojust and the European Judicial Network may make use of the Eurojust national coordination system when determining under point (b) of Article 20(7) whether a request should be handled with the assistance of Eurojust or the European Judicial Network.

2. The Secretariat of the Network for joint investigation teams and the Secretariat of the Network set up by Decision 2002/494/JHA shall form part of the staff of Eurojust. Those secretariats shall function as separate units. They may draw on the administrative resources of Eurojust which are necessary for the performance of their tasks. The coordination of the secretariats shall be ensured by Eurojust. This paragraph applies to the secretariat of any relevant network involved in judicial cooperation in criminal matters for which Eurojust is to provide support in the form of a secretariat. Eurojust may support relevant European networks and bodies involved in judicial cooperation in criminal matters, including where appropriate by means of a secretariat hosted at Eurojust.

3. The network set up by Decision 2008/852/JHA may request that Eurojust provide a secretariat of the network. If such request is made, paragraph 2 shall apply.

Article 49

Relations with Europol

1. Eurojust shall take all appropriate measures to enable Europol, within Europol's mandate, to have indirect access, on the basis of a hit/no-hit system, to information provided to Eurojust, without prejudice to any restrictions indicated by the Member State, Union body, office or agency, third country or international organisation that provided the information in question. In the case of a hit, Eurojust shall initiate the procedure by which the information that generated the hit may be shared in accordance with the decision of the Member State, Union body, office or agency, third country or international organisation that provided the information to Eurojust.

2. Searches of information in accordance with paragraph 1 shall be carried out only for the purpose of identifying whether information available at Europol matches with information processed at Eurojust.

3. Eurojust shall allow searches in accordance with paragraph 1 only after obtaining from Europol information on which Europol staff members have been designated as authorised to perform such searches.

4. If during Eurojust's information processing activities in respect of an individual investigation, Eurojust or a Member State identifies the need for coordination, cooperation or support in accordance with Europol's mandate, Eurojust shall notify Europol thereof and shall initiate the procedure for sharing the information, in accordance with the decision of the Member State that provided the information. In such cases Eurojust shall consult with Europol.

5. Eurojust shall establish and maintain close cooperation with Europol to the extent relevant to performing the tasks of the two agencies and to achieving their objectives, taking account of the need to avoid duplication of effort.

To that end, the Executive Director of Europol and the President of Eurojust shall meet on a regular basis to discuss issues of common concern.

6. Europol shall respect any restriction of access or use, whether in general or specific terms, that has been indicated by a Member State, Union body, office or agency, third country or international organisation, in relation to information that it has provided.

Article 50

Relations with the EPPO

1. Eurojust shall establish and maintain a close relationship with the EPPO based on mutual cooperation within their respective mandates and competences and on the development of operational, administrative and management links between them as defined in this Article. To that end, the President of Eurojust and the European Chief Prosecutor shall meet on a regular basis to discuss issues of common interest. They shall meet at the request of the President of Eurojust or of the European Chief Prosecutor.

2. Eurojust shall treat requests for support from the EPPO without undue delay, and, where appropriate, shall treat such requests as if they had been received from a national authority competent for judicial cooperation.

3. Whenever necessary to support the cooperation established in accordance with paragraph 1 of this Article, Eurojust shall make use of the Eurojust national coordination system set up in accordance with Article 20, as well as the relations it has established with third countries, including its liaison magistrates

4. In operational matters relevant to the EPPO's competences, Eurojust shall inform the EPPO of and, where appropriate, associate it with its activities concerning cross-border cases, including by:

(a) sharing information on its cases, including personal data, in accordance with the relevant provisions in this Regulation;

(b) requesting the EPPO to provide support.

5. Eurojust shall have indirect access to information in the EPPO's case management system on the basis of a hit/no-hit system. Whenever a match is found between data entered into the case management system by the EPPO and data held by Eurojust, the fact that there is a match shall be communicated to both Eurojust and to the EPPO, as well as to the Member State which provided the data to Eurojust. Eurojust shall take appropriate measures to enable the EPPO to have indirect access to information in its case management system on the basis of a hit/no-hit system.

6. The EPPO may rely on the support and resources of the administration of Eurojust. To that end, Eurojust may provide services of common interest to the EPPO. The details shall be regulated by an arrangement.

Article 51

Relations with other Union bodies, offices and agencies

1. Eurojust shall establish and maintain cooperative relations with the European Judicial Training Network.

2. OLAF shall contribute to Eurojust's coordination work regarding the protection of the financial interests of the Union, in accordance with its mandate under Regulation (EU, Euratom) No 883/2013.

3. The European Border and Coast Guard Agency shall contribute to Eurojust's work including by transmitting relevant information processed in accordance with its mandate and tasks under point (m) of Article 8(1) of Regulation (EU) 2016/1624 of the European Parliament and of the Council ([1]). The European Border and Coast Guard Agency's processing of any personal data in connection therewith shall be regulated by Regulation (EU) 2018/1725.

4. For the purposes of receiving and transmitting information between Eurojust and OLAF, without prejudice to Article 8 of this Regulation, Member States shall ensure that the national members of Eurojust are regarded as competent authorities of the Member States solely for the purposes of Regulation (EU, Euratom) No 883/2013. The exchange of information between OLAF and national members shall be without prejudice to obligations to provide the information to other competent authorities under those Regulations.

SECTION III

International cooperation

Article 52

Relations with the authorities of third countries and international organisations

1. Eurojust may establish and maintain cooperation with authorities of third countries and international organisations.

To that end, Eurojust shall prepare a cooperation strategy every four years in consultation with the Commission, which specifies the third countries and international organisations with which there is an operational need for cooperation.

2. Eurojust may conclude working arrangements with the entities referred to in Article 47(1).

3. Eurojust may designate contact points in third countries in agreement with the competent authorities concerned, in order to facilitate cooperation in accordance with the operational needs of Eurojust.

Article 53

Liaison magistrates posted to third countries

1. For the purpose of facilitating judicial cooperation with third countries in cases in which Eurojust is providing assistance in accordance with this Regulation, the College may post liaison magistrates to a third country subject to the existence of a working arrangement as referred to in Article 47(3) with the competent authorities of that third country.

2. The tasks of the liaison magistrates shall include any activity designed to encourage and accelerate any form of judicial cooperation in criminal matters, in particular by establishing direct links with the competent authorities of the third country concerned. In the performance of their tasks, the liaison magistrates may exchange operational personal data with the competent authorities of the third country concerned in accordance with Article 56.

3. The liaison magistrate referred to in paragraph 1 shall have experience of working with Eurojust and adequate knowledge of judicial cooperation and how Eurojust operates. The posting of a liaison magistrate on behalf of Eurojust shall be subject to the prior consent of the magistrate and of his or her Member State.

4. Where the liaison magistrate posted by Eurojust is selected among national members, deputies or Assistants:

(a) the Member State concerned shall replace him or her in his or her function as a national member, deputy or Assistant;

(b) he or she shall cease to be entitled to exercise the powers granted to him or her under Article 8.

([1]) Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC (OJ L 251, 16.9.2016, p. 1).

5. Without prejudice to Article 110 of the Staff Regulations of Officials, the College shall draw up the terms and conditions for the posting of liaison magistrates, including their level of remuneration. The College shall adopt the necessary implementing arrangements in this respect in consultation with the Commission.

6. The activities of liaison magistrates posted by Eurojust shall be subject to the supervision of the EDPS. The liaison magistrates shall report to the College, which shall inform the European Parliament and the Council in the annual report and in an appropriate manner of their activities. The liaison magistrates shall inform national members and competent national authorities of all cases concerning their Member State.

7. The competent authorities of the Member States and liaison magistrates referred to in paragraph 1 may contact each other directly. In such cases, the liaison magistrate shall inform the national member concerned of such contacts.

8. The liaison magistrates referred to in paragraph 1 shall be connected to the case management system.

Article 54

Requests for judicial cooperation to and from third countries

1. Eurojust may, with the agreement of the Member States concerned, coordinate the execution of requests for judicial cooperation issued by a third country where such requests require execution in at least two Member States as part of the same investigation. Such requests may also be transmitted to Eurojust by a competent national authority.

2. In urgent cases and in accordance with Article 19, the OCC may receive and transmit the requests referred to in paragraph 1 of this Article if they have been issued by a third country which has concluded a cooperation agreement or working arrangement with Eurojust.

3. Without prejudice to Article 3(5), where requests for judicial cooperation which relate to the same investigation and which require execution in a third country are made by the Member State concerned, Eurojust shall facilitate judicial cooperation with that third country.

SECTION IV

Transfers of personal data

Article 55

Transmission of operational personal data to Union institutions, bodies, offices and agencies

1. Subject to any further restrictions pursuant to this Regulation, in particular pursuant to Articles 21(8), 47(5) and 76, Eurojust shall only transmit operational personal data to another Union institution, body, office or agency if the data are necessary for the legitimate performance of tasks covered by the competence of the other Union institution, body, office or agency.

2. Where the operational personal data are transmitted following a request from another Union institution, body, office or agency, both the controller and the recipient shall bear the responsibility for the legitimacy of that transfer.

Eurojust shall be required to verify the competence of the other Union institution, body, office or agency and to make a provisional evaluation of the necessity of the transmission of the operational personal data. If doubts arise as to this necessity, Eurojust shall seek further information from the recipient.

The other Union institution, body, office or agency shall ensure that the necessity of the transmission of the operational personal data can be subsequently verified.

3. The other Union institution, body, office or agency shall process the operational personal data only for the purposes for which they were transmitted.

Article 56

General principles for transfers of operational personal data to third countries and international organisations

1. Eurojust may transfer operational personal data to a third country or international organisation, subject to compliance with the applicable data protection rules and the other provisions of this Regulation, and only where the following conditions are met:

(a) the transfer is necessary for the performance of Eurojust's tasks;

(b) the authority of the third country or the international organisation to which the operational personal data are transferred is competent in law enforcement and criminal matters;

(c) where the operational personal data to be transferred in accordance with this Article have been transmitted or made available to Eurojust by a Member State, Eurojust shall obtain prior authorisation for the transfer from the relevant competent authority of that Member State in compliance with its national law, unless that Member State has authorised such transfers in general terms or subject to specific conditions;

(d) in the case of an onward transfer to another third country or international organisation by a third country or international organisation, Eurojust shall require the transferring third country or international organisation to obtain the prior authorisation of Eurojust for that onward transfer.

Eurojust shall only provide authorisation under point (d) with the prior authorisation of the Member State from which the data originate after taking due account of all relevant factors, including the seriousness of the criminal offence, the purpose for which the operational personal data were originally transferred and the level of personal data protection in the third country or international organisation to which the operational personal data are to be transferred onward.

2. Subject to the conditions set out in paragraph 1 of this Article, Eurojust may transfer operational personal data to a third country or to an international organisation only where one of the following applies:

(a) the Commission has decided pursuant to Article 57 that the third country or international organisation in question ensures an adequate level of protection, or in the absence of such an adequacy decision, appropriate safeguards have been provided for or exist in accordance with Article 58(1), or in the absence of both an adequacy decision and of such appropriate safeguards, a derogation for specific situations applies pursuant to Article 59(1);

(b) a cooperation agreement allowing for the exchange of operational personal data has been concluded before 12 December 2019 between Eurojust and that third country or international organisation, in accordance with Article 26a of Decision 2002/187/JHA; or

(c) an international agreement has been concluded between the Union and the third country or international organisation pursuant to Article 218 TFEU that provides for adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals.

3. The working arrangements referred to in Article 47(3) may be used to set out modalities to implement the agreements or adequacy decisions referred to in paragraph 2 of this Article.

4. Eurojust may in urgent cases transfer operational personal data without prior authorisation from a Member State in accordance with point (c) of paragraph 1. Eurojust shall only do so if the transfer of the operational personal data is necessary for the prevention of an immediate and serious threat to the public security of a Member State or of a third country or to the essential interests of a Member State, and where the prior authorisation cannot be obtained in good time. The authority responsible for giving prior authorisation shall be informed without delay.

5. Member States and Union institutions, bodies, offices and agencies shall not transfer operational personal data they have received from Eurojust onward to a third country or an international organisation,. As an exception, they may make such a transfer in cases where Eurojust has authorised it after taking into due account all relevant factors, including the seriousness of the criminal offence, the purpose for which the operational personal data were originally transmitted and the level of personal data protection in the third country or international organisation to which the operational personal data are transferred onward.

6. Articles 57, 58 and 59 shall apply in order to ensure that the level of protection of natural persons ensured by this Regulation and by Union law is not undermined.

Article 57

Transfers on the basis of an adequacy decision

Eurojust may transfer operational personal data to a third country or to an international organisation where the Commission has decided in accordance with Article 36 of Directive (EU) 2016/680 that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection.

Article 58

Transfers subject to appropriate safeguards

1. In the absence of an adequacy decision, Eurojust may transfer operational personal data to a third country or an international organisation where:

(a) appropriate safeguards with regard to the protection of operational personal data are provided for in a legally binding instrument; or

(b) Eurojust has assessed all the circumstances surrounding the transfer of operational personal data and has concluded that appropriate safeguards exist with regard to the protection of operational personal data.

2. Eurojust shall inform the EDPS about categories of transfers under point (b) of paragraph 1.

3. When a transfer is based on point (b) of paragraph 1, such a transfer shall be documented and the documentation shall be made available to the EDPS on request. The documentation shall include a record of the date and time of the transfer and information about the receiving competent authority, about the justification for the transfer and about the operational personal data transferred.

Article 59

Derogations for specific situations

1. In the absence of an adequacy decision, or of appropriate safeguards pursuant to Article 58, Eurojust may transfer operational personal data to a third country or an international organisation only on the condition that the transfer is necessary:

(a) in order to protect the vital interests of the data subject or another person;

(b) to safeguard legitimate interests of the data subject;

(c) for the prevention of an immediate and serious threat to public security of a Member State or a third country; or

(d) in individual cases for the performance of the tasks of Eurojust, unless Eurojust determines that the fundamental rights and freedoms of the data subject concerned override the public interest in the transfer.

2. Where a transfer is based on paragraph 1, such a transfer shall be documented and the documentation shall be made available to the EDPS on request. The documentation shall include a record of the date and time of the transfer, and information about the receiving competent authority, about the justification for the transfer and about the operational personal data transferred.

CHAPTER VI

FINANCIAL PROVISIONS

Article 60

Budget

1. Estimates of all the revenue and expenditure of Eurojust shall be prepared for each financial year, corresponding to the calendar year, and shall be shown in Eurojust's budget.

2. Eurojust's budget shall be balanced in terms of revenue and of expenditure.

3. Without prejudice to other resources, Eurojust's revenue shall comprise:

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

(b) any voluntary financial contribution from the Member States;

(c) charges for publications and any service provided by Eurojust;

(d) ad hoc grants.

4. The expenditure of Eurojust shall include staff remuneration, administrative and infrastructure expenses and operating costs, including funding for joint investigation teams.

Article 61

Establishment of the budget

1. Each year the Administrative Director shall draw up a draft statement of estimates of Eurojust's revenue and expenditure for the following financial year, including the establishment plan, and shall send it to the Executive Board. The European Judicial Network and other Union networks involved in judicial cooperation in criminal matters referred to in Article 48 shall be informed of the parts related to their activities in due time before the estimate is forwarded to the Commission.

2. The Executive Board shall, on the basis of the draft statement of estimates, review the provisional draft estimate of Eurojust's revenue and expenditure for the following financial year, which it shall forward to the College for adoption.

3. The provisional draft estimate of Eurojust's revenue and expenditure shall be sent to the Commission by no later than 31 January each year. Eurojust shall send the final draft estimate, which shall include a draft establishment plan, to the Commission by 31 March of the same year.

4. The Commission shall send the statement of estimates to the European Parliament and to the Council (the 'budgetary authority') together with the draft general budget of the Union.

5. On the basis of the statement of estimates, the Commission shall enter in the draft general budget of the Union the estimates it considers necessary for the establishment plan and the amount of the contribution to be charged to the general budget, which it shall place before the budgetary authority in accordance with Articles 313 and 314 TFEU.

6. The budgetary authority shall authorise the appropriations for the contribution from the Union to Eurojust.

7. The budgetary authority shall adopt Eurojust's establishment plan. Eurojust's budget shall be adopted by the College. It shall become final following the final adoption of the general budget of the Union. Where necessary, Eurojust's budget shall be adjusted by the College accordingly.

8. Article 88 of Commission Delegated Regulation (EU) No 1271/2013 ([1]) shall apply to any building project likely to have significant implications for Eurojust's budget.

Article 62

Implementation of the budget

The Administrative Director shall act as the authorising officer of Eurojust and shall implement Eurojust's budget under his or her own responsibility, within the limits authorised in the budget.

Article 63

Presentation of accounts and discharge

1. Eurojust'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).

([1]) 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).

2. Eurojust shall send the report on the budgetary and financial management for year N to the European Parliament, the Council and the Court of Auditors by 31 March of year N + 1.

3. The Commission's Accounting Officer shall send Eurojust's provisional accounts for year N, consolidated with the Commission's accounts, to the Court of Auditors by 31 March of year N + 1.

4. In accordance with Article 246(1) of Regulation (EU, Euratom) 2018/1046, the Court of Auditors shall make its observations on Eurojust's provisional accounts by 1 June of year N + 1.

5. On receipt of the Court of Auditors' observations on Eurojust's provisional accounts pursuant to Article 246 of Regulation (EU, Euratom) 2018/1046, the Administrative Director shall draw up Eurojust's final accounts under his or her own responsibility and shall submit them to the Executive Board for an opinion.

6. The Executive Board shall deliver an opinion on Eurojust's final accounts.

7. The Administrative Director shall, by 1 July of year N + 1, send the final accounts for year N to the European Parliament, to the Council, to the Commission and to the Court of Auditors, together with the Executive Board's opinion.

8. The final accounts for year N shall be published in the *Official Journal of the European Union* by 15 November of year N + 1.

9. The Administrative Director shall send the Court of Auditors a reply to its observations by 30 September of year N + 1. The Administrative Director shall also send this reply to the Executive Board and to the Commission.

10. At the European Parliament's request, the Administrative Director shall submit to it any information required for the smooth application of the discharge procedure for the financial year in question in accordance with Article 261(3) of Regulation (EU, Euratom) 2018/1046.

11. On a recommendation from the Council acting by a qualified majority, the European Parliament shall, before 15 May of year N + 2, grant a discharge to the Administrative Director in respect of the implementation of the budget for year N.

12. The discharge of Eurojust's budget shall be granted by the European Parliament on a recommendation of the Council following a procedure comparable to that provided for in Article 319 TFEU and Articles 260, 261 and 262 of Regulation (EU, Euratom) 2018/1046, and based on the audit report of the Court of Auditors.

If the European Parliament refuses to grant the discharge by 15 May of year N + 2, the Administrative Director shall be invited to explain his or her position to the College, which shall take its final decision on the position of the Administrative Director in light of the circumstances.

Article 64

Financial rules

1. The financial rules applicable to Eurojust shall be adopted by the Executive Board in accordance with Delegated Regulation (EU) No 1271/2013 after consultation with the Commission. Those financial rules shall not depart from Delegated Regulation (EU) No 1271/2013 unless such departure is specifically required for Eurojust's operation and the Commission has given its prior consent.

In respect of the financial support to be given to joint investigation teams' activities, Eurojust and Europol shall jointly establish the rules and conditions upon which applications for such support are to be processed.

2. Eurojust may award grants related to the fulfilment of its tasks under Article 4(1). Grants provided for tasks relating to point (f) of Article 4(1) may be awarded to the Member States without a call for proposals.

CHAPTER VII

STAFF PROVISIONS

Article 65

General provisions

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

2. Eurojust staff shall consist of staff recruited according to the rules and regulations applicable to officials and other servants of the Union, taking into account all the criteria referred to in Article 27 of the Staff Regulations of Officials, including their geographical distribution.

Article 66

Seconded national experts and other staff

1. In addition to its own staff, Eurojust may make use of seconded national experts or other staff not employed by Eurojust.

2. The College shall adopt a decision laying down rules on the secondment of national experts to Eurojust and on the use of other staff, in particular to avoid potential conflicts of interest.

3. Eurojust shall take appropriate administrative measures, inter alia, through training and prevention strategies, to avoid conflicts of interest, including conflicts of interests relating to post-employment issues.

CHAPTER VIII

EVALUATION AND REPORTING

Article 67

Involvement of the Union institutions and national parliaments

1. Eurojust shall transmit its annual report to the European Parliament, to the Council and to national parliaments, which may present observations and conclusions.

2. Upon his or her election, the newly elected President of Eurojust shall make a statement before the competent committee or committees of the European Parliament and answer questions put by its members. Discussions shall not refer directly or indirectly to concrete actions taken in relation to specific operational cases.

3. The President of Eurojust shall appear once a year for the joint evaluation of the activities of Eurojust by the European Parliament and national parliaments within the framework of an interparliamentary committee meeting, to discuss Eurojust's current activities and to present its annual report or other key documents of Eurojust.

Discussions shall not refer directly or indirectly to concrete actions taken in relation to specific operational cases.

4. In addition to the other obligations of information and consultation set out in this Regulation, Eurojust shall transmit to the European Parliament and to national parliaments in their respective official languages for their information:

(a) the results of studies and strategic projects elaborated or commissioned by Eurojust;

(b) the programming document referred to in Article 15;

(c) working arrangements concluded with third parties.

Article 68

Opinions on proposed legislative acts

The Commission and the Member States exercising their rights on the basis of point (b) of Article 76 TFEU may request Eurojust's opinion on all proposed legislative acts referred to in Article 76 TFEU.

Article 69

Evaluation and review

1. By 13 December 2024, and every 5 years thereafter, the Commission shall commission an evaluation of the implementation and impact of this Regulation, and the effectiveness and efficiency of Eurojust and its working practices. The College shall be heard in the evaluation. The evaluation may, in particular, address the possible need to modify the mandate of Eurojust, and the financial implications of any such modification.

2. The Commission shall forward the evaluation report together with its conclusions to the European Parliament, to national parliaments, to the Council and to the College. The findings of the evaluation shall be made public.

CHAPTER IX

GENERAL AND FINAL PROVISIONS

Article 70

Privileges and immunities

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

Article 71

Language arrangements

1. Council Regulation No 1 ([1]) shall apply to Eurojust.

2. The College shall decide Eurojust's internal language arrangements by a two-thirds majority of its members.

3. The translation services required for the functioning of Eurojust shall be provided by the Translation Centre for the bodies of the European Union, as established by Council Regulation (EC) No 2965/94 ([2]), unless the unavailability of the Translation Centre requires another solution to be found.

Article 72

Confidentiality

1. The national members and their deputies and Assistants referred to in Article 7, Eurojust staff, national correspondents, seconded national experts, liaison magistrates, the Data Protection Officer, and the members and staff of the EDPS shall be bound by an obligation of confidentiality with respect to any information which has come to their knowledge in the course of the performance of their tasks.

2. The obligation of confidentiality shall apply to all persons and to all bodies that work with Eurojust.

([1]) Council Regulation No 1 determining the languages to be used by the European Economic Community (OJ 17, 6.10.1958, p. 385).
([2]) Council Regulation (EC) No 2965/94 of 28 November 1994 setting up a Translation Centre for bodies of the European Union (OJ L 314, 7.12.1994, p. 1).

3. The obligation of confidentiality shall also apply after leaving office or employment and after the termination of the activities of the persons referred to in paragraphs 1 and 2.

4. The obligation of confidentiality shall apply to all information received or exchanged by Eurojust, unless that information has already lawfully been made public or is accessible to the public.

Article 73

Conditions of confidentiality of national proceedings

1. Without prejudice to Article 21(3), where information is received or exchanged via Eurojust, the authority of the Member State which provided the information may stipulate conditions, pursuant to its national law, on the use by the receiving authority of that information in national proceedings.

2. The authority of the Member State which receives the information referred to in paragraph 1 shall be bound by those conditions.

Article 74

Transparency

1. Regulation (EC) No 1049/2001 of the European Parliament and the Council ([1]) shall apply to documents held by Eurojust.

2. The Executive Board shall, within six months of the date of its first meeting, prepare the detailed rules for applying Regulation (EC) No 1049/2001 for adoption by the College.

3. Decisions taken by Eurojust under Article 8 of Regulation (EC) No 1049/2001 may be the subject of a complaint to the European Ombudsman or of an action before the Court, under the conditions laid down in Articles 228 and 263 TFEU respectively.

4. Eurojust shall publish on its website a list of the Executive Board members and summaries of the outcome of the meetings of the Executive Board. The publication of those summaries shall be temporarily or permanently omitted or restricted if such publication would risk jeopardising the performance of Eurojust's tasks, taking into account its obligations of discretion and confidentiality and the operational character of Eurojust.

Article 75

OLAF and the Court of Auditors

1. In order to facilitate the combating of fraud, corruption and other unlawful activities under Regulation (EU, Euratom) No 883/2013, within six months from the entry into force of this Regulation, Eurojust shall 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) ([2]). Eurojust shall adopt appropriate provisions that apply to all national members, their deputies and Assistants, all seconded national experts and all Eurojust staff, 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 on the spot, over all grant beneficiaries, contractors and subcontractors who have received Union funds from Eurojust.

([1]) 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).

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

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 ([1]), with a view to establishing whether there have been any irregularities affecting the financial interests of the Union in connection with expenditure funded by Eurojust.

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

5. The staff of Eurojust, the Administrative Director and the members of the College and Executive Board shall, without delay and without their responsibility being called into question as a result, notify OLAF and the EPPO of any suspicion of irregular or illegal activity within their respective mandate, which has come to their attention in the fulfilment of their duties.

Article 76

Rules on the protection of sensitive non-classified information and classified information

1. Eurojust shall establish internal rules on the handling and confidentiality of information and on the protection of sensitive non-classified information, including the creation and processing of such information at Eurojust.

2. Eurojust shall establish internal rules on the protection of EU classified information which shall be consistent with Council Decision 2013/488/EU ([2]) in order to ensure an equivalent level of protection for such information.

Article 77

Administrative inquiries

The administrative activities of Eurojust shall be subject to the inquiries of the European Ombudsman in accordance with Article 228 TFEU.

Article 78

Liability other than liability for unauthorised or incorrect processing of data

1. Eurojust's contractual liability shall be governed by the law applicable to the contract in question.

2. The Court shall have jurisdiction to give judgment pursuant to any arbitration clause contained in a contract concluded by Eurojust.

3. In the case of non-contractual liability, Eurojust shall, in accordance with the general principles common to the laws of the Member States and independently of any liability under Article 46, make good any damage caused by Eurojust or its staff in the performance of their duties.

4. Paragraph 3 shall also apply to damage caused through the fault of a national member, a deputy or an Assistant in the performance of their duties. However, when he or she is acting on the basis of the powers granted to him or her pursuant to Article 8, his or her Member State shall reimburse Eurojust the sums which Eurojust has paid to make good such damage.

5. The Court shall have jurisdiction in disputes over compensation for damages referred to in paragraph 3.

([1]) 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).

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

6. The national courts of the Member States competent to deal with disputes involving Eurojust's liability as referred to in this Article shall be determined by reference to Regulation (EU) No 1215/2012 of the European Parliament and of the Council ([1]).

7. The personal liability of Eurojust's staff towards Eurojust shall be governed by the applicable provisions laid down in the Staff Regulations of Officials and Conditions of Employment of Other Servants.

Article 79

Headquarters agreement and operating conditions

1. The seat of Eurojust shall be The Hague, the Netherlands.

2. The necessary arrangements concerning the accommodation to be provided for Eurojust in the Netherlands and the facilities to be made available by the Netherlands together with the specific rules applicable in the Netherlands to the Administrative Director, members of the College, Eurojust staff and members of their families shall be laid down in a headquarters agreement between Eurojust and the Netherlands concluded once the College's approval is obtained.

Article 80

Transitional arrangements

1. Eurojust as established by this Regulation shall be the general legal successor in respect of all contracts concluded by, liabilities incumbent upon, and properties acquired by Eurojust as established by Decision 2002/187/JHA.

2. The national members of Eurojust as established by Decision 2002/187/JHA who have been seconded by each Member State under that Decision shall take the role of national members of Eurojust under Section II of Chapter II of this Regulation. Their terms of office may be extended once under Article 7(5) of this Regulation after the entry into force of this Regulation, irrespective of a previous extension.

3. The President and Vice-Presidents of Eurojust as established by Decision 2002/187/JHA at the time of the entry into force of this Regulation shall take the role of the President and Vice-Presidents of Eurojust under Article 11 of this Regulation, until the expiry of their terms of office in accordance with that Decision. They may be re-elected once after the entry into force of this Regulation under Article 11(4) of this Regulation, irrespective of a previous re-election.

4. The Administrative Director who was last appointed under Article 29 of Decision 2002/187/JHA shall take the role of the Administrative Director under Article 17 of this Regulation until the expiry of his or her term of office as decided under that Decision. The term of office of that Administrative Director may be extended once after the entry into force of this Regulation.

5. This Regulation shall not affect the validity of agreements concluded by Eurojust as established by Decision 2002/187/JHA. In particular, all international agreements concluded by Eurojust before 12 December 2019 shall remain valid.

6. The discharge procedure in respect of the budgets approved on the basis of Article 35 of Decision 2002/187/JHA shall be carried out in accordance with the rules established by Article 36 thereof.

7. This Regulation shall not affect employment contracts which have been concluded under Decision 2002/187/JHA prior to the entry into force of this Regulation. The Data Protection Officer who was last appointed under Article 17 of that Decision shall take the role of the Data Protection Officer under Article 36 of this Regulation.

Article 81

Replacement and repeal

1. Decision 2002/187/JHA is hereby replaced for the Member States bound by this Regulation with effect from 12 December 2019.

Therefore, Decision 2002/187/JHA is repealed with effect from 12 December 2019.

2. With regard to the Member States bound by this Regulation, references to the Decision referred to in paragraph 1 shall be construed as references to this Regulation.

([1]) Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

Article 82

Entry into force and application

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. It shall apply from 12 December 2019.

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

Done at Strasbourg, 14 November 2018.

For the European Parliament	*For the Council*
The President	*The President*
A. TAJANI	K. EDTSTADLER

ANNEX I

List of forms of serious crime with which Eurojust is competent to deal in accordance with Article 3(1):

— terrorism,

— organised crime,

— drug trafficking,

— money-laundering activities,

— crime connected with nuclear and radioactive substances,

— immigrant smuggling,

— trafficking in human beings,

— motor vehicle crime,

— murder and grievous bodily injury,

— illicit trade in human organs and tissue,

— kidnapping, illegal restraint and hostage taking,

— racism and xenophobia,

— robbery and aggravated theft,

— illicit trafficking in cultural goods, including antiquities and works of art,

— swindling and fraud,

— crime against the financial interests of the Union,

— insider dealing and financial market manipulation,

— racketeering and extortion,

— counterfeiting and product piracy,

— forgery of administrative documents and trafficking therein,

— forgery of money and means of payment,

— computer crime,

— corruption,

— illicit trafficking in arms, ammunition and explosives,

— illicit trafficking in endangered animal species,

— illicit trafficking in endangered plant species and varieties,

— environmental crime, including ship source pollution,

— illicit trafficking in hormonal substances and other growth promoters,

— sexual abuse and sexual exploitation, including child abuse material and solicitation of children for sexual purposes,

— genocide, crimes against humanity and war crimes.

ANNEX II

CATEGORIES OF PERSONAL DATA REFERRED TO IN ARTICLE 27

1. (a) surname, maiden name, given names and any alias or assumed names;

   (b) date and place of birth;

   (c) nationality;

   (d) sex;

   (e) place of residence, profession and whereabouts of the person concerned;

   (f) social security number or other official numbers used in the Member State to identify individuals, driving licences, identification documents and passport data, customs and Tax Identification Numbers;

   (g) information concerning legal persons if it includes information relating to identified or identifiable individuals who are the subject of a judicial investigation or prosecution;

   (h) details of accounts held with banks or other financial institutions;

   (i) description and nature of the alleged offences, the date on which they were committed, the criminal category of the offences and the progress of the investigations;

   (j) the facts pointing to an international extension of the case;

   (k) details relating to alleged membership of a criminal organisation;

   (l) telephone numbers, email addresses, traffic data and location data, as well as any related data necessary to identify the subscriber or user;

   (m) vehicle registration data;

   (n) DNA profiles established from the non-coding part of DNA, photographs and fingerprints.

2. (a) surname, maiden name, given names and any alias or assumed names;

   (b) date and place of birth;

   (c) nationality;

   (d) sex;

   (e) place of residence, profession and whereabouts of the person concerned;

   (f) the description and nature of the offences involving the person concerned, the date on which the offences were committed, the criminal category of the offences and the progress of the investigations;

   (g) social security number or other official numbers used by the Member States to identify individuals, driving licences, identification documents and passport data, customs and Tax Identification Numbers;

   (h) details of accounts held with banks and other financial institutions;

   (i) telephone numbers, email addresses, traffic data and location data, as well as any related data necessary to identify the subscriber or user;

   (j) vehicle registration data.

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

Publications Office of the European Union
2985 Luxembourg
LUXEMBOURG

EN