Council of the European Union

Brussels, 26 March 2015
(OR. en)

7466/15

Interinstitutional File:
2012/0011 (COD)

DATAPROTECT 37
JAI 192
MI 184
DIGIT 7
DAPIX 46
FREMP 59
COMIX 136
CODEC 400

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	6833/15 DATAPROTECT 26 JAI 156 MI 144 DRS 18 DAPIX 30 FREMP 45 COMIX 102 CODEC 295 6834/15 DATAPROTECT 27 JAI 157 MI 145 DRS 19 DAPIX 31 FREMP 46 COMIX 103 CODEC 296
Subject:	Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Chapters II, VI and VII

Delegations will find attached the texts of Chapters II (Annex I), VI and VII (one-stop-shop) (Annex II) as agreed in the partial general approach reached at the Council on 13 March 2015.

All changes made to the original Commission proposal are underlined text; where text has been deleted, this is indicated by (…). Where existing text has been moved, this text is indicated in *italics*.

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

(…)[1].

23a) The application of pseudonymisation to personal data can reduce the risks for the data subjects concerned and help controllers and processors meet their data protection obligations. The explicit introduction of 'pseudonymisation' through the articles of this Regulation is thus not intended to preclude any other measures of data protection.

23b) (…)

[1] The question of the application of the Regulation to deceased persons may need to be revisited in the future.

23c) In order to create incentives for applying pseudonymisation when processing personal data, measures of pseudonymisation whilst allowing general analysis should be possible within the same controller when the controller has taken technical and organisational measures necessary to ensure that the provisions of this Regulation are implemented, taking into account the respective data processing and ensuring that additional information for attributing the personal data to a specific data subject is kept separetly. The controller who processes the data shall also refer to authorised persons within the same controller. In such case however the controller shall make sure that the individual(s) performing the pseudonymisation are not referenced in the meta-data[2].

24) When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, when combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. Identification numbers, location data, online identifiers or other specific factors as such should not (…) be considered as personal data if they do not identify an individual or make an individual identifiable[3].

[2] COM, IE, IT, AT, SE, UK reservation and FR scrutiny reservation on two last sentences.
[3] DE reservation. AT and SI thought the last sentence of the recital should be deleted.

25) Consent should be given unambiguously by any appropriate method enabling a freely-given, specific and informed indication of the data subject's wishes, either by a written, including[4] electronic, oral statement or, if required by specific circumstances, by any other clear affirmative action by the data subject signifying his or her agreement to personal data relating to him or her being processed. This could include ticking a box when visiting an Internet website or any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Where it is technically feasible and effective, the data subject's consent to processing may be given by using the appropriate settings of a browser or other application[5]. In such cases it is sufficient that the data subject receives the information needed to give freely specific and informed consent when starting to use the service. (…). Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, unambiguous consent should be granted for all of the processing purposes. It is often not possible to fully identify the purpose of data processing for scientific purposes at the time of data collection. Therefore data subjects can give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research[6]. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose and provided that this does not involve disproportionate efforts in view of the protective purpose[7]. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided[8].

---

4 HU and DE would prefer to distinguish electronic from written statements.

5 PL and AT reservation.

6 FR and COM scrutiny reservation.

7 AT, CZ, IE and FR scrutiny reservation; COM reservation.

8 UK, supported by CZ and IE, proposed adding: 'Where the intention is to store data for an as yet unknown research purpose or as part of a research resource [such as a biobank or cohort], then this should be explained to data subjects, setting out the types of research that may be involved and any wider implications. This interpretation of consent does not affect the need for derogations from the prohibition on processing sensitive categories of data for scientific purposes' .

25a) Genetic data should be defined as personal data relating to the genetic characteristics of an individual which have been inherited or acquired as they result from an analysis of a biological sample from the individual in question, in particular by chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained.

26) Personal data concerning health should include (…) data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health of the data subject[9]; including information about the registration of the individual for the provision of health services (…); a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; (…) information derived from the testing or examination of a body part or bodily substance, including genetic data and biological samples; (…) or any information on for example a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as for example from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.

[9] The Presidency points out that this recital may have to be aligned to the definition of health data (Article 4(12)) to be agreed in the future.

27) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union. In this case the latter should be considered as the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes (…) and means of processing through stable arrangements. This criterion should not depend on whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union and, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment but the supervisory authority of the processor should be considered as a concerned supervisory authority and participate to the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered as concerned supervisory authorities when the draft decision concerns only the controller.

Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered as the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

28) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.

29) Children (…) deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. (…)[10]. This concerns especially the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of child data when using services offered directly to a child[11].

30) Any processing of personal data should be lawful and fair. (…). It should be transparent for the individuals that personal data concerning them are collected, used, consulted or otherwise processed and to which extent the data are processed or will be processed. The principle of transparency requires that any information and communication relating to the processing of those data should be easily accessible and easy to understand, and that clear and plain language is used. This concerns in particular the information of 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 individuals concerned and their right to get confirmation and communication of personal data being processed concerning them. Individuals should be made aware on risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise his or her rights in relation to the processing. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data.[12] The data should be adequate and relevant (…) for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. (…). Personal data should only be processed if the purpose of the processing could not reasonably be fulfilled by other means[13]. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

---

10 COM reservation on deletion of the UN Convention on the Rights of the Child reference.

11 CZ and AT reservation.

12 DE suggested inserting the following sentence: 'Data processing for archiving and statistical purposes in the public interest and for scientific or historical purposes is considered compatible and can be conducted on the basis of the original legal basis (e.g. consent), if the data have been initially collected for these purposes'.

13 UK reservation: this was too burdensome.

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 the use of personal data and the equipment used for the processing.

31) In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate legal basis laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or 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.

31a) Wherever this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant the constitutional order of the Member State concerned, however such legal basis or legislative measure should be clear and precise and its application foreseeable for those subject to it as required by the case law of the Court of Justice of the European Union and the European Court on Human Rights.

32) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given the 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 that, and the extent to which, consent is given. 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 its content should not be unusual within the overall context. 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 and free choice and is unable to refuse or withdraw consent without detriment.

33) (…)

34) In order to safeguard that consent has been 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 this imbalance makes it unlikely that consent was given freely in all the circumstances of that specific situation. Consent is presumed not to be freely given, if it does not allow separate consent to be given to different data processing operations despite it is appropriate in the individual case, or if the performance of a contract is made dependent on the consent despite this is not necessary for such performance and the data subject cannot reasonably obtain equivalent services from another source without consent[14].

35) Processing should be lawful where it is necessary in the context of a contract or the intended entering into a contract.

35a) This Regulation provides for general rules on data protection and that in specific cases Member States are also empowered to lay down national rules on data protection. The Regulation does therefore not exclude Member State law that defines the circumstances of specific processing situations, including determining more precisely the conditions under which processing of personal data is lawful. National law may also provide for special processing conditions for specific sectors and for the processing of special categories of data.

36) Where processing is carried out in compliance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a (…) basis in Union law or in the national law of a Member State. (…). It should be also for Union or national law to determine the purpose of the processing. Furthermore, this (…) basis could specify the general conditions of the Regulation governing the lawfulness of data processing, determine specifications for determining the controller, the type of data which are subject to the processing, the data subjects concerned, the entities to which the data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing.

[14] COM, DK, IE and FR, SE reservation. CZ thought the wording should be more generic.

It should also be for Union or national law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or by private law such as a professional association, where grounds of public interest so justify including for health purposes, such as public health and social protection and the management of health care services.

37) The processing of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's life or that of another person. (…). Some types of *data 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 epidemic and its spread or in situations of humanitarian emergencies, in particular in situations of natural disasters*[15].

38) The legitimate interests of a controller including of a controller to which the data may be disclosed or of a third party may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. Legitimate interest could exist for example when there is a relevant and appropriate connection between the data subject and the controller in situations such as the data subject being a client or in the service of the controller[16]. (…) At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can expect at the time and in the context of the collection of the data that processing for this purpose may take place. In particular such assessment must take into account whether the data subject is a child, given that children deserve specific protection. The data subject should have the right to object to the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. (…)

---

15 CZ, FR, SE and PL thought the entire recital was superfluous.

16 HU scrutiny reservation.

38a) Controllers that are part of a group of undertakings or institution affiliated to a central bodymay have a legitimate interest to transmit personal data within the group of undertakings for internal administrative purposes**,** including the processing of clients' or employees' personal data. The general principles for the transfer of personal data**,** within a group of undertakings, to an undertaking located in a third country (…) remain unaffected.[17]

39) The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller *concerned*. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

[17] FR reservation.

40) The processing of personal data for other purposes than the purposes for which the data have been initially collected should be only allowed where the processing is compatible with those purposes for which the data have been initially collected. In such case no separate legal basis is required other than the one which allowed the collection of the data. (…) 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 or Member State law may determine and specify the tasks and purposes for which the further processing shall be regarded as lawful. The further processing (…) for archiving purposes in the public interest or, statistical, scientific or historical (…) purposes (…) or in view of future dispute resolution[18] should be considered as compatible lawful processing operations. The legal basis provided by Union or Member State law for the collection and processing of personal data may also provide a legal basis for further processing for other purposes if these purposes are in line with the assigned task and the controller is entitled legally to collect the data for these other purposes[19].

In order to ascertain whether a purpose of further processing is compatible with the purpose for which the data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account any link between those purposes and the purposes of the intended further processing, the context in which the data have been collected, including the reasonable expectations of the data subject 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 processing operations. Where the intended other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject. (…).

---

18 ES pointed out the text of Article 6 had not been modified regarding dispute resolution.

19 FR, IT and UK scrutiny reservation.

In any case, the application of the principles set out by this Regulation and in particular the information of the data subject on those other purposes and on his or her rights (…) including the right to object, should be ensured. (…). Indicating possible criminal acts or threats to public security by the controller and transmitting these data to a competent authority should be regarded as being in the legitimate interest pursued by the controller[20]. However such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.[21]

41) Personal data which are, by their nature, particularly sensitive (…) in relation to fundamental rights and freedoms, deserve specific protection as the context of their processing may create important risks for the fundamental rights and freedoms. These data should also 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 European Union of theories which attempt to determine the existence of separate human races. Such data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation[22]for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, 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 be 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.

---

20 AT, PL and COM reservation.

21 IE, SE and UK queried the last sentence of recital 40, which was not reflected in the body of the text. DE, supported by CZ, IE, GR and PL, wanted it to be made clear that Article 6 did not hamper direct marketing or credit information services or businesses in general according to GR.

22 AT scrutiny reservation.

Special categories of personal data may also be processed where the data have manifestly been made public or voluntarily and at the request of the data subject transferred to the controller for a specific purpose specified by the data subject, where the processing is done in the interest of the data subject.

Member State and Union Law may provide that the general prohibition for processing such special categories of personal data in certain cases may not be lifted by the data subject's explicit consent.

42) Derogating from the prohibition on processing sensitive categories of data should also be allowed when provided for in Union or Member State law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where (…) grounds of public interest so justify, in particular *processing data* in the field of employment law, social security and social protection law, including pensions and *for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health or ensuring high standards of quality and safety of health care and services and of medicinal products or medical devices or assessing public policies adopted in the field of health, also by producing quality and activity indicators*.

This may be done for health purposes, including public health (…) and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving in the public interest or historical, statistical and scientific (…) purposes.

A derogation should also allow processing of such data where necessary for the establishment, exercise or defence of legal claims, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure.

42a) *Special categories of personal data which deserve higher protection, may only be processed for health-related purposes where necessary to achieve those purposes for the benefit of individuals and society as a whole, in particular in the context of the management of health or social care services* and systems including the processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, *and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes or for archiving, historical, statistical or scientific purposes as well as for studies conducted in the public interest in the area of public health. 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 these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy (...). Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of individuals. (...)*[23].

[23] Moved from recital 122.

42b) *The processing of special categories personal data* (…) *may be necessary for reasons of public interest in the areas of public health, without consent of the data subject. This processing is subject to for suitable and specific measures so as to protect the rights and freedoms of individuals. In that context, 'public health' should be interpreted as defined in 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, meaning all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of personal data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers, insurance and banking companies*[24].

43) Moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognised religious associations is carried out on grounds of public interest.

44) Where in the course of electoral activities, the operation of the democratic system requires in a Member State that political parties compile data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.

45) If the 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.

[24] Moved from recital 123.

HAVE ADOPTED THIS REGULATION:

Article 4

Definitions

(3b) 'pseudonymisation' means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person (…)[25].

CHAPTER II

PRINCIPLES

Article 5

Principles relating to personal data processing

1. Personal data must be:

   (a) processed lawfully, fairly and in a transparent manner in relation to the data subject[26];

[25] DE, supported by UK, proposed reinserting the following reference 'or can be attributed to such person only with the investment of a disproportionate amount of time, expense and manpower'.

[26] DE proposed adding "and non-discriminatory" and "taking into account the benefit of data processing within a free, open and social society". This was viewed critically by several delegations (CZ, ES, IE, IT, PL).

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; further processing of personal data for archiving purposes in the public interest or *scientific*, statistical[27] or historical purposes shall in accordance with Article 83 not be considered incompatible with the initial purposes[28];

(c) adequate, relevant and not excessive in relation to the purposes for which they are processed (…)[29];

(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;

---

27 FR thought Chapter III should contain specific rules for protecting personal data processed for statistical purposes; DE and PL thought statistical purposes should also be qualified by the public interest filter. DE, supported by SI, suggested adding: "if the data have initially been collected for these purposes".

28 Referring to Article 6(2), DE and RO queried whether this phrase implied that a change of the purpose of processing was always lawful in case of scientific processing, also in the absence of consent by the data subject. BE queried whether the concept of compatible purposes was still a useful one. HU and ES scrutiny reservations on reference to Article 83. FR thought that health data could be processed only in the public interest or with the consent of the data subject.

29 COM reservation on the deletion of the data minimisation principle. AT, CY, DE, EE, FR, HU, IT, PL, FI and SI preferred to return to the initial COM wording, stating 'limited to the minimum necessary'. DE, supported by PL, also suggested adding: "they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data". DK and UK were opposed to any further amendments to this point.

(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 data will be processed for archiving purposes in the public interest or *scientific*, statistical, or historical purposes in accordance with Article 83 subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of data subject[30];

(ee) processed in a manner that ensures appropriate security of the personal data.

(f) (…)

2. The controller shall be responsible for compliance with paragraph 1[31].

Article 6

Lawfulness of processing[32]

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

(a) the data subject has given unambiguous[33]consent to the processing of their personal data for one or more specific purposes[34];

(b) 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;

---

30 FR and SK scrutiny reservation. SK indicated that the case of private archiving was still not addressed. CZ and SE thought the last part of this sentence should be deleted.

31 It was previously proposed to add '*also in case of personal data being processed on its behalf by a processor*', but further to suggestion from FR, this rule on liability may be dealt with in the context of Chapter VIII.

32 DE, AT, PT, SI and SK scrutiny reservation.

33 FR, PL and COM reservation in relation to the deletion of 'explicit' in the definition of 'consent'; UK thought that the addition of 'unambiguous' was unjustified.

34 RO scrutiny reservation.

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

(d) processing is necessary in order to protect the vital interests of the data subject or of another person;

(e) 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;

(f) processing is necessary for the purposes of the legitimate interests[35] pursued by the controller or by a third party [36] except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (…)[37] [38].

2. Processing of personal data which is necessary for archiving purposes in the public interest, or for historical, statistical or scientific purposes shall be lawful subject also to the conditions and safeguards referred to in Article 83.

---

35 FR scrutiny reservation.

36 Reinstated at the request of BG, CZ, DE, ES, HU, IT, NL, SE, SK and UK. COM, IE, FR and PL reservation on this reinstatement.

37 Deleted at the request of BE, CZ, DK, IE, MT, SE, SI, SK, PT and UK. COM, AT, CY, DE, FI, FR, GR and IT wanted to maintain the last sentence. COM reservation against deletion of the last sentence, stressing that processing by public authorities in the exercise of their public duties should rely on the grounds in point c) and e).

38 DK and FR regretted there was no longer a reference to purposes set out in Article 9(2) and thought that the link between Article 6 and 9 needed to be clarified.

3. The basis for the processing referred to in points (c) and (e) of paragraph 1 must be established in accordance with:

(a) Union law, or

(b) national law of the Member State to which the controller is subject[39].

The purpose of the processing shall be determined in this legal basis or as regards the processing referred to in point (e) of paragraph 1, be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia the general conditions governing the lawfulness of data processing by the controller, the type of data which are subject to the processing, the data subjects concerned; the entities to, and the purposes for which the data may be disclosed; the purpose limitation; storage periods and processing operations and processing procedures, including measures to ensure lawful and fair processing, including for other specific processing situations as provided for in Chapter IX.

[39] It was pointed out that the text of Article 6 may have an adverse effect on the collection of personal data under administrative, criminal and civil law collections by third country public authorities, in that Article 6 provides that processing 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 may only take place to the extent established in accordance with Union or Member State law. Compliance with the administrative, regulatory, civil and criminal law requirements of a third country incumbent on controllers that engage in commercial or other regulated activities with respect to third countries, or voluntary reporting of violations of law to, or cooperation with, third country administrative, regulatory, civil and criminal law enforcement authorities appear not be allowed under the current draft of Article 6 . The Presidency thinks this point will have to be examined in the future, notably in the context of Chapter I.

3a. In order to ascertain whether a purpose of further processing (…) is compatible with the one for which the data are initially collected, the controller shall take into account, unless the data subject has given consent[40], inter alia[41]:

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

(b) the context in which the data have been collected;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9;

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

(e) the existence of appropriate safeguards[42].

4. Where the purpose of further processing is incompatible with the one for which the personal data have been collected by the same controller, the further processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1[43] [44]. Further processing by the same controller for incompatible purposes on grounds of legitimate interests of that controller or a third party shall be lawful if these interests override the interests of the data subject[45].

---

40 DK, IT and PT scrutiny reservation; IT deemed this irrelevant to compatibility test.

41 DK, FI, NL, RO, SI and SE stressed the list should not be exhaustive.

42 DE, SK and PL reservation: safeguards as such do not make further processing compatible. FR queried to which processing this criterion related: the initial or further processing. DE and UK pleaded for the deletion of paragraph 3a.

43 ES, AT and PL reservation; DE, HU scrutiny reservation. FR suggested adding 'if the process concerns the data mentioned in Articles 8 and 9'.

44 HU, supported by CY, FR, AT and SK, thought that a duty for the data controller to inform the data subject of a change of legal basis should be added here. The Presidency refers to the changes proposed in ADD 1 to 17072/3/14 REV 3.

45 COM reservation; BE, AT, FI, HU, IT and PL scrutiny reservation: (some of) these delegations would have liked to delete this last sentence; DE wanted to limit the second sentence to private controllers.

5. (…)

Article 7

Conditions for consent

1. Where Article 6(1)(a) applies the controller shall be able to demonstrate that unambiguous[46] consent was given by the data subject.

1a. Where Article 9(2)(a) applies, the controller shall be able to demonstrate that explicit consent was given by the data subject.

2. If the data subject's consent is to be given in the context of a written declaration which also concerns other matters, the request for consent must 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.

[46] COM reservation related to the deletion of 'explicit' in the definition of consent.

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[47].

4. (…)

Article 8

Conditions applicable to child's consent in relation to information society services [48]

1. Where Article 6 (1)(a) applies, in relation to the offering of information society services directly to a child[49], the processing of personal data of a child (…)[50] shall only be lawful if and to the extent that such consent is given or authorised by the holder of parental responsibility over the child or is given by the child in circumstances where it is treated as valid by Union or Member State law.

1a. 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.

2. 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.

---

47 IE reservation. The Presidency concurs with SE that the last sentence belongs rather in Article 14. To that end the Presidency has made some suggestions set out in ADD 1 to 17072/3/14 REV 3.

48 CZ, MT, ES, SI would have preferred to see this Article deleted.

49 Several delegations (DE, HU, ES, FR, SE, SK, PT) disagreed with the restriction of the scope and thought the phrase 'in relation to the offering of information society services directly to a child' should be deleted.

50 COM reservation on the deletion of a harmonised age threshold.

3. [The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the methods to obtain verifiable consent referred to in paragraph 1(…)[51]].

4. **(…).**

Article 9

Processing of special categories of personal data[52]

1. The processing of personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life (…) 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 (…), except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or

[51] DE, ES, FR, SE and UK suggested deleting this paragraph. CZ suggested adding "and for identifying that a service is offered directly to a child". DE, supported by BE and FR, suggested giving the EDPB the power to issue guidelines in this regard.

[52] COM, DK, SE and AT scrutiny reservation. SK thought the inclusion of biometric data should be considered.

(b) 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 in so far as it is authorised by Union law or Member State law or a collective agreement pursuant to Member State law providing for adequate safeguards; or

(c) 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; or

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body 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 the 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; or

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

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or

(g) processing is necessary for (…)[53] reasons of public interest, on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests; or

[53] AT, PL and COM reservation on deletion of 'important'; DK suggested adding 'in the public interest vested in the controller'.

(h) processing[54] is necessary for the purposes of preventive or occupational medicine[55], for the assessment of the working capacity of the employee[56], 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 Member State law [57] or pursuant to contract with a health professional[58] and subject to the conditions and safeguards referred to in paragraph 4[59]; or

(ha) (…);

(hb) 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 health care and of medicinal products or medical devices, on the basis of Union law or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject data; or

(i) processing is necessary for archiving purposes in the public interest or historical, statistical or scientific (…) purposes and subject to the conditions and safeguards laid down in Union or Member State law, including those referred to in Article 83.

(j) (…)[60]

3. (…)[61]

---

54 HU suggested reinstating "of health data" here and in point (hb).

55 AT would like to see this deleted; BE pointed out this type of medicine practice is not (entirely) regulated by law under Belgian law and therefore the requirement of paragraph 4 is not met.

56 PL and AT would like to see this deleted.

57 COM, IE, PL scrutiny reservation.

58 FR and PL reservation.

59 AT, DE and ES scrutiny reservation. DE and ES queried what happened in cases where obtaining consent was not possible (e.g. in case of contagious diseases; persons who were physically or mentally not able to provide consent); NL thought this should be further clarified in recital 42. BE queried what happened in the case of processing of health data by insurance companies. COM explained that this was covered by Article 9(2) (a), but SI was not convinced thereof.

60 Deleted at the request of AT, COM, EE, ES, FR, HU, IT, LU, MT, PL, PT, RO and SK. DE and FI wanted to reintroduce the paragraph.

61 COM reservation on the deletion of paragraph 3 on delegated acts.

4. *Personal data referred to in paragraph 1 may on the basis of Union or Member State law 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*.

4a. **(…)**[62].

5. Member States may maintain or introduce more specific provisions with regard to genetic data or health data. This includes the possibility for Member States to **(…)** introduce further conditions for the processing of these data[63]**.**

Article 9a

Processing of data relating to criminal convictions and offences[64]

P*rocessing of data relating to criminal convictions and offences or related security measures* based on Article 6(1) *may only be carried out either under the control of official authority (...) or when the processing is* (…) *authorised by Union law or Member State law providing for adequate safeguards* for the rights and freedoms of data subjects. A complete register of criminal convictions may be kept only under the control of official authority[65].

---

62 Deleted further to the request from COM, CZ, DK, GR, IE, MT, SE, FI and UK scrutiny reservation. FR wanted to keep paragraph 4a in Article 9 or at least keep the text in a recital.

63 COM scrutiny reservation.

64 DE and HU would prefer to see these data treated as sensitive data in the sense of Article 9(1). EE and UK are strongly opposed thereto.

65 SI, SK reservation on last sentence.

Article 10

Processing not requiring 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 or acquire (…) additional information nor to engage in additional processing in order to identify the data subject for the sole purpose of complying with (…) this Regulation[66].**(…)**

2. Where, in such cases the controller is not in a position to identify the data subject, articles 15, 16, 17, 17a, 17b and 18 do not apply except where the data subject, for the purpose of exercising his or her rights under these articles, provides additional information enabling his or her identification[67].

---

[66] AT, DE, HU, PL scrutiny reservation and UK and FR and COM reservation.

[67] DK, RO, SE and SI scrutiny reservation; COM and FR reservation; FR wanted to add in the end of the paragraph "In any case, the data subject should only have to provide the minimum additional information necessary in order to be able to exercise his or her rights which can never be denied by the controller.

ANNEX II

16a) *While this Regulation applies also to the activities of courts* and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. *The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity*, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including its decision-making. Supervision of such data processing operations may be entrusted to specific bodies within the judicial system of the Member State, which should in particular control compliance with the rules of this Regulation, promote the awareness of the judiciary of their obligations under this Regulation and deal with complaints in relation to such processing.

27) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union. In this case the latter should be considered as the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes (…) and means of processing through stable arrangements. This criterion should not depend on whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union and, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment but the supervisory authority of the processor should be considered as a concerned supervisory authority and participate to the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered as concerned supervisory authorities when the draft decision concerns only the controller.

Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered as the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

92) The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of individuals with regard to the processing of their personal data. Member States may establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.

92a) The independence of supervisory authorities should not mean that the supervisory authorities cannot be subjected to control or monitoring mechanism regarding their financial expenditure. Neither does it imply that supervisory authorities cannot be subjected to judicial review.

93) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth co-operation with other supervisory authorities, the European Data Protection Board and the Commission.

94) Each supervisory authority should be provided with the (…) financial and human resources, premises and infrastructure, which are necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and co-operation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate annual budget, which may be part of the overall state or national budget.

95) The general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be either appointed by the parliament and/or the government or the head of State of the Member State or by an independent body entrusted by Member State law with the appointment by means of a transparent procedure. In order to ensure the independence of the supervisory authority, the member or members should refrain from any action incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not. (…).

95a) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should cover in particular the processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State, the processing of personal data, carried out by public authorities or private bodies acting in the public interest processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the European Union when targeting data subjects residing in its territory. This should include dealing with complaints lodged by a data subject, conducting investigations on the application of the Regulation, promoting public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data.

96) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation 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. For that purpose, this Regulation should oblige and empower the supervisory authorities to co-operate with each other and the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation.

96a) Where the processing of personal data takes place in the context of the activities of an establishment of a controller or processor in the Union and the controller or processor is established in more than one Member State, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. It should cooperate with the other authorities that are concerned, because the controller or processor has an establishment on the territory of their Member State, because data subjects residing on their territory are substantially affected, or because a complaint has been lodged with them. Also where a data subject not residing in that Member State has lodged a complaint, the supervisory authority to which such complaint has been lodged should also be a concerned supervisory authority. Within its tasks to issue guidelines on any question covering the application of this Regulation, the European Data Protection Board may issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State and on what constitutes a relevant and reasoned objection[68].

96b) The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with the provisions of this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the concerned supervisory authorities in the decision-making process. In cases where the decisions is to reject the complaint by the data subject in whole or in part that decision should be adopted by the supervisory authority at which the complaint has been lodged.

[68] DE proposal; CZ and LU scrutiny reservation.

96c) The decision should be agreed jointly by the lead supervisory authority and the concerned supervisory authorities and should be directed towards the main or single establishment of the controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure the compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities in the Union.

97) Each supervisory authority (…) not acting as lead supervisory authority should be competent to deal with (…) local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involving only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay on this matter. After being informed, the lead supervisory authority should decide, whether it will deal with the case within the one-stop-shop mechanism or whether the supervisory authority which informed it should deal with the case at local level. When deciding whether it will deal with the case, the lead supervisory authority should take into account, whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it, in order to ensure effective enforcement of a decision vis-à-vis the controller or processor. Where the lead supervisory authority decides to deal with the case, the supervisory authority which informed it should have the possibility to submit a draft for a decision, of which the lead supervisory authority should take utmost account when preparing its draft decision in the one-stop-shop mechanism.

98) The rules on the lead supervisory authority and the one-stop-shop mechanism should not apply where the processing is carried out by public authorities or private bodies acting in the public interest. In such cases the only supervisory authority competent to exercise the powers conferred to it in accordance with this Regulation should be the supervisory authority of the Member State where the public authority or private body is established.

99) (…)

100) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, particularly in cases of complaints from individuals, and without prejudice to the powers of prosecutorial authorities under national law, to bring infringements of this Regulation to the attention of the judicial authorities and/or engage in legal proceedings. Such powers should also include the power to forbid the processing on which the authority is consulted. Member States may specify other tasks related to the protection of personal data under this Regulation. The powers of supervisory authorities (…) should be exercised in conformity with appropriate procedural safeguards set out in Union law and national law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in national procedural law, such as the requirement to obtain a prior judicial authorisation.

Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to national procedural law. The adoption of such legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision.

100) (…).

101) Where the supervisory authority to which the complaint has been lodged is not the lead supervisory authority, the lead supervisory authority should closely co-operate with the supervisory authority to which the complaint has been lodged according to the provisions on co-operation and consistency laid down in this Regulation. In such cases, the lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority to which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority.

101a) The supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of the Regulation should seek an amicable settlement and, if this proves unsuccessful, exercise its full range of powers in cases where another supervisory authority should act as a lead supervisory authority for the processing activities of the controller or processor but the concrete subject matter of a complaint or the possible infringement concerns only processing activities of the controller or processor in the one Member State where the complaint has been lodged or the possible infringement detected and the matter does not substantially affect or is not likely to substantially affect data subjects in other Member States. This should include specific processing carried out in the territory of the Member State of the supervisory authority or with regard to data subjects on the territory of that Member State; or to processing that is carried out in the context of an offer of goods or services specifically aimed at data subjects in the territory of the Member State of the supervisory authority; or that has to be assessed taking into account relevant legal obligations under national law.

102) Awareness raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as individuals in particular in the educational context.

103) The supervisory authorities should assist each other in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market. Where a supervisory authority requesting mutual assistance, in the case of no response of the requested supervisory authority within one month of receiving the request, adopts a provisional measure, such provisional measure should be duly justified and only of a temporary nature.

104) Each supervisory authority should have the right to participate in joint operations between supervisory authorities. The requested supervisory authority should be obliged to respond to the request in a defined time period.

105) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities (…) should be established. This mechanism should in particular apply where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States (…). It should also apply where any *concerned* supervisory authority or the Commission[69] requests that such matter should be dealt with in the consistency mechanism. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

[69] HU reservation on the reference to the Commission.

106) In application of the consistency mechanism, the European Data Protection Board should, within a determined period of time, issue an opinion, if a (…) majority of its members so decides or if so requested by any *concerned* supervisory authority or the Commission. The European Data Protection Board should also be empowered to adopt legally binding decisions in case of disputes between supervisory authorities. For that purposes it should issue, in principle with a two-third majority of its members, legally binding decisions in clearly defined cases where there are conflicting views among supervisory authorities in particular in the cooperation mechanism between the lead supervisory authority and *concerned* supervisory authorities on the merits of the case, notably whether there is an infringement of this Regulation or not.

107) (…)

108) There may be an urgent need to act in order to protect the rights and freedoms of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. Therefore, a supervisory authority should be able to adopt provisional measures with a specified period of validity when applying the consistency mechanism.

109) The application of this mechanism should be a condition for the lawfulness of a measure intended to produce legal effects by a supervisory authority in those cases where its application is mandatory. In other cases of cross-border relevance, the cooperation mechanism between the lead supervisory authority and *concerned* supervisory authorities should be applied and mutual assistance and joint operations might be carried out between the *concerned* supervisory authorities on a bilateral or multilateral basis without triggering the consistency mechanism.

110) In order to promote the consistent application of this Regulation, the European Data Protection Board should be set up as an independent body of the Union. To fulfil its objectives, the European Data Protection Board should have legal personality. The European Data Protection Board should be represented by its Chair. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of a head of a supervisory authority of each Member State or his or her representative (…). The Commission *and the European Data Protection Supervisor* should participate in its activities without voting rights. The European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting co-operation of the supervisory authorities throughout the Union. The European Data Protection Board should act independently when exercising its tasks.

110a) The European Data Protection Board should be assisted by a secretariat provided by the secretariat of the European Data Protection Supervisor. The staff of the secretariat of the European Data Protection Supervisor involved in carrying out the tasks conferred on the European Data Protection Board by this Regulation should perform its tasks exclusively under the instructions of, and report to the Chair of the European Data Protection Board. Organisational separation of staff should concern all services needed for the independent functioning of the European Data Protection Board.

111) Every data subject should have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence , and have the right to an effective judicial remedy in accordance with Article 47 of the Charter of Fundamental Rights if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority 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 supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can be completed also electronically, without excluding other means of communication.

112) 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 body, organisation or association which aims to protect the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State, to lodge a complaint on his or her behalf with a supervisory authority or exercise the right to a judicial remedy on behalf of data subjects. Such a body, organisation or association should have the right to lodge, independently of a data subject's complaint, a complaint where it has reasons to consider that a personal data breach referred to in Article 32(1) has occurred and Article 32(3) does not apply.

113) Any natural or legal person has the right to bring an action for annulment of decisions of the European Data Protection Board before the Court of Justice of the European Union (the "Court of Justice") under the conditions provided for in Article 263 TFEU. As addressees of such decisions, the concerned supervisory authorities who wish to challenge them, have to bring action within two months of their notification to them, in accordance with Article 263 TFEU. Where decisions of the European Data Protection Board are of direct and individual concern to a controller, processor or the complainant, the latter may bring an action for annulment against those decisions and they should do so within two months of their publication on the website of the European Data Protection Board, in accordance with Article 263 TFEU. Without prejudice to this right under Article 263 TFEU, each natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning this person.

Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints[70]. However, this right does not encompass other measures of supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with the national procedural law of that Member State. Those courts should exercise full jurisdiction which should include jurisdiction to examine all questions of fact and law relevant to the dispute before it. Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings to the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law including this Regulation.

[70] GR reservation.

Furthermore, where a decision of a supervisory authority implementing a decision of the European Data Protection Board is challenged before a national court and the validity of the decision of the European Data Protection Board is at issue, that national court does not have the power to declare the European Data Protection Board's decision invalid but must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU as interpreted by the Court of Justice in the *Foto-frost* case[71], whenever it considers the decision invalid. However, a national court may not refer a question on the validity of the decision of the European Data Protection Board at the request of a natural or legal person which had the opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down by Article 263 TFEU.

[71] Case C-314/85.

Article 4

Definitions

(13) 'main establishment' means[72]

- as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes (…) and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented , in this case the establishment having taken such decisions shall be considered as the main establishment[73].
- as regards a processor with establishments in more than one Member State, the place of its central administration in the Union and, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

(19a) '*concerned* supervisory authority ' means

- a supervisory authority which is concerned by the processing because:

  a) the controller or processor is established on the territory of the Member State of that supervisory authority;

[72] AT remarked that, in view technological developments, it was very difficult to pinpoint the place of processing and , supported by ES, HU, PL, expressed a preference for a formal criterion, which referred to the incorporation of the controller. AT pointed out that such criterion would avoid the situation that, depending on the processing activity concerned, there would be a different main establishment and consequently a different lead DPA.

[73] BE reservation.

b) data subjects residing in this Member State are substantially[74] affected or likely to be substantially affected by the processing; or

c) the underlying complaint has been lodged to that supervisory authority.

(19b) "transnational processing of personal data" means either:

(a) processing which takes place in the context of the activities of establishments in more than one Member State of a controller or a processor in the Union and the controller or processor is established in more than one Member State; or

(b) processing which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect[75] data subjects in more than one Member State.

(19c) "relevant and reasoned objection" means :

an objection as to whether there is an infringement of this Regulation or not, or, as the case may be, whether the envisaged action in relation to the controller or processor is in conformity with the Regulation. The objection shall clearly demonstrate[76] the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects[77] and where applicable, the free flow of personal data.

---

74 IE and UK would prefer the term 'materially'.

75 Several Member States thought that this should be clarified in recital: CZ, FI, HU, SE.

76 BE thought that this was a threshold too high.

77 IE thought that also risks to the controller should be covered.

CHAPTER VI
INDEPENDENT SUPERVISORY AUTHORITIES

SECTION 1
INDEPENDENT STATUS

Article 46

Supervisory authority

1. Each Member State shall provide that one or more independent public authorities are responsible for monitoring the application of this Regulation.

1a. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union (…). For this purpose, the supervisory authorities shall co-operate with each other and the Commission in accordance with Chapter VII.

2. Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority which shall represent those authorities in the European Data Protection Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 57.

[3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to this Chapter, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them[78]].

Article 47

Independence

1. Each supervisory authority shall act with complete independence in performing the duties[79] and *exercising* the powers entrusted to it in accordance with this Regulation.

---

78 DE, FR and EE that thought that this paragraph could be moved to the final provisions.

79 GR scrutiny reservation.

2. The member or members of each supervisory authority shall, in the performance of their duties and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect and neither seek nor take instructions from anybody[80].

3. (…)[81]

4. (…)[82]

5. Each Member State shall ensure that each supervisory authority is provided with the (…) human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and exercise of its powers, including those to be carried out in the context of mutual assistance, co-operation and participation in the European Data Protection Board.

6. Each Member State shall ensure that each supervisory authority has its own staff which shall (…) be subject to the direction of the member or members of the supervisory authority.

7. Member States shall ensure that each supervisory authority is subject to financial control[83] which shall not affect its independence. Member States shall ensure that each supervisory authority has separate, public, annual budgets, which may be part of the overall state or national budget.

---

80 IE reservation: IE thought the latter part of this paragraph was worded too strongly.

81 AT, BE, DE and HU would prefer to reinstate this text. CZ, EE and SE were satisfied with the deletion.

82 COM and DE, AT reservation on deletion of paragraphs 3 and 4.

83 EE reservation.

Article 48

General conditions for the members of the supervisory authority

1. Member States shall provide that the member or members of each supervisory authority must be appointed (…) by the parliament and/or the government or the head of State of the Member State concerned or by an independent body entrusted by Member State law with the appointment by means of a transparent procedure[84].

2. The member or members shall have the qualifications, experience and skills required to perform their duties and exercise their powers.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement in accordance with the law of the Member State concerned[85].

4. (…)

5. (…)[86].

---

84 Several delegations (FR, SE, SI and UK) thought that other modes of appointment should have been allowed for. FR (and RO) thought that a recital should clarify that "independent body" also covers courts.

85 COM reservation and DE scrutiny reservation on the expression "in accordance with the law of the Member States concerned". The question is whether this means that the Member States are being granted the power to define the duties further or whether the wording should be understood as meaning that only constitutional conditions or other legal framework conditions (e.g. civil service law) should be taken into account. DE and HU also suggest that rules in the event of death or invalidity be added (see, for example, Article 42(4) of Regulation (EC) No 45/2001) as well as referring to a procedure for the nomination of a representative in case the member is prevented from performing his or her duties. CZ, NO, SE see no need for paragraph 3

86 COM, DE and AT scrutiny reservation on deletion of paragraphs 4 and 5.

Article 49

Rules on the establishment of the supervisory authority

1. Each Member State shall provide by law for:

(a) the establishment (…) of each supervisory authority;

(b) the qualifications (…) required to perform the duties of the members of the supervisory authority[87];

(c) the rules and procedures for the appointment of the member or members of each supervisory authority (…);

(d) the duration of the term of the member or members of each supervisory authority which shall not be (…) less than four years, except for the first appointment after entry into force of this Regulation, part of which may take place for a shorter period where this is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;

(e) whether and, if so, for how many terms the member or members of each supervisory authority shall be eligible for reappointment;

(f) the (…) conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions and occupations incompatible therewith during and after the term of office and rules governing the cessation of employment;

(g) (…)[88].

2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy *both during and after their term of office*, with regard to any confidential information which has come to their knowledge in the course of the performance of their (…) duties or exercise of their powers.

---

87 IE reservation: IE thought these qualifications need not be laid down in law.

88 CZ, DE scrutiny reservation on deletion of this point.

Article 50

Professional secrecy

(…)

SECTION 2
COMPETENCE, TASKS AND POWERS

Article 51

Competence

1. Each supervisory authority shall be competent to perform the tasks and exercise the powers conferred on it in accordance with this Regulation on the territory of its own Member State. (…)
2. Where the processing is carried out by public authorities or private bodies acting on the basis of points (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent[89]. In such cases Article 51a does not apply.

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity[90]. (…).

Article 51a

Competence of the lead supervisory authority

1. Without prejudice to Article 51, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the transnational processing of this controller or processor in accordance with the procedure in Article 54a.

2. (…)

---

89 COM opposes the exclusion of private bodies from the one-stop mechanism, pointing to the example of cross-border infrastructure provided by private bodies in the public interest. AT, IE, FR and FI preferred to refer to ' processing carried out by public authorities and bodies of a Member State or by private bodies acting on the basis of a legal obligation to discharge functions in the public interest'.

90 FR, HU, RO and UK scrutiny reservation. DE suggested adding "other matters assigned to courts for independent performance. The same shall apply insofar as judicially independent processing has been ordered, approved or declared admissible", as the derogation must apply whenever courts' work falls within the scope of their institutional independence, which is not only the case in the core area of judicial activity but also in areas where courts are assigned tasks specifically for independent performance.

2a. By derogation from paragraph 1, each supervisory authority shall be competent to deal with a complaint lodged with it or to deal with a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

2b. In the cases referred to in paragraph 2a, the supervisory authority shall inform the lead supervisory authority without delay on this matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will deal with the case in accordance with the procedure provided in Article 54a, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

2c. Where the lead supervisory authority decides to deal with the case, the procedure provided in Article 54a shall apply. The supervisory authority which informed the lead supervisory authority may submit to such supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in paragraph 2 of Article 54a.

2d. In case the lead supervisory authority decides not to deal with it, the supervisory authority which informed the lead supervisory authority shall deal with the case according to Articles 55 and 56.

3. The lead supervisory authority shall be the sole interlocutor of the controller or processor for their transnational processing.

4. (…).

Article 51b

Identification of the supervisory authority competent for the main establishment

(…)

Article 51c

One-stop shop register

(…)[91]

Article 52

Tasks [92]

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

(aa) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data. Activities addressed specifically to children shall receive specific attention;

(ab) advise, in accordance with national law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data;

(ac) promote the awareness of controllers and processors of their obligations under this Regulation;

(ad) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end;

---

[91] AT reservation on the deletion of Articles 51b and 51c.

[92] DE, IT, AT, PT and SE scrutiny reservation.

(b) deal with complaints lodged by a data subject, or body, organisation or association representing a data subject in accordance with Article 73, and investigate, to the extent appropriate, the subject matter of the complaint and inform the data subject or the body, organisation or association 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;

(c) cooperate with, including sharing information, and provide mutual assistance to other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

(d) conduct investigations on the application of this Regulation, including on the basis of ~~a~~ information received from another supervisory or other public authority;

(e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(f) adopt standard contractual clauses referred to in Article 26(2c);

(fa) establish and make a list in relation to the requirement for data protection impact assessment pursuant to Article 33(2a);

(g) give advice on the processing operations referred to in Article 34(3);

(ga) encourage the drawing up of codes of conduct pursuant to Article 38 and give an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 38 (2);

(gb) promote the establishment of data protection certification mechanisms and of data protection seals and marks, and approve the criteria of certification pursuant to Article 39 (2a)**;**

(gc) where applicable, carry out a periodic review of certifications issued in accordance with Article 39(4);

(h) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 38a and of a certification body pursuant to Article 39a;

(ha) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 38a and of a certification body pursuant to Article 39a;

(hb) authorise contractual clauses referred to in Article 42(2a)(a);

(i) approve binding corporate rules pursuant to Article 43;

(j) contribute to the activities of the European Data Protection Board;

(k) fulfil any other tasks related to the protection of personal data.

2. (…)

3. (…).

4. Each supervisory authority shall facilitate the submission of complaints referred to in point (b) of paragraph 1, by measures such as providing a complaint submission form which can be completed also electronically, without excluding other means of communication.

5. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and for the data protection officer, if any.

6. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request[93].

[93] DE and SE reservation: this could be left to general rules.

Article 53

Powers[94]

1. Each Member State shall provide by law that its supervisory authority shall have at least[95] the following investigative powers:

(a) to order the controller and the processor, and, where applicable, the controller's representative to provide any information it requires for the performance of its tasks;

(aa) to carry out investigations in the form of data protection audits[96];

(ab) to carry out a review on certifications issued pursuant to Article 39(4);

(b) (…)

(c) (…)

(d) to notify the controller or the processor of an alleged infringement of this Regulation;

(da) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

(db) to obtain access to any premises of the controller and the processor , including to any data processing equipment and means, in conformity with Union law or Member State procedural law.

---

94 DE, RO, PT and SE scrutiny reservation; SE thought this list was too broad. Some Member States were uncertain (CZ, RO and UK) or opposed (DE, DK, and IE) to categorising the DPA powers according to their nature.

95 RO argued in favour of the inclusion of an explicit reference to the power of DPAs to issue administrative orders regarding the uniform application of certain data protection rules. COM and ES scrutiny reservation on 'at least' in paragraphs 1 and 1a.

96 CZ, IT, PL scrutiny reservation. CZ and PL pleaded for a recital explaining that audit could be understood as inspection.

1a. (…).

1b. Each Member State shall provide by law that its supervisory authority 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[97] to a controller or processor where processing operations have infringed provisions of this Regulation[98];

(c) (…);

(ca) 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;

(d) 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; in particular by ordering the rectification, restriction or erasure of data pursuant to Articles 16, 17 and 17a and the notification of such actions to recipients to whom the data have been disclosed pursuant to Articles 17(2a) and 17b;

(e) to impose a temporary or definitive limitation on processing (…);

(f) to order the suspension of data flows to a recipient in a third country or to an international organisation;

(g) to impose an administrative fine pursuant to Articles 79 and 79a[99], in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case.

---

97 PL scrutiny reservation.

98 PL scrutiny reservation on points (a) and (b).

99 DK constitutional reservation on the introduction of administrative fines, irrespective of the level of the fines.

1c. Each Member State shall provide by law that its supervisory authority shall have the following authorisation and advisory powers:

(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 34,

(aa) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with national law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

(ab) to authorise processing referred to in Article 34(7a), if the law of the Member State requires such prior authorisation;

(ac) to issue an opinion and approve draft codes of conduct pursuant to Article 38(2);

(ad) to accredit certification bodies under the terms of Article 39a;

(ae) to issue certifications and approve criteria of certification in accordance with Article 39(2a);

(b) to adopt standard data protection clauses referred to in point (c) of Article 42(2);

(c) to authorise contractual clauses referred to in point (a) of Article 42 (2a);

(ca) to authorise administrative agreements referred to in point (d) of Article 42 (2a);

(d) to approve binding corporate rules pursuant to Article 43.

2. *The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter of Fundamental Rights of the European Union.*[100]

3. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and (…), where appropriate, to commence or engage otherwise in legal proceedings[101], in order to enforce the provisions of this Regulation[102].

4. (…)

5. (…)

---

100 CY, ES, FR, IT and RO thought this could be put in a recital as these obligations were binding upon the Member States at any rate.

101 DE, FR and RO reservation on proposed DPA power to engage in legal proceedings. UK scrutiny reservation. CZ and HU reservation on the power to bring this to the attention of the judicial authorities.

102 DE thought para. 3 should be deleted.

Article 54

Activity Report

Each supervisory authority shall draw up an annual report of its activities. The report shall be transmitted to the national Parliament, the government and other authorities as designated by national law. It shall be made available to the public, the European Commission and the European Data Protection Board.

CHAPTER VII[103]
CO-OPERATION AND CONSISTENCY
SECTION 1
CO-OPERATION

Article 54a

Cooperation between the lead supervisory authority and other concerned supervisory authorities [104]

1. The lead supervisory authority (…) shall cooperate with the other concerned supervisory authorities in accordance with this article in an endeavour to reach consensus (…). The lead supervisory authority and the concerned supervisory authorities shall exchange all relevant information with each other.

1a. The lead supervisory authority may request at any time other concerned supervisory authorities to provide mutual assistance pursuant to Article 55 and may conduct joint operations pursuant to Article 56, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.

2. The lead supervisory authority shall, without delay communicate the relevant information on the matter to the other concerned supervisory authorities. It shall without delay submit a draft decision to the other concerned supervisory authorities for their opinion and take due account of their views.

---

103 AT and FR scrutiny reservation on Chapter VII.

104 CZ, CY, DE, EE, FR, FI, IE, LU, RO and PT scrutiny reservation.

3. Where any[105] of the other concerned supervisory authorities within a period of four weeks after having been consulted in accordance with paragraph 2, expresses a relevant and reasoned objection *to the draft decision*, the lead supervisory authority shall, if it does not follow the objection or is of the opinion it is not relevant and reasoned, submit the matter to the consistency mechanism referred to in Article 57. (…)

3a. Where the lead supervisory authority intends to follow the objection made, it shall submit to the other concerned supervisory authorities a revised draft decision for their opinion. This revised draft decision shall be subject to the procedure referred to in paragraph 3 within a period of two weeks.

4. Where none of the other concerned supervisory authority has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 3 and 3a, the lead supervisory authority and the concerned supervisory authorities shall be deemed to be in agreement with this draft decision and shall be bound by it.

4a. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other concerned supervisory authorities and the European Data Protection Board of the decision in question including a summary of the relevant facts and grounds. The supervisory authority to which a complaint has been lodged shall inform the complainant on the decision.

4b. By derogation from paragraph 4a, where a complaint is dismissed or rejected, the supervisory authority to which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

---

105 A number of Member States (CZ, IE, NL, PL, FI and UK) still prefers a quantitative threshold by which an objection would need to be supported by 1/3 of the concerned supervisory authorities before the lead authority is obliged to refer the matter to the EDPB.

4bb. Where the lead supervisory authority and the concerned supervisory authorities are in agreement to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter.The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller and notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof[106], while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint and notify it on that complainant[107] and shall inform the controller or processor thereof. [108]

4c. After being notified of the decision of the lead supervisory authority pursuant to paragraph 4a and 4bb, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards the processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other concerned supervisory authorities.

4d. Where, in exceptional circumstances, a concerned supervisory authority has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 61 shall apply.

5. The lead supervisory authority and the other concerned supervisory authorities shall supply the information required under this Article (…) to each other by electronic means, using a standardised format.

---

106 Further to suggestions from HU and IE.

107 SI scrutiny reservation. PL reservation on paras 4b and 4bb: PL and FI thought para. 4bb should be deleted as it was opposed to the concept of a split decision. IT thought para 4bb overlapped with para 4b.

108 Further to suggestions from HU and IE.

Article 54b

Cooperation between the lead supervisory authority and the other supervisory authorities concerned in individual cases of possible non-compliance with the Regulation

(…)

Article 55

Mutual assistance[109]

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations. (...)

2. Each supervisory authority shall take all appropriate measures required to reply to the request of another supervisory authority without undue delay and no later than one month[110] after having received the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation (…).

3. The request for assistance shall contain all the necessary information[111], including the purpose of the request and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

4. A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless:

---

109 DE, SE and UK scrutiny reservation.

110 ES, supported by PT, had suggested 15 days. RO and SE found one month too short. COM indicated that it was only a deadline for replying, but that paragraph 5 allowed longer periods for executing the assistance requested.

111 EE and SE scrutiny reservation.

(a) it is not competent for the subject-matter of the request or for the measures it is requested to execute[112]; or

(b) compliance with the request would be incompatible with the provisions of this Regulation or with Union or Member State law to which the supervisory authority receiving the request is subject.

5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to respond to the request. In cases of a refusal under paragraph 4, it shall explain its reasons for refusing the request[113].

6. Supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means[114], using a standardised format.

7. No fee shall be charged for any action taken following a request for mutual assistance. Supervisory authorities may agree with other supervisory authorities rules for indemnification by other supervisory authorities for specific expenditure arising from the provision of mutual assistance in exceptional circumstances[115].

---

112 Several delegations stressed the importance of establishing which is the competent DPA: DE, EE, SE, SI, and IT asked for further clarification.

113 RO scrutiny reservation.

114 PT (supported by RO) suggested adding "or other means if for some reason, electronic means are not available, and the communication is urgent".

115 PT, UK and DE asked for clarification in relation to the resources needed / and estimate of costs.

8. Where a supervisory authority does not provide the information referred to in paragraph 5 within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure[116] on the territory of its Member State in accordance with Article 51(1) and shall submit the matter to the European Data Protection Board (…) in accordance with the consistency mechanism referred to in Article 57[117].

9. The supervisory authority shall specify the period of validity of such a provisional measure which shall not exceed three months[118]. The supervisory authority shall, without delay, communicate such a measure, together with its reasons for adopting it, to the European Data Protection Board (…) in accordance with the consistency mechanism referred to in Article 57.

10. The Commission may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)[119].

---

116 LU requested more clarification with regard to what would happen if this provisional measure were not confirmed.

117 EE, FR, RO and UK reservation. DE scrutiny.

118 DE asked for deletion of this deadline; the measure should be withdrawn if the conditions for imposing it were no longer fulfilled.

119 DE, IT, EE and CZ reservation.

Article 56

Joint operations of supervisory authorities[120]

1. The supervisory authorities may, where appropriate, conduct joint operations, including joint investigations and joint enforcement measures in which members or staff from other Member States' supervisory authorities are involved.

2. In cases where the controller or processor has establishments in several Member States or where a significant number of[121] data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in the joint operations, as appropriate. The competent supervisory authority shall invite the supervisory authority of each of those Member States to take part in the joint operations concerned and respond without delay to the request of a supervisory authority to participate.

3. A supervisory authority may, in compliance with its own Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the host supervisory authority's national law. (…) [122]

---

120 DE, EE, PT and UK scrutiny reservation.

121 COM reservation; IT, supported by FR and CZ suggested stressing the multilateral aspect.

122 DE, LU, PT and COM scrutiny reservation on the deletion of this last phrase.

3a. Where, in accordance with paragraph 1, staff of a seconding supervisory authority are operating in another Member State, the Member State of the host supervisory authority shall be liable for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.

3b. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse the latter in full any sums it has paid to the persons entitled on their behalf.

3c. Without prejudice to the exercise of its rights vis-à-vis third parties and with the exception of paragraph 3b, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement of damages it has sustained from another Member State[123].

4. (…)

5. Where a joint operation is intended and a supervisory authority does not comply within one month with the obligation laid down in the second sentence of paragraph 2, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 51(1).

6. The supervisory authority shall specify the period of validity of a provisional measure referred to in paragraph 5, which shall not exceed three months. The supervisory authority shall, without delay, communicate such a measure, together with its reasons for adopting it, to the European Data Protection Board (…) in accordance with the consistency mechanism referred to in Article 57.

123 UK reservation on paras. 3a, 3b and 3c.

SECTION 2

CONSISTENCY[124]

Article 57

Consistency mechanism[125]

1. For the purpose set out in Article 46(1a), the supervisory authorities shall co-operate with each other through the consistency mechanism as set out in this section[126].

2. The European Data Protection Board shall issue an opinion whenever a competent *supervisory authority* intends *to adopt* any of the measures below (…). To that end, the competent supervisory authority shall communicate the draft decision to the European Data Protection Board, when it:

   (a) (…);

   (b) (…);

   (c) aims at adopting a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 33(2a); or

   (ca) concerns a matter pursuant to Article 38(2b) whether a draft code of conduct or an amendment or extension to a code of conduct is in compliance with this Regulation; or

   (cb) aims at approving the criteria for accreditation of a body pursuant to paragraph 3 of Article 38a or a certification body pursuant to (…) paragraph 3 of Article 39a;

---

124 IT and SI scrutiny reservation. DE parliamentary reservation and UK reservation on the role of COM in the consistency mechanism.

125 EE, FI and UK scrutiny reservation.

126 CZ, DE, ES and RO thought that supervisory authorities of third countries for which there is an adequacy decision should be involved in the consistency mechanism; if third countries participated in the consistency mechanism, they would be bound by uniform implementation and interpretation.

(d) aims at determining standard data protection clauses referred to in point (c) of Article 42(2); or

(e) aims to authorising contractual clauses referred to in point (d) of Article 42(2); or

(f) aims at approving binding corporate rules within the meaning of Article 43.

3. The European Data Protection Board shall adopt a binding decision in the following cases:

a) Where, in a case referred to in paragraph 3 of Article 54a, a *concerned* supervisory authority has expressed a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected an objection as being not relevant and/or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of the Regulation;

b) Where, there are conflicting views on which of the *concerned* supervisory authorities is competent for the main establishment;

c) (…)

d) Where a competent supervisory authority does not request the opinion of the European Data Protection Board in the cases mentioned in paragraph 2 of this Article, or does not follow the opinion of the European Data Protection Board issued under Article 58. In that case, any concerned supervisory authority or the Commission may communicate the matter to the European Data Protection Board.

4. Any supervisory authority, the Chair of the European Data Protection Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the European Data Protection Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.

5. Supervisory authorities and the Commission shall electronically communicate to the European Data Protection Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft decision, the grounds which make the enactment of such measure necessary, and the views of other *concerned* supervisory authorities.

6. The chair of the European Data Protection Board shall without undue delay electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat of the European Data Protection Board shall, where necessary, provide translations of relevant information.

Article 58

Opinion by the European Data Protection Board[127]

1. (…)

2. (…)

3. (…)

4. (…)

5. (…)

6. (…)

[127] UK scrutiny reservation.

7. In the cases referred to in paragraphs 2 and 4 of Article 57, the European Data Protection Board shall issue an opinion on the subject- matter submitted to it provided it has not already issued an opinion on the same matter. This opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. This period may be extended by a further month, taking into account the complexity of the subject matter. Regarding the draft decision circulated to the members of the Board in accordance with paragraph 6 of Article 57, a member which has not objected within the period indicated by the Chair, shall be deemed to be in agreement with the draft decision.

7a. Within the period referred to in paragraph 7 the competent supervisory authority shall not adopt its draft decision in accordance with paragraph 2 of Article 57.

7b. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 2 and 4 of Article 57 and the Commission of the opinion and make it public.

8. The supervisory authority referred to in paragraph 2 of Article 57 shall take utmost account of the opinion of the European Data Protection Board and shall within two weeks after receiving the opinion, electronically communicate to the chair of the European Data Protection Board whether it maintains or will amend its draft decision and, if any, the amended draft decision, using a standardised format.

9. Where the concerned supervisory authority informs the chair of the European Data Protection Board within the period referred to in paragraph 8 that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, paragraph **3** of Article 57 shall apply.

10. (…)

11. (…)

Article 58a

Decisions by the European Data Protection Board[128]

1. In the cases referred to in paragraph 3 of Article 57, the European Data Protection Board shall adopt a decision on the subject-matter submitted to it in order to ensure the correct and consistent application of this Regulation in individual cases. The decision shall be reasoned and addressed to the lead supervisory authority and all the concerned supervisory authorities and binding on them.

2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-third majority of the members of the Board. This period may be extended by a further month on account of the complexity of the subject-matter.

3. In case the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board[129]. In case the members of the Board are split, the decision shall by adopted by the vote of its Chair.

4. The concerned supervisory authorities shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.

5. (…)

---

128 PL scrutiny reservation. IE thought the controller should have standing to intervene in the proceedings before the EDPB.

129 AT and HU reservation. HU believes that this option will make the general two-thirds majority rule meaningless and symbolic, since there will be no effective incentive for the EDPB to adopt a decision that reflects the view of the vast majority of DPAs of the Member States, as eventually every decision could be adopted by only a slight majority of them. It would also undermine the general validity of the EDPB's decision, since the fact that the Board could not come to an agreement on a particular matter supported by at least the two-thirds of its members might give rise to serious doubts whether the finding of such decision is commonly shared across the Union. AT believes that a simple majority would be more effective and would not prolong the procedure.

6. The Chair of the European Data Protection Board shall notify, without undue delay, the decision referred to in paragraph 1 to the concerned supervisory authorities. It shall inform the Commission thereof. The decision shall be published on the website of the European Data Protection Board without delay after the supervisory authority has notified the final decision referred to in paragraph 7.

7. The lead supervisory authority or, as the case may be, the supervisory authority to which the complaint has been lodged shall adopt their final decision on the basis of the decision referred to in paragraph 1[130], without undue delay and at the latest by one month after the European Data Protection Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority to which the complaint has been lodged, shall inform the European Data Protection Board of the date when its final decision is notified respectively to the controller or the processor and the data subject. The final decision of the concerned supervisory authorities shall be adopted under the terms of Article 54a, paragraph 4a, 4b and 4bb. The final decision shall refer to the decision referred to in paragraph 1 and shall specify that the decision referred to in paragraph 1 will be published on the website of the European Data Protection Board in accordance with paragraph 6. The final decision shall attach the decision referred to in paragraph 1.

Article 59

Opinion by the Commission[131]

(…)

130 FI reservation; would prefer a system under which the EDPB decision would be directly applicable and would not have to be transposed by the lead DPA.

131 COM and FR reservation on deletion.

Article 60

Suspension of a draft measure[132]

(…)

Article 61

Urgency procedure[133]

1. In exceptional circumstances, where a concerned supervisory authority considers that there is an urgent need to act in order to protect rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Article 57[134] or the procedure referred to in Article 54a, immediately adopt provisional measures intended to produce legal effects within the territory of its own Member State[135], with a specified period of validity. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them, to the other concerned supervisory authorities, the European Data Protection Board and to the Commission.

2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the European Data Protection Board, giving reasons for requesting such opinion or decision.

---

132 COM and FR reservation on deletion.

133 DE scrutiny reservation.

134 HU remarked that it should be clarified whether provisional measures can be adopted pending a decision by the EDPB. The Presidency thinks that the reference to Article 57 makes it clear that this is indeed possible.

135 COM scrutiny reservation.

3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the European Data Protection Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.

4. By derogation from paragraph 7 of Article 58 and paragraph 2 of Article 58a, an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.

Article 62

Implementing acts

1. The Commission may adopt implementing acts of general scope for:

   (a) (…)[136];

   (b) (…);

   (c) (…);

   (d) specifying the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in Article 57(5) and (6) and in Article 58(8).

   Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

[136] COM reservation on deletion.

2. (…)

3. (…)

Article 63

Enforcement

(…)

SECTION 3
EUROPEAN DATA PROTECTION BOARD

Article 64

European Data Protection Board

1a. The European Data Protection Board is hereby established as body of the Union and shall have legal personality.

1b. The European Data Protection Board shall be represented by its Chair**.**

2. The European Data Protection Board shall be composed of the head of one supervisory authority of each Member State or his/her representative ~~and of the European Data Protection Supervisor~~.

3. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, (…) a joint representative shall be appointed in accordance with the national law of that Member State.

4. The Commission and the European Data Protection Supervisor or his/her representative shall have the right to participate in the activities and meetings of the European Data Protection Board *without voting right*. The Commission shall designate a representative. The chair of the European Data Protection Board shall, communicate to the Commission **(…)** the activities of the European Data Protection Board.

Article 65

Independence

1. The European Data Protection Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 66 (…) and 67.[137]

2. Without prejudice to requests by the Commission referred to in point (b) of paragraph 1 and in paragraph 2 of Article 66, the European Data Protection Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody[138].

Article 66

Tasks of the European Data Protection Board

1. The European Data Protection Board shall promote the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the Commission, in particular:

   (aa) monitor and ensure the correct application of this Regulation in the cases provided for in Article 57(3) without prejudice to the tasks of national supervisory authorities;

   (a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;

   (b) examine, on its own initiative or on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation;

137 UK and SI scrutiny reservation.
138 DE scrutiny reservation.

(ba) draw up guidelines for supervisory authorities concerning the application of measures referred to in paragraph 1, 1b and 1c of Article 53 and the fixing of administrative fines pursuant to Articles 79 and 79a[139];

(c) review the practical application of the guidelines, recommendations and best practices referred to in points (b) and (ba);

(ca) encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 38 and 39;

(cb) carry out the accreditation of certification bodies and its periodic review pursuant to Article 39a and maintain a public register of accredited bodies pursuant to paragraph 6 of Article 39a and of the accredited controllers or processors established in third countries pursuant to paragraph 4 of Article 39[140];

(cd) specify the requirements mentioned in paragraph 3 of Article 39a with a view to the accreditation of certification bodies under Article 39;

(ce) give the Commission an opinion on the level of protection of personal data in third countries or international organisations, in particular in the cases referred to in Article 41;

(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in paragraph 2 and on matters submitted pursuant to paragraph 4 of Article 57;

(e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities;

---

139 DK constitutional reservation on the introduction of administrative fines, irrespective of the level of the fines.

140 HU said that paragraphs (ca) and (cb) were contrary to the text of the general approach reached in June 2014 (11028/14); it is for the national supervisory authority to do this.

(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;

(g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide;

(h) (…);

(i) maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues dealt with in the consistency mechanism.

2. Where the Commission requests advice from the European Data Protection Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 87 and make them public.

Article 67

Reports

1. (…)

2. The European Data Protection Board *shall draw up an annual report regarding the protection of natural persons with regard to the processing of personal data in the Union and*, where relevant, *in third countries* and international organisations. The report shall be made public and be transmitted to the European Parliament, the Council and the Commission.

3. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (c) of Article 66(1) as well as of the binding decisions referred to in paragraph 3 of Article 57.

Article 68

Procedure

1. The European Data Protection Board shall adopt binding decisions referred to in paragraph 3 of Article 57 in accordance with majority requirements set out in paragraphs 2 and 3 of Article 58a. As regards decisions related to the other tasks listed in Article 66 hereof, they shall be taken by a simple majority of its members.

2. The European Data Protection Board shall adopt its own rules of procedure by a two-third majority of its members and organise its own operational arrangements.

Article 69

Chair

1. The European Data Protection Board shall elect a chair and two deputy chairs from amongst its members by simple majority[141](…)[142].

2. The term of office of the chair and of the deputy chairs shall be five years and be renewable once[143].

---

141 IE proposal.
142 COM reservation on deletion.
143 COM scrutiny reservation.

Article 70

Tasks of the chair

1. The chair shall have the following tasks:

   (a) to convene the meetings of the European Data Protection Board and prepare its agenda;

   (aa) to notify decisions adopted by the European Data Protection Board pursuant to Article 58a to the lead supervisory authority and the *concerned* supervisory authorities;

   (b) to ensure the timely performance of the tasks of the European Data Protection Board, in particular in relation to the consistency mechanism referred to in Article 57.

2. The European Data Protection Board shall lay down the attribution of tasks between the chair and the deputy chairpersons in its rules of procedure.

Article 71

Secretariat

1. The European Data Protection Board shall have a secretariat, which shall be provided by the secretariat of the European Data Protection Supervisor (…).

1a. The secretariat shall perform its tasks exclusively under the instructions of the Chair of the European Data Protection Board.

1b. The staff of the secretariat of the European Data Protection Supervisor involved in carrying out the tasks conferred on the European Data Protection Board by this Regulation shall be organizationally separated from, and subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor[144].

1c. Where needed, the European Data Protection Board in consultation with the European Data Protection Supervisor shall establish and publish a Code of Conduct implementing this Article and applicable to the staff of the secretariat of the European Data Protection Supervisor involved in carrying out the tasks conferred on the European Data Protection Board by this Regulation.

2. The secretariat shall provide analytical[145], administrative and logistical support to the European Data Protection Board.

3. The secretariat shall be responsible in particular for:

   (a) the day-to-day business of the European Data Protection Board;

   (b) the communication between the members of the European Data Protection Board, its chair, and the Commission and for communication with other institutions and the public;

   (c) the use of electronic means for the internal and external communication;

---

144 CZ reservation on last part of the task.

145 UK suggested deleting "analytical".

(d) the translation of relevant information;

(e) the preparation and follow-up of the meetings of the European Data Protection Board;

(f) the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the European Data Protection Board.

Article 72

Confidentiality[146]

1. The discussions[147] of the European Data Protection Board shall be confidential.

2. Access to documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001.

---

146 DE, EE, ES, RO, PL, PT, SE and UK reservation: it was thought that the EDPB should operate in a manner as transparent as possible and a general confidentiality duty was obviously not conducive to this. This article should be revisited once there is more clarity on the exact role and powers of the board, including the question whether the EDPS shall ensure the Secretariat.

147 IT scrutiny reservation: it suggested replacing this term with 'minutes' or 'summary records', thereby distinguishing between confidentiality of decision-making and access to documents.