Council of the European Union

Brussels, 17 September 2015
(OR. en)

11972/15

Interinstitutional File:
2012/0010 (COD)

LIMITE

DATAPROTECT 137
JAI 654
DAPIX 147
FREMP 181
COMIX 400
CODEC 1177

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	10964/15, 11251/15, 11252/15
No. Cion doc.:	5833/12
Subject:	Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the free movement of such data

1. Delegations will find attached the full text of the Directive in subject. Chapters II, III, VI and VIII will be discussed at the Friends of the Presidency meeting on 21-22 September and Chapters I, IV, V, VII, IX and X in Coreper on 23 September 2015.
2. Delegations are informed that for the purposes of this document the text of chapters II and VIII is identical to the text in document 11711/15.
3. The note to Coreper is set out in document 11978/15 and to the Friends of the Presidency in document 11975/15.

4. All changes made to the original Commission proposal are underlined; where text has been deleted, this is indicated by (…). Where existing text has been moved, this text is indicated in *italics*. Changes compared to the previous documents 11251/15 and 11252/15 (N.B. for Chapters I, II and VIII the text is identical to doc 11711/15) are marked in **bold** and deleted text in ~~strikethrough~~. The comments of delegations are reflected in the footnotes.

ANNEX

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or the safeguarding against and the prevention of threats to public security, and the free movement of such data[1]

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2) thereof,

Having regard to the proposal from the European Commission,

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

After consulting the European Data Protection Supervisor[2],

[1] DE, ES, FI, HU, IT, NL, LV, PT, SI, UK scrutiny reservation on the whole text.

[2] OJ C… , p.

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty of the Functioning of the European Union lay down that everyone has the right to the protection of personal data concerning him or her.

(2) The (…) principles and rules on the protection of individuals with regard to the processing of their personal data should, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their right to the protection of personal data. It should contribute to the accomplishment of an area of freedom, security and justice.

(3) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data collection and sharing has increased spectacularly. Technology allows (…) to make use of personal data on an unprecedented scale in order to pursue (…) activities such as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

(4) This requires facilitating the free flow of data between competent (…) authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences *or the execution of criminal* penalties or the safeguarding against and the prevention of threats to public security within the Union and the transfer to third countries and international organisations, while ensuring a high level of protection of personal data. These developments require building a strong and more coherent data protection framework in the Union, backed by strong enforcement.

(5) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[3] applies to all personal data processing activities in Member States in both the public and the private sectors. However, it does not apply to the processing of personal data 'in the course of an activity which falls outside the scope of Community law', such as activities in the areas of judicial co-operation in criminal matters and police co-operation.

[3] OJ L 281, 23.11.1995, p. 31.

(6) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters[4] applies in the areas of judicial co-operation in criminal matters and police co-operation. The scope of application of this Framework Decision is limited to the processing of personal data transmitted or made available between Member States.

(7) Ensuring a consistent and high level of protection of the personal data of individuals and facilitating the exchange of personal data between competent (…) authorities of Members States is crucial in order to ensure effective judicial co-operation in criminal matters and police cooperation. To that aim, the level of protection of the rights and freedoms of individuals with regard to the processing of personal data by competent (…) authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences *or the execution of criminal penalties* or the safeguarding against and the prevention of threats to public security should be equivalent in all Member States. Effective protection of personal data throughout the Union requires strengthening the rights of data subjects and the obligations of those who process personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data in the Member States. [5]

(8) Article 16(2) of the Treaty on the Functioning of the European Union mandates the European Parliament and the Council to lay down the rules relating to the protection of individuals with regard to the processing of personal data and the rules relating to the free movement of personal data.

(9) On that basis, Regulation EU …../XXX 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) lays down general rules to protect (…) individuals in relation to the processing of personal data and to ensure the free movement of personal data within the Union.

---

4 OJ L 350, 30.12.2008, p. 60.

5 UK suggested the deletion of this recital since the case has not been made for the need of equivalent standards of data protection in all MS and is not in line with the subsidiarity principle.

(10) In Declaration 21 on the protection of personal data in the fields of judicial co-operation in criminal matters and police co-operation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the Conference acknowledged that specific rules on the protection of personal data and the free movement of such data in the fields of judicial co-operation in criminal matters and police co-operation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields.

(11) Therefore a distinct Directive should meet the specific nature of these fields and lay down the rules relating to the protection of individuals with regard to the processing of personal data by competent (…) authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences *or the execution of criminal penalties*[6]. Such competent authorities may include not only public authorities such as the judicial authorities, the police or other law enforcement authorities but also any body/entity entrusted by national law[7] to perform public duties or exercise public powers for the purposes of prevention, investigation, detection or prosecution of criminal offence or the *execution of criminal penalties*. However where such body/entity processes personal data for other purposes than for the performance of public duties and/or the exercise of public powers for the prevention, investigation, detection or prosecution of criminal offences *or the execution of criminal penalties*, Regulation XXX applies. Therefore Regulation XXX applies in cases where a body/entity, collects personal data for other purposes and further processes those personal data for compliance with a legal obligation to which it is subject *e.g.* financial institutions retain for the purpose of investigation, detection and prosecutions certain data which are processed by them, and provide those data only to the competent national authorities in specific cases and in accordance with national law. A body/entity which processes personal data on behalf of such authorities (…) within the scope of this Directive should be bound, by a contract or other legal act and the provisions applicable to processors pursuant to this Directive, while the application of Regulation XXX remains unaffected for processing activities of the processor outside the scope of this Directive.[8]

---

6 CH wanted to add the following sentence in the end of the recital: "At the same time the legitimate activities of the competent public authorities should not be jeopardized in any way."

7 UK said, in line with its comments on Article 3(14), that it preferred using *in accordance with national law'* rather than 'entrusted by'.

8 FI scrutiny reservation and SE reservation.

(11a) The activities carried out by the police or other law enforcement authorities are mainly focused on the prevention, investigation, detection or prosecution of criminal offences including police activities without prior knowledge if an incident is a criminal offence or not. These can also include the exercise of authority by taking coercive measures such as police activities at demonstrations, major sporting events and riots. [9]
Those activities performed by the above-mentioned authorities also include maintaining law and order as a task conferred on the police or other law enforcement authorities where necessary[10] to safeguard against and prevent threats to public security,[11] aimed at preventing human behaviour which may lead to threats to fundamental interests of the society protected by the law and which may lead to a criminal offence.

Member States may entrust competent authorities with other tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of the General Data Protection Regulation.

(11b) Since this Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, **activities concerning national security,** activities of agencies or units dealing with national security issues **and processing of personal data by the Member States when carrying out activities in relation to the Common Foreign and Security Policy of the Union,** should not be considered as (…) activities falling under the scope of this Directive.

---

9 DE suggested adding to the text 'Hereby 'criminal offence' covers all infringements of the rules of law which are punishable under national law, provided that the person concerned has the opportunity to have the case tried by a court having jurisdiction in particular in criminal matters'.
AT proposed to add to the recital: 'Administrative tasks such as tasks with regard to the right of association and assembly, immigration and asylum or civil protection shall not be considered as activities falling under the prevention of threat of public security.'

10 CZ wanted to replace 'where necessary' to 'in order to'.

11 LT and RO preferred to keep the 'or'

(12) In order to ensure the same level of protection for individuals through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between competent (…) authorities, the Directive should provide harmonised rules for the protection and the free movement of personal data (…) processed for the purposes of prevention, investigation, detection or prosecution of criminal offences *or the execution of criminal penalties* or the safeguarding against and the prevention of threats to public security. The approximation of Member States' laws should not result in any lessening of the data protection they afford but should, on the contrary, seek to ensure a high level of protection within the Union. Member States should not be precluded from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent (…) authorities.

(13) This Directive is without prejudice to the **(…)** principle of public access to official documents (…). Under ~~the~~ Regulation XXX personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union law or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data (…).

(14) The protection afforded by this Directive should concern natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.

(15) The protection of individuals should be technologically neutral and not depend on the technologies **(…),** used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means, as well as to manual processing if the data are contained or are intended to be contained in a filing system. Files or sets of files as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Directive.

(…)

(15a) Regulation (EC) No 45/2001[12] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal instruments applicable to such processing of personal data should be adapted to the principles and rules of Regulation XXX.

[12] OJ L 8, 12.1.2001, p. 1.

(15b) **(…)** This Directive does not preclude Member States from specifying processing operations and processing procedures in national rules on criminal procedures in relation to the processing of personal data by courts and other judicial authorities, in particular as regards personal data contained in a judicial decision or in records in relation to criminal proceedings. [13]

(16) The principles of data protection should apply to any information concerning an identified or identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means likely reasonably 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 no longer identifiable.

14

(16a) Genetic data should be defined as personal data relating to the genetic characteristics of an individual which have been inherited or acquired **(…)** which give unique information about the physiology or health of that individual, resulting in particular by chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained.[15] ~~**DNA profiles used by competent authorities with the purpose of identifying should be considered to be 'identifiers'**~~**.**

---

13 BE reservation of substance and SE scrutiny reservation.

14 CH suggested to insert a recital with the following text: "The transmitting Member State should have the possibility to subject the processing by the receiving Member State to conditions in particular with regard to the purpose for which personal data could be used, but it should not refuse the transmission of information to this State on the simple grounds that this State does not have an adequate data protection level." CH added the underlined sentence.

15 FR scrutiny reservation.

(17) 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 (…)**;** 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.[16]

(18) Any **processing of personal data must be (…) lawful and fair in relation to the individuals concerned, and only processed for specific purposes laid down by law. The principle of fair processing does not in itself prevent the law enforcement authorities from carrying out activities such as covert investigations or video surveillance. Such activities can be done for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or the safeguarding against and the prevention of threats to public security as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the individual concerned. Individuals should be made aware of risks[17], rules, safeguards and rights in relation to the processing of his/her 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. 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 not kept longer than is necessary for the purpose for which they are processed ~~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. 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.

---

16 FR scrutiny reservation.

17 DE wanted to delete the reference to *risks* because in the area of the Directive the data subject was obliged to have its data processed.

(19) For the prevention, investigation and prosecution of criminal offences it is necessary for competent (…) authorities to (…) process personal data, collected in the context of the prevention, investigation, detection or prosecution of specific[18] criminal offences beyond that context to develop an understanding of criminal phenomena and trends, to gather intelligence about organised criminal networks, and to make links between different offences detected.

(19a) In order to maintain security of the processing and to prevent processing in breach of this Directive, personal data should be processed in a manner that ensures an appropriate level of security and confidentiality, including preventing unauthorised access to or ~~the~~ use of personal data and the equipment used for the processing, taking into account available state of the art and technology and the costs of implementation in relation to the risks and the nature of the personal data to be protected.

~~(20) Personal data should be collected for specified, explicit and legitimate purposes within the scope of this Directive and not be processed for purposes incompatible with the purpose for which it was collected. (…)Personal data should be adequate, relevant and not excessive for the purposes for which the personal data are processed. (…).(…) Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted.~~

[18] ES, supported by HR, wanted to delete "specific" since crime prevention was not about a specific crime but related to group of offences or all offences.

(21) The principle of accuracy of data should be applied taking account of the nature and purpose of the processing concerned. Since personal data relating to different categories of data subjects are processed, *the competent* ***(...)*** *authorities (…) should, as far as possible*[19]*, make a distinction between personal data of different categories of data subjects such as persons convicted of a criminal offence, suspects, (…)victims and third parties.*[20] In particular in judicial proceedings, statements containing personal data are based on the subjective perception of individuals and are in some cases not always verifiable. Consequently, the requirement of accuracy should not appertain to the accuracy of a statement but merely to the fact that a specific statement has been made.

(22) In the interpretation and application of the provisions of this Directive, by competent (…) authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences *or the execution of criminal penalties* or the safeguarding against and the prevention of threats of public security, account should be taken of the specificities of the sector, including the specific objectives pursued.

(23) (…)[21]

(24) (…) The competent (…) authorities should (...) ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. ~~**In particular, personal data should be distinguished, as far as possible, according to the degree of their accuracy and reliability; (…) facts should be distinguished from personal assessments**~~ In order to ensure both the protection of individuals and the **accuracy, completeness or up-to-datedness** ~~quality~~ and reliability of the **personal data transmitted or made available** ~~processed by~~ the competent (…) authorities **should, as far as possible, add necessary *information* in all transmissions of personal data**.

---

19 CZ suggested to replace *possible* with *relevant.*CZ meant that it was unrealistic to distinguish between different categories of data.

20 DE scrutiny reservation on the addition of the new text.

21 Cion reservation on deletion. Cion said that both the Europol Convention and the Eurojust Regulation have an Article on the requirement of making a distinction of the different categories of data.

(24a) Wherever this Directive 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.

(24b) The processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or the safeguarding against and the prevention of threats to public security should cover any operation or set of operations which is performed upon personal data or sets of personal data for those purposes, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, alignment or combination, restriction, erasure or destruction as well as the disclosure to a recipient by transmission, dissemination or otherwise making available to any recipient. Such recipient should mean a natural or legal person, public authority, agency or any other body, to which the data are lawfully disclosed by the competent authority for those purposes. For the processing of personal data by a recipient or another authority who is not or is not acting as a competent authority in the meaning of this Directive and to whom personal data are lawfully disclosed by a competent authority, the General Data Protection Regulation should apply.

(25) In order to be lawful, the processing of personal data should be necessary for (…) the performance of a task carried out in the public interest by a competent authority based on Union law or Member State law for the purposes of prevention, investigation, detection or prosecution of criminal offences *or the execution of criminal penalties* or the safeguarding against and the prevention of threats to public security**,** including processing necessary (…) in order to protect the vital interests of the data subject or of another person **(…)**.[22] The performance of the task of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent authorities allows them to require/order individuals to abide to the requests made. In this case**,** the data subject's consent (as defined in Regulation XXX) should not provide a legal ground for processing personal data by competent (…) authorities. Where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the data subject's reaction could not be considered as a freely-given indication of his or her wishes. This should not preclude Member States to provide by law, for example, that an individual could be required **(…)** to agree to the monitoring of his/her location as a condition for probation or expressly authorize processing of data which can be particularly invasive for his/her person, such as processing of special categories of data**.**

22 CH, supported by HR, HU and CZ, suggested adding the following text after "public security": "Furthermore, a processing of personal data should be lawful if the data subject has given his or her consent to the processing of his or her personal data for one or more specific purposes. The data subject's consent means any freely-given specific, informed and explicit indication of his or her wishes by which the data subject signifies his agreement to personal data relating to him being processed."

(25a) Member States should provide that where Union law or the national law applicable to the transmitting competent (…) authority provides for specific conditions **applicable** in specific circumstances to the processing of personal data, such as for example the use of handling codes the transmitting (…) authority should inform the recipient to whom data are transmitted about such conditions and the requirement to respect them. Such conditions may for example include that the recipient to whom the data are transmitted **does not transmit further the data or use it for other purposes or** does not inform the data subject in case of a limitation to the right of information without the prior approval of the transmitting **competent** authority. These obligations apply also to transfers to recipients in third countries or international organisations. Member States should provide that the transmitting competent (…) authority does not apply such conditions **(…)** to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters IV and V of Title V of the Treaty on the Functioning of the European Union other than those applicable to similar **(…)**data transmissions within the Member State of the transmitting competent authority.

(26) 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 Directive 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 subject to appropriate safeguards for the rights and freedoms for the data subject and is allowed in specific cases authorised by a law **(…)**; or if not already authorised by such a law the processing is necessary to protect the vital interests of the data subject or of another person; **(…)**or the processing relates to data which is manifestly made public by the data subject (…).Appropriate safeguards for the rights and freedoms of the data subject may for example include the possibility to collect those data only in connection with other data on the individual concerned, to adequately secure the data collected, stricter rules on the access of staff of the competent (…) authority to the data, or the prohibition of transmission of those data. Processing of such data should also be allowed by law when the data subject has explicitly agreed in cases where the processing of data is particularly intrusive for the persons**.** However, the agreement of the data subject should not provide in itself a legal ground for processing such sensitive personal data by competent **(…)** authorities.

(27) The data subject should have the right not to be subject to a decision evaluating personal aspects relating to him or her which is based solely on automated processing, which produces legal effects concerning him or her or significantly affects him or her. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention, in particular to express his or her point of view, to get an explanation of the decision reached after such assessment and the right to contest the decision.

(28) In order to exercise their rights, any information to the data subject should be easily accessible, including on the website of the controller and easy to understand, requiring the use of clear and plain language.

(29) Modalities should be provided for facilitating the data subject's exercise of their rights under the provisions adopted pursuant to this Directive, including mechanisms to request, free of charge, (…) access to data, as well as rectification, erasure and restriction. The controller should be obliged to respond to requests of the data subject without undue delay **~~and give reasons where the controller does not intend to comply with the data subject's request~~**.

However, if requests are manifestly unfounded or excessive such as when the data subject unreasonably and repetitiously requests information or where the data subject abuses its right to receive information for example by providing false or misleading information when making the request, the controller could refuse to act on the request.

(30) (…) At least the following information should be made available to the data subject: (…) the identity of the controller, the existence of the processing operation, **~~and its~~** the purposes of the processing, (…) and (…) the right to lodge a complaint. (…) This could take place on the website of the competent authority.

(31) (…)

(32) A natural person should have the right of access to data which has been collected concerning him or her, and to exercise this right easily and at reasonable intervals in order to be aware of and verify the lawfulness of the processing. Every data subject should therefore have the right to know about and obtain communication in particular of the purposes for which the data are processed, (…) for what period, and which recipients receive the data, including in third countries. (…) **For that right to be complied with, it is sufficient that the applicant be in possession of a full summary of those data in an intelligible form, that is to say a form which allows that applicant to become aware of those data and to check that they are accurate and processed in compliance with this Directive, so that he may, where relevant, exercise the rights conferred on him by this Directive.**

(33) Member States should be allowed to adopt legislative measures delaying, restricting or omitting the information of data subjects or the access to their personal data to the extent that and as long as such (…) a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the individual concerned, to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, detection, investigation ~~and~~ **or** prosecution of criminal offences or for the execution of criminal penalties, to safeguard public security or national security, or to safeguard ~~the data subject or~~ the rights and freedoms of others.

(34) Any refusal or restriction of access should in principle be set out in writing to the data subject **and** includ**e**~~ing~~ the factual or legal reasons on which the decision is based.

(35) (…)

(36) A natural person should have the right to have inaccurate personal data concerning him or her rectified, in particular when pertaining to facts, and the right of erasure where the processing of such data is not in compliance with the provisions laid down in this Directive. However, the right to rectification should not affect, for example, the content of a witness testimony. A natural person ~~should~~ **may** also have the right to have **an item of** ~~the~~ personal data restricted where the accuracy is contested. Methods to restrict processing of personal data could include, inter alia, temporarily moving the selected data to another processing system or making the selected data unavailable. In automated filing systems the restriction of processing of personal data should in principle be ensured by technical means; the fact that the processing of personal data is restricted should be indicated in the system in such a way that it is clear that the processing of the personal data is restricted.

(36a)[23] **Where the controller denies a data subject his or her right of access, rectification, erasure or restriction of processing,** ~~**Where Member States have adopted legislative measures restricting wholly or partly the right to access,**~~ the data subject should have the right to request that the (…) national supervisory authority checks the lawfulness of the processing. The data subject should be informed of this right. When ~~**access is exercised by**~~ the supervisory authority **intervenes** on behalf of the data subject, the data subject should be informed by the supervisory authority at least that all necessary verifications **or reviews** by the supervisory authority have taken place. ~~**and of the result as regards to the lawfulness of the processing in question.**~~

(36aa) *Where the personal data are processed in the course of a criminal investigation and proceedings, (…) the exercise of the rights of information, access, rectification, erasure and restriction of processing may be carried out in accordance with national rules on judicial proceedings.*

(37) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate measures and be able to demonstrate (…) the compliance of processing activities with the ~~**rules**~~ **provisions** adopted pursuant to this Directive. These measures should take into account the nature, scope, context and purposes of the processing and the risk for the rights and freedoms of data subjects. Where proportionate in relation to the processing activities, the measures should include the implementation of appropriate data protection policies. These policies should specify the application of the data protection **provisions** adopted pursuant to this Directive.[24]

---

23 Moved from recital 35

24 DE wanted to delete the last part of recital 37 as well as the text in Article 18.1a. Cion said that policies meant guidelines binding for the controller.

(37a) **(…)** Risks for the rights and freedoms of data subjects, of varying likelihood and severity, may result from data processing which could lead to physical, material or moral damage, in particular where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy, unauthorized reversal of pseudonymisation, or any other significant economic or social disadvantage; or where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing and prediction of aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable individuals, in particular of children, are processed; where processing involves a large amount of personal data and affects a large number of data subjects.

(37b) The likelihood and severity of the risk should be determined in function of the nature, scope, context and purposes of the data processing. Risk should be evaluated on an objective assessment, by which it is established whether data processing operations involve a high risk. A high risk is a particular risk of prejudice to the rights and freedoms of **data subjects**.

(38) The protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organisational measures be taken to ensure that the requirements of the Directive are met. In order to be able to demonstrate compliance with the provisions adopted pursuant to this Directive, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default. Such measures could consist inter alia of **the use of** pseudonymis**ation~~ing personal data~~** as soon as possible. [25] **The use of pseudonymisation for the purposes of this Directive can serve as a tool in particular that could facilitate, in particular, the free flow of relevant data within the Area of Freedom, Security and Justice.**

[25] FR wanted to delete the second but last sentence of the paragraph.

(39) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Directive, including where a controller determines the purposes (…) and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(39a) The carrying out of processing by a processor should be governed by a legal act including a contract binding the processor to the controller and stipulating in particular that the processor ~~**shall**~~ **should** act only on instructions from the controller.[26]

(40) Processing activities including transfers by way of appropriate safeguards and in specific situations should be recorded by the controller ~~**or**~~ **and the** processor, in order to monitor compliance with this Directive. Each controller and processor should be obliged to co-operate with the supervisory authority and make these records, on request, available to it, so that it might serve for monitoring processing operations.

(40a) Logs should be kept at least for operations in automated processing systems such as collection, alteration, consultation, disclosure, combination or erasure. The logs should be used for verification of the lawfulness of the data processing, self-monitoring and for ensuring data integrity and data security. ~~**Within this context and if relevant,**~~ **This does not preclude the use of the logs** ~~**the logs could be used**~~ in accordance with Member State law for operational matters in the course of criminal investigations and proceedings.

(41) In order to ensure effective protection of the rights and freedoms of data subjects (…) the controller or processor should consult with the supervisory authority in certain cases prior to intended processing.

---

26 FR wanted to delete the last sentence of the paragraph.

(42) A personal data breach may, if not addressed in an adequate and timely manner, result in physical, material or moral damage (…) to individuals**,** such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, damage to the reputation, unauthorized reversal of pseudonymisation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage to the individual concerned. Therefore, as soon as the controller becomes aware that (…) a personal data breach has occurred which may result in (...) physical, material or moral damage, the controller should notify the breach to the supervisory authority without undue delay. The individuals whose **~~personal data~~ rights and freedoms** (…) could be severely affected by the breach should be informed without undue delay in order to allow them to take the necessary precautions (…).

(43) The communication of a personal data breach to the data subject should not be required if the controller has implemented appropriate technological protection measures, and that those measures were applied to the data affected by the personal data breach. Such technological protection measures should include those that render the data unintelligible to any person who is not authorised to access it**, in particular by encrypting personal data.** Likewise, the communication to the data subject is not required if the controller has taken subsequent measures which ensure that the high risk for the rights and freedoms of affected data subjects is no longer likely to (…) materialise.

(44) (…) A person with expert knowledge of data protection law and practices may assist the controller or processor to monitor internal compliance with the provisions adopted pursuant to this Directive. This person may inform and advise the controller or the processor and the employees who are processing personal data of their relevant data protection obligations. A data protection officer may be appointed jointly by several **~~public~~ competent** authorities or bodies, taking into account of their organisational structure and size (…). Such data protection officers must be in a position to perform their duties and tasks in an independent (…) manner.[27]

[27] CH suggested deleting the last sentence of recital 44.

(45) Member States should ensure that a transfer to a third country or to an international organisation only takes place if it is necessary for the prevention, investigation, detection or prosecution of criminal offences *or the execution of criminal penalties* **or ~~as well as by the police or other law enforcement authorities for the purposes of~~ (…)** the safeguarding against and the prevention of threats to public security, and the controller in the third country or international organisation is an authority competent within the meaning of this Directive. A transfer may take place in cases where the Commission has decided that the third country or international organisation in question ensures an adequate level or protection, or when appropriate safeguards have been adduced or when derogations for specific situations apply.

(45a)[28] *Where personal data are transferred from a Member State to third countries or international (…) organisations, such transfer should, in principle, take place only after the Member State from which the data were obtained has given its authorisation to the transfer. The interests of efficient law enforcement cooperation require that where the nature of a threat to the public security of a Member State or a third country or to the essential interests of a Members State is so immediate as to render it impossible to obtain prior authorisation in good time, the competent* ***~~public~~*** *authority should be able to transfer the relevant personal data to the third country or international organisation concerned without such prior authorisation.* [29] **Member States should provide that any specific conditions concerning the transfer should be communicated to third countries and/or ~~and~~ international organisations.**

(46) Where the Commission has not adopted a decision in accordance with Article 41 of Regulation (EU) XXX, it may decide with effect for the entire Union that certain third countries, or a territory or one or more specified sectors within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any specific authorisation.

---

28 Moved from recital 49a

29 DE wanted that it was set out that "prior authorisation" could mean already given authorisation within the EU or generally. CH suggested adding the following sentence in the end of recital 49a: "Furthermore, a transfer of personal data should be lawful if the data subject has given his or her consent to the transfer of his or her personal data for one or more specific purposes."

(47) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should take into account how a given third country respects the rule of law, access to justice, as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law.

(48) The Commission should equally be able to recognise that a third country, or a territory or a specified sector within a third country, or an international organisation, no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited unless the requirements of Articles 35-36 are fulfilled. Provision should be made for procedures for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

(49) Transfers not based on such an adequacy decision should only be allowed where appropriate safeguards have been adduced in a legally binding **~~and enforceable~~** instrument, which ensure the protection of the personal data or where the controller (…) has assessed all the circumstances surrounding the data transfer (…) and, based on this assessment, considers that appropriate safeguards with respect to the protection of personal data exist. Such legally binding instruments could for example be legally binding bilateral agreements which have been concluded by the Member States and implemented in their legal order and may be enforced by their data subjects, **ensuring ~~Those safeguards should ensure~~** compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress**.** The controller may take into account cooperation agreements concluded between Europol or Eurojust and third countries which allow for the exchange of personal data when carrying out the assessment of all the circumstances surrounding the data transfer. **The controller may also take into account that the transfer of personal data will be subject to confidentiality obligations and the principle of specificity, ensuring that the data will not be processed for other purposes than for the purposes of the transfer. In addition the controller may take into account that the personal data will not be used to request, hand down or execute the death penalty or any form of cruel and inhumane treatment.**

(49a) **(…)**

(49aa) Where no adequacy decision or appropriate safeguards exist, a transfer or a category of transfers could only take place in specific situation**s** if necessary in order to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides, or where it is necessary for the prevention of an immediate and serious threat to the public security of a Member State or a third country, or necessary in an individual case for the purposes of prevention, investigation, detection or prosecution of criminal offences *or the execution of criminal penalties* (…) or the safeguarding against and the prevention of public security, or necessary in an individual case**s** for the establishment, exercise or defence of legal claims.

(49b) Competent authorities of Member States are applying existing bilateral or multilateral international agreements concluded with third countries in the field of judicial co-operation in criminal matters and police co-operation, **for the exchange of ~~in order to obtain from private parties established in third countries the~~** relevant information to allow them to perform their legally assigned tasks. In principle, this takes place through or at least with the cooperation of the competent authorities of the concerned third countries. However, in **(…)** specific individual cases, it may occur that the procedures provided for by the international agreements applicable do not allow to **exchange ~~obtain~~** the relevant information in a timely manner, so that competent authorities of Member States have to transfer personal data directly to **recipients and public authorities ~~private parties~~** established in third countries. **This may be the case ~~for example in urgent cases~~** when criminal offences have been committed by means of electronic communication technology like social networks, or where data generated by communication technology are relevant as evidence of the perpetration of a criminal offence. Even if this **exchange ~~direct communication~~** between competent authorities and **recipients and public authorities established in third countries ~~private bodies should remain exceptional and strictly necessary and~~** should only take place in **(…) individual and specific** cases, this Directive should provide for **~~specific~~** conditions to regulate **such ~~these specific~~** cases. These provisions should not be considered as derogations to any existing bilateral or multilateral international agreement in the field of judicial co-operation in criminal matters and police co-operation. **~~to the extent that such agreements are compatible with Union law.~~ (…)** These **~~specific~~** rules should apply in addition to the other rules of the Directive, in particular **~~to the provisions~~ those** on the lawfulness of processing and **~~the other provisions~~** of Chapter V.

(50) (…)

(51) The establishment of supervisory authorities in Member States, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of their personal data. The supervisory authorities should monitor the application of the provisions adopted pursuant to this Directive and contribute to ~~its~~ **their** consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data. For that purpose, the supervisory authorities should co-operate with each other and the Commission.

(52) Member States may entrust a supervisory authority already established (…) under Regulation (EU)…./ XXX with the responsibility for the tasks to be performed by the national supervisory authorities to be established under this Directive.

(53) Member States should be allowed to establish more than one supervisory authority to reflect their constitutional, organisational and administrative structure. Each supervisory authority should be provided with (…) 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.

(53a)[30] ~~**The independence of s**~~Supervisory authorities should ~~**not mean that the supervisory authorities cannot**~~ be subject~~**ed**~~ to **independent** control or monitoring mechanism**s** regarding their financial expenditure, **provided that this financial control does not affect their independence**. ~~**Neither does it imply that supervisory authorities cannot be subjected to judicial review.**~~

(54) 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 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**(…).

[30] Moved from recital 54a

(55) While this Directive applies also to the activities of national 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 judges in the performance of their judicial tasks[31]. **~~However,~~ T**his exemption should be limited to (…) judicial activities in court cases and not apply to other activities where judges might be involved in accordance with national law. **~~However, the~~ Member States may also provide that the competence of the supervisory authority may not cover the processing of personal data of other independent judicial authorities when acting in their judicial capacity. In any event, the compliance with the rules of this Directive by the courts and other independent judicial authorities should always be subject to independent supervision in accordance with Article 8 (3) of the Charter of Fundamental Rights of the EU.**

(56) *Each supervisory authority should deal with complaints lodged by any data subject and should investigate the matter. 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.*

31 CH suggested replacing "in order to safeguard …judicial tasks" with the following: "so that it doesn't interfere with national rules on judicial proceedings."

(57) In order to ensure consistent monitoring and enforcement of this Directive throughout the Union, the supervisory authorities should have *in each Member State* the same tasks and effective powers, including **investigative ~~powers of investigation~~**, **(…)** corrective **~~powers,~~ (…) and advisory powers. ~~and sanctions and authorisation and advisory powers~~** , **~~particularly in cases of complaints from individuals, and w~~W**ithout prejudice to the powers of prosecutorial authorities under national law, **supervisory authorities should also have the power** to bring infringements of this Directive to the attention of the judicial authorities and/or to engage in legal proceedings. Such powers should also include **the power 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, to notify the controller or the processor of an alleged infringement of the provisions adopted pursuant to this Directive, 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 law, to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Directive and to order the suspension of data flows to a recipient in a third country or to an international organisation. ~~the power to forbid the processing on which the authority is consulted.~~**

The powers of supervisory authorities should be exercised in conformity with appropriate procedural safeguards set out in Union law and Member State 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 Directive, 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. Investigat**ive~~ory~~** powers as regards access to premises should be exercised in accordance with specific requirements in national 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~~ a** legally binding decision **~~implies that it may~~ should be subject ~~give rise~~** to judicial review in the Member State of the supervisory authority that adopted the decision.

(58) The supervisory authorities should assist one another in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of the provisions adopted pursuant to this Directive.

(59) The European Data Protection Board established by Regulation (EU)…./XXX should contribute to the consistent application of this Directive throughout the Union, including advising the Commission and promoting the co-operation of the supervisory authorities throughout the Union.

(60) Every data subject should (...) have the right to lodge a complaint with a supervisory authority (…) ~~in particular~~ **namely** 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 [32] if the data subject considers that his or her rights under provisions adopted pursuant to this Directive 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.

---

32 CZ wanted to insert the following text after *remedy* "under conditions stipulated by the law of the Member State" to make it possible for the MS to stipulate in national law that the data subject must first exhaust all available administrative remedies before addressing the courts against inaction.

(61) Each natural or legal person should have[33] the right to 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. 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.[34] 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.

(62) *Where a data subject considers that his or her rights under this Directive 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 to exercise the right to a judicial remedy.* ***~~Member States may provide that such a body, organisation or association should have the right to lodge, independently of a data subject's mandate, in such Member State a complaint and/or have the right to an effective judicial remedy where it has reasons to consider that the rights of a data subject have been infringed as a result of the processing of personal data which is not in compliance with the provisions adopted pursuant to this Directive. This body, organisation or association may not be allowed to claim compensation on a data subject's behalf.~~***

(63) (…)

---

33 CZ wanted to add the following text after *have*: "under conditions stipulated by the law of the Member State and to add the following sentence after the first sentence: "Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established. "The addition of the second sentence was to avoid forum shopping.

34 SE wanted to delete the last part of the recital, after supervisory authority.

(64) Any damage which a person may suffer as a result of **(...)** processing that is not in compliance with the provisions adopted pursuant to this Directive should be compensated by the controller or processor **(…).** The concept of damage should be broadly interpreted in the light of the case law of the Court of Justice of the European Union in a manner which fully reflects the objectives of this Directive. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law.

When reference is made to a processing that is not in compliance with the provisions adopted pursuant to this Directive it also covers processing that is not in compliance with **(...)** implementing acts adopted in accordance with this Directive.

Data subjects should receive full and effective compensation for the damage they have suffered. ~~**Where controllers or processors are involved in the same processing each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with national law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor who has (…) paid full compensation, may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.**~~

(65) Penalties should be imposed on any natural or legal person[35], whether governed by private or public law, that fails to comply with this Directive. Member States should ensure that the penalties are effective, proportionate and dissuasive and must take all measures to implement the penalties.[36]

(66) (…)

(67) In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission for: (…) the adequate level of protection afforded by a third country or a territory or a specified sector within that third country or an international organisation; **the format and procedures for** *mutual assistance* **and** the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board. **(…)**Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers[37].

(68) The examination procedure should be used for the adoption of implementing acts on (…) the adequate level of protection afforded by a third country or a territory or a specified sector within that third country or an international organisation; **the format and procedures for** mutual assistance **and** the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, **(…)** given that those acts are of general scope.

(69) The Commission should adopt immediately applicable implementing acts where, in duly justified cases relating to a third country or a territory or a specified sector within that third country or an international organisation which no longer ensure an adequate level of protection, imperative grounds of urgency so require.

---

35 SE, supported by FI, wanted to delete the reference to *legal person* because penalties cannot be imposed on such persons. SE, supported by DK, suggested alternatively to refer to *sanctions* in the beginning of the sentence to remedy this problem. Cion said that this was a standard recital and that Article 55 was a standard Article.

36 FI scrutiny reservation.

37 OJ L 55, 28.2.2011, p. 13.

(70) Since the objectives of this Directive, namely to protect the fundamental rights and freedoms of data subjects and in particular their right to the protection of personal data and to ensure the free exchange of personal data by competent **(…)** authorities within the Union, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

(71) Framework Decision 2008/977/JHA should be repealed by this Directive. Processing already under way on the date of the entry into force of this Directive should be brought into conformity with this Directive within the period of two years after which this Directive enters into force. However, where such processing is in compliance with the Union law applicable prior to the entry into force of this Directive, the requirements of this Directive concerning the prior consultation of the supervisory authority should not apply to the processing operations already under way prior to the entry into force of this Directive, given that these requirements, by their very nature, are to be met prior to the processing.

(72) Specific provisions of acts of the Union adopted in the field of judicial co-operation in criminal matters and police co-operation **(…)** which were adopted prior to the date of the adoption of this Directive, regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, should remain unaffected, **such as, for example, the specific provisions concerning the protection of personal data applied pursuant to Council Decision 2008/615/JHA[38], or Article 23 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000/C 197/01)[39].** The Commission should evaluate the situation with regard to the relationship between this Directive and the acts adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, in order to assess the need for alignment of these specific provisions with this Directive.

---

38 Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, p. 1.

39 Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197, 12.7.2000, p. 1.

(73) In order to ensure a comprehensive and coherent protection of personal data in the Union, international agreements concluded by Member States prior to the entry force of this Directive (…), and which are in compliance with the relevant Union law *applicable* prior to the entry into force of this Directive, should remain **unaffected ~~in force until amended, replaced or revoked~~**. To the exten**t** that such agreements are not compatible with Union law, Member States are[40] required to take all appropriate steps to eliminate any incompatibilities[41] (…).

(74) This Directive is without prejudice to the rules on combating the sexual abuse and sexual exploitation of children and child pornography as laid down in Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011.[42]

(75) In accordance with Article 6a of the Protocol on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, the United Kingdom and Ireland are not bound by the rules laid down in this Directive which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the Treaty on the Functioning of the European Union where the United Kingdom and Ireland are not bound by the rules governing the forms of judicial co-operation in criminal matters or police co-operation which require compliance with the provisions laid down on the basis of Article 16 of the Treaty on the Functioning of the European Union.

(76) In accordance with Articles 2 and 2a of the Protocol on the position of Denmark, as annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not bound by the rules laid down in this Directive or subject to their application which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the Treaty on the Functioning of the European Union. Given that this Directive builds upon the Schengen acquis, under Title V of Part Three of the Treaty on the Functioning of the European Union, Denmark shall, in accordance with Article 4 of that Protocol, decide within six months after adoption of this Directive whether it will implement it in its national law.

---

40 CH, supported by CZ and SE, suggested adding ",as far as possible," or as regards CH to delete the last sentence.

41 FR and CZ wanted to delete the last sentence.

42 OJ L 335, 17.12.2011, p. 1. SE suggested to delete this text because many other texts could also be mentioned here.

(77) As regards Iceland and Norway, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis[43].

(78) As regards Switzerland, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis[44].

(79) As regards Liechtenstein, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis[45].

(80) This Directive respects the fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaty, notably the right to respect for private and family life, the right to the protection of personal data, the right to an effective remedy and to a fair trial. Limitations placed on these rights are in accordance with Article 52(1) of the Charter as they are necessary to meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

(81) In accordance with the Joint Political Declaration of Member States and the Commission on explanatory documents of 28 September 2011, Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a directive and the corresponding parts of national transposition instruments. With regard to this Directive, the legislator considers the transmission of such documents to be justified.

---

43 OJ L 176, 10.7.1999, p. 36.

44 OJ L 53, 27.2.2008, p. 52.

45 OJ L 160 of 18.6.2011, p. 19.

(82) This Directive should not preclude Member States from implementing the exercise of the rights of data subjects on information, access, rectification, erasure and restriction of their personal data processed in the course of criminal proceedings, and their possible restrictions thereto, in national rules on criminal procedure.

CHAPTER I
GENERAL PROVISIONS[46]

Article 1

Subject matter and objectives

1. This Directive lays down the rules relating to the protection of individuals with regard to the processing of personal data[47] by competent (…) authorities[48] for the purposes of the prevention**,** investigation, detection or prosecution of criminal offences *or the execution of criminal penalties* or[49] the safeguarding against **and** the prevention of threats to public security. [50]

[46] PL, FI, UK scrutiny reservation on Chapter I.

[47] SK thought that only automated forms of processing should be covered.

[48] FR suggested the insertion of "the Member States'" before "competent authorities".

[49] EL expressed concerns on the change from '*and'* to *'or'* because it meant that it broadened the scope too much by decoupling the purpose of 'prevention of threats to public security' from the purposes of 'prevention of criminal offences': it preferred to revert to *'and'*. LT asked if this wording of Article 1 of the Directive covered 'administrative offences'. Cion replied that it did on condition that it was linked to a potential criminal offence. RO preferred to refer to 'public order'.

[50] AT said that it had to be clear that any data processing activities for pure administrative purposes such as speed monitoring, food safety, assessment of individual grounds for asylum or registration of events and assemblies are covered by the Regulation irrespective of which authority, agency or body is carrying out such processing (DS 1384/15).

1a. This Directive shall not preclude Member States from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent (…) authorities.

2. In accordance with this Directive, Member States shall:

(a) protect the fundamental rights and freedoms of individuals and in particular their right to the protection of personal data; and

(b) ensure that the exchange of personal data by competent (…) authorities within the Union, where such exchange is required by Union or national law, is neither restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.[51] [52] [53] [54] [55]

---

51 SE suggested to insert the following text after *Union 'where such exchange is required by Union or national law'*.

52 SK suggested to reformulate this paragraph as follows: "not restrict nor prohibit the exchange of personal data by competent authorities within the Union if individuals data protection is safeguarded".

53 CH suggested to insert a recital to clarify that MS could foresee more restrictive provisions with regard to the purpose for which data could be used.

54 DE suggested to add "by restrictions or prohibitions stricter than those applicable at national level."

55 ES suggested to let current (b) become (c) and add the following text under new paragraph "b) ensure that the treatment of personal data by the competent authorities let them perform efficiently their legal duties as regards the detection, prevention, investigation or prosecution of criminal offences, [the maintenance of public order,] or the execution of criminal penalties".

Article *2*

Scope [56]

1. This Directive applies to the processing of personal data by competent (…) authorities for the purposes set out in Article 1(1).[57]

2. This Directive applies to the processing of personal data wholly or partly by automated means[58], and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.[59]

3. This Directive shall not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law (…);

(...)

(b) by the Union institutions, bodies, offices and agencies.

[60]

---

[56] EE scrutiny reservation.

[57] CZ, DK, RO, SE, SI, UK and HR were of the opinion that the regulating of national processing of personal data by competent authorities in the area of law enforcement and criminal justice was not in conformity of the principle of subsidiarity.

[58] HU suggested to delete the words "whether or not by automated means" or as a alternative to deletion to add: "irrespective of the means by which personal data are processed,"

[59] DE scrutiny reservation.

[60] FI suggested the insertion of the following paragraph "(4) This Directive does not apply to personal data contained in a judicial decision or to records processed in courts during criminal proceedings." to ensure that national rules on judicial proceedings were not affected. ES suggested to add a new paragraph (c) with the following wording: "c) concerning terrorism, organized crime and situations of serious disturbances to the democratic social order." ES scrutiny reservation on national security.

Article 3

Definitions[61]

For the purposes of this Directive:

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic[62], mental, economic, cultural or social identity of that person.

(2) (…)

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

(4) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future; [63]

(4a) '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.

---

61 DE scrutiny reservation. UK, supported by IE, thought that a definition of *consent* should be inserted in Article 3 as a possible legal ground for processing. In contrast IT did not approve the idea of a definition of consent. CH noted that in the draft for the modernised Convention 108 consent is legal basis for processing. Cion set out that consent was a legal ground in the 95 Directive and GDPR but thought that it should not be a legal basis for processing in the context of the Directive. Cion meant in the DE examples of blood sample or DNA testing consent was not the legal basis it was the law that required it; it related to consent to the measure. SI agreed with Cion that in law enforcement there was no such thing as a free consent.

62 FR reservation.

63 CZ reservation.

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

(6) 'controller' means the competent (…) authority, which alone or jointly with others determines the purposes (…) and means of the processing of personal data; where the purposes (…) and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;

(7) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller[64];

(8) 'recipient' means a natural[65] or legal person, public authority, agency or any other body **(…),** to which the personal data are disclosed[66], whether a third party or not; ~~**however, authorities which may receive data in the framework of a particular inquiry within the meaning of Article 1 (1) shall not be regarded as recipients;**~~

67

---

64 PL scrutiny reservation.

65 CZ, DE was opposed to the inclusion of natural persons in this definition, as only the authority which receives/processes personal data should be considered as recipient, not the individual working at those authorities.

66 HU suggested the following addition: "… body "*other than the data subject, the data controller or the data processor*" to which …" or alternatively to delete the following from the definition: "natural or legal person, public authority, agency or any other body" and replace with: "third party". As a consequence add a definition on "third party" as follows: " 'third party' means a natural of legal person, public authority, agency or nay other body other than the data subject, the data controller or the data processor".

67 DE asked to insert a definition of "consent of the data subject" with the following wording: *"(8a) 'consent of the data subject' means any indication of wishes in the form of a declaration or other unequivocal act made without coercion in a specific instance and in the knowledge of the facts by which the data subject indicates that he consents to the processing of his personal data';"* CH agreed on that need of a definition on *consent* but suggested the following wording: *'the data subject's consent" means any freely-given specific, informed and explicit indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him being processed';"* Support from NO, BE and SI to set out a consent as a legal basis for processing; for SI in exceptional specific cases. Support from ES, AT, HU and RO to include a definition of consent. HU suggested inserting a definition from the general approach on a draft Directive on the use of PNR data for the prevention. detection, investigation and prosecution of terrorist offences and serious crimes: " 'depersonalising through masking out of data' means rendering certain data elements of such data invisible to a user without deleting these data elements". Cion said that it could not see the context where consent would be necessary and queried if a consent could be considered given "freely" in a criminal situation.

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

(10) 'genetic data' means all personal data, (…) relating to the genetic characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the health of that individual, resulting in particular from an analysis of a biological sample from the individual in question**;**

(11) (...);

(12) 'data concerning health' means (…) data related to the physical or mental health of an individual, which reveal information about his or her health status;

(12a) 'profiling' means any form of automated processing of personal data consisting of using those data to (…) evaluate personal aspects relating to an **(…)** natural person, in particular to analyse and predict aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements;

(…)

68

68 DE considered it necessary to insert a definition of *criminal offence* with the following wording: (**12b**) *'criminal offence' covers all infringements of the rules of law which are punishable under national law, provided that the person concerned has the opportunity to have the case tried by a court having jurisdiction in particular in criminal matters.* Cion did not see the need for such a definition since it was a standard term. HU wanted it clarified if *petty* offences were covered.

(14) 'competent[69] (…) authority' means any (...) public authority competent in each Member State for the prevention, investigation, detection or prosecution of criminal offences *or the execution of criminal penalties* or the safeguarding against and the prevention of threats to public security [70] or any body/entity[71] entrusted by national law[72] to perform public duties or exercise public powers for the purposes set out in Article 1(1)(…).
[73]

(15) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 39.

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

[69] DE scrutiny reservation.

[70] PL remarked that courts were excluded from this definition. FI stressed that courts were not covered by this definition. CZ said that the Directive should be applied to ordinary courts. Cion said that courts and prosecutors should be covered by the Directive.

[71] Cion scrutiny reservation, linked to the authorities being covered by the definition.

[72] UK, supported by CZ, IE and SE, suggested to replace *by national law* with "in accordance with national law" to cover cases when such duties or powers were not set out in national legislation.

[73] BE reservation on private bodies maintaining public order (public security). FI, NL and PT scrutiny reservation. IE waiting reservation.

CHAPTER II[74]

PRINCIPLES

Article 4

Principles relating to personal data processing[75]

1. Member States shall provide that personal data must be:

(a) processed lawfully *and fairly*;[76]

(b) collected for specified, explicit and legitimate purposes **~~referred to~~ set out** in Article 1 (1) **~~and not further (…)processed in a way (…) incompatible with those purposes~~**;

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

(d) accurate and, where necessary[77], kept up to date; (…)[78]

(e) kept in a form which permits identification of data subjects[79] for no longer than is necessary for the purposes for which the personal data are processed;[80]

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

(…)

1a. **(...)**

[81]

---

74 FI, PL, SI, UK scrutiny reservation on Chapter II.

75 PL scrutiny reservation.

76 HU suggested to add "and to the extent and for the duration necessary to achieve its purpose" in the end of paragraph (a) or add a new paragraph (bb) "processed only to the extent and for the duration necessary to achieve its purpose.". EE and SE scrutiny reservation on the reinserting of *fairly.*

77 AT and EL want the deletion.

78 CH, supported by NO, RO, suggested the following wording for (d): "(d) accurate and, where possible and necessary**,** completed or kept up to date; (…)."

79 SE wanted to delete the words "in a form which permits identification of the data subject" since data that does not allow identification of persons is not personal data.

80 HU suggested to add that the personal data must be "processed lawfully and to the extent and for the duration necessary to achieve its purpose".

81 AT pleaded for the re-introduction of provisions along the lines of Article 4.3 and 4 of DPFD.

2. **(...)** Processing by the same or another controller for other purposes ~~**referred to**~~ **set out** in Article 1 (1) than the one for which the data are collected **(…)** shall[82] be permitted in so far as:

(…)

(b) the controller is authorised to process such personal data for such purpose in accordance with the applicable legal provisions[83]; and

(c) processing is necessary and proportionate to that other purpose.

3. Processing by the same or another controller **may include** ~~**for the purposes referred to in Article 1 (1) may include processing (…) *for***~~ archiving**, (…)** *scientific, statistical or historical* **processing for the purposes set out in Article 1 (1)** ~~***purposes***~~, subject to appropriate safeguards for the rights and freedoms of data subjects.

84

4. The controller shall be responsible for compliance with paragraphs 1, 2 and 3.

Article 5

Distinction between different categories of data subjects[85]

(…)

---

82 AT, supported by IE, suggested to replace *shall* with *may*.

83 AT suggested to replace *legal provisions* with *EU or Member States' law*.

84 HU suggested to add a new paragraph to Article 4 as follows: "2. The basis of the processing referred to in points (a) and (b) of paragraph 1 must be provided for in (a) Union law, or (b) the law of the State to which the controller is subject.

85 Cion reservation against deletion. DK and SE welcomed the deletion and requested that the corresponding recitals to be removed. Contrary to this AT that wished to maintain both recitals 23 and 24.

Article 6

Verification of quality of data that are transmitted or made available[86]

1. Member States shall provide that the competent authorities shall take all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, each competent authority shall as far as practicable verify quality of personal data before they are transmitted or made available. As far as possible, in all transmissions of **personal** data, ~~**available**~~ **necessary** information shall be added which enables the receiving competent authority to assess the degree of accuracy, completeness, up-to-datedness and reliability **of personal data**.[87]

2. If it emerges that incorrect personal data have been transmitted or the data have been unlawfully transmitted, the recipient must be notified without delay. In such case the personal data must be rectified, erased or restricted in accordance with Article 15.[88]

Article 7[89]

Lawfulness of processing

Member States shall provide that the processing of personal data is lawful only if and to the extent that processing is necessary.

(a) **(...)** for the performance of a task carried out by a competent (…) authority for the purposes set out in Article 1(1), based on Union law or Member State law (…)

(b) **(...)**[90]

(c) (...)

[91]

---

86 CZ suggested to delete the Article.

87 FR wants deletion of para 1.

88 UK meant that it was necessary to have a reference to Article 13 as well so as not to reveal to the data subject that data has been collected and their content.

89 DE and SI scrutiny reservation.

90 For SE it was for the sake of the principle of public access to official records that point (b) had to be reinserted: this was a red line for SE.

91 ES suggested the insertion of the following paragraph: "d) to protect the freedoms and rights of the data subject or of another person and, in particular, to protect their interests as regards exercising legal claims,". ES considered that data processed by law enforcement officials are collected to provide authorities and citizens with information and data on incidents in general.

(d) (...)

92

93

Article 7a

Specific processing conditions [94]

~~1. Member States shall provide that personal data received from or made available by a competent authority may be transmitted to another recipient only if no rights or legitimate interests of the data subject are affected and where the transmission of the personal data is necessary for:~~

92 ES suggested to insert the following paragraph: "(e) To protect other fundamental rights of the data subject or another person that deserve a higher degree of protection."

93 DE suggested the insertion of new paragraph 2 as follows: "Member State law may provide that in duly justified cases data processing by competent authorities can be done on the basis of the freely given consent of the data subject. Those provisions have to provide for appropriate safeguards for the rights and freedoms of the data subjects, including provisions assuring that the refusal of the data subject to give his or her consent shall not produce adverse legal effects upon him or her." AT, BE, CZ, ES, HU, IE and CH supported DE on the need for consent as a legal basis whereas FI, FR, IT, NL and PT cautioned against a general rule allowing consent as a legal basis and PT found that consent could only be used in special circumstances. IE found it useful with consent in order to remove suspicions, CZ mentioned stalking and FI reporting of crime in general. AT meant however that the current drafting did not exclude consent as a legal basis; IE doubted that national law could allow for it. FR meant that recital 25 was enough whereas DE meant that recital 25 was contradicory on this issue. For DE it was enough that the MS could set out consent as a legal basis; DE scrutiny reservation. Cion opposed consent as a legal basis.

94 CH, EE, NL, SK, PL, PT and SK scrutiny reservation. FR and SE reservation.

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

~~**(b) the prevention of serious harm to the rights of individuals.**~~

1a. Where competent authorities are entrusted by Member State law with the performance of tasks other than **for** the purposes ~~**referred to**~~ **set out** in Article 1 (1), Regulation XXX shall apply for the processing for such purposes, including for archiving purposes in the public interest or for scientific, statistical or historical purposes, unless the processing is carried out in an activity which falls outside the scope of Union law. [95]

1.b Member States shall provide that where Union law or the national law applicable to the transmitting competent (…) authority provides specific conditions (...) to the processing of personal data,[96] the transmitting competent authority shall inform the recipient to whom the data are transmitted about such conditions and the requirement to respect them.

---

[95] DE suggested a new recital for this paragraph of Article 2(1) as follows: "In cases where competent authorities are entrusted by Member State law with the performance of tasks other than those referred to in Art. 1 par. 1, Regulation XXX shall be applicable to data processing which is done purely for those purposes outside of Art. 1 par. 1. This provides for legal certainty both on the part of the data subjects and on the part of the acting competent authority. Therefore data processing activities of competent authorities involving tasks encompassed by Art. 1 par. 1 are governed by this Directive. This includes cases where filing systems are designed to meet operational needs falling within the scope of this Directive. However, it might be possible that filing systems which are designed and used for purposes laid down in Art. 1 par. 1 are also used in specific cases for purposes outside the scope of Art. 1 par. 1. In those cases general provisions concerning the establishment and handling of those filing systems shall be in line with this Directive whereas Regulation XXX shall not apply."
DE meant that this reasoning was meant to help achieving the goal of bringing as many aspects of data processing done by competent authorities under the umbrella of this Directive. Furthermore this understanding helps to avoid data maximization by creating mirror databases which include the same data being processed for purposes inside and outside the scope of this Directive

[96] In order to create an uniformity of handling codes at EU level and for practical reasons, BE asked to insert “these conditions are set out in accordance with the Europol handling codes. The transmitting ...” BE suggested that the same adaptations be set out in recital 25a.

2. Member States shall provide that the transmitting competent (…) authority does not apply conditions pursuant to paragraph 1b to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters IV and V of Title V of the Treaty on the Functioning of the European Union other than those applicable to similar **~~national data~~** transmissions **of data** within the Member State of the transmitting competent authority.
97

2a. (...)

97 BE, supported by AT and FI, suggested to insert a paragraph 3 which came from Article 16.2 of DPFD with the following text: "3. When personal data have been transmitted or made available between Member States, each Member State may, in accordance with the provisions of its national law, ask that the other Member State does not inform the data subject. In such case the latter Member State shall not inform the data subject without the prior consent of the other Member State."

Article 8[98]

Processing of special categories of personal data

(…)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 of data concerning health or sex life[99] shall only be allowed when strictly[100] necessary and subject to appropriate safeguards for the rights and freedoms of the data subject and only if:

(a**)** (…)**(…)**authorised by Union law or Member State law **(…)**; or

(…)[101];

(b) **(…)**

(b) **(…)**to protect the vital interests[102] of the data subject or of another person.; or

(…)

(c) the processing relates to data which are manifestly made public by the data subject.

103

---

98 PL and SI scrutiny reservation on Article 8.

99 RO wanted to add "biometric data" to the category with a special character. .

100 SE reservation on *strictly* because it wanted to verify the consequences of this qualifier. FR , supported by BE and PT, said that they preferred the text inspired by Article 27(4) in the Eurojust Regulation "…may be processed only when such data are strictly necessary and if they supplement other personal data already processed. Such processing shall be authorized by Union law or Member State law."

101 SI scrutiny reservation.

102 ES wanted to replace *vital* with *essential.*

103 DE, supported by CZ, suggested to insert a paragraph (d) with the following wording: "(d) the data subject has consented to the processing". ES, supported by CH, DK, HU, IE, CZ and HR suggested to insert a paragraph with the following wording: "(d) the data subject has given his explicit consent".

Article 9

(…) ***Automated individual decision making (…)***[104]

~~1.~~ Member States shall provide that a decision based solely[105] on automated processing**, ~~on~~** including, profiling**,** which produces an adverse legal effect for the data subject or significantly affects him or her (…) shall be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller**. ~~to express his or her point of view and to contest the decision~~** (…).

1a. (...)

[104] Scrutiny reservation FI, DE, ES, IT and SI.

[105] FR asked for the deletion of the word "solely".

CHAPTER III

RIGHTS OF THE DATA SUBJECT

Article 10

Communication and modalities for exercising the rights of the data subject

1. (…)

2. Member States shall provide that the controller (...) takes (...) all reasonable steps to provide any information referred to in Article 10a **(...)** and any communication under Articles 12 and 15 and 29 relating to the processing of personal data to the data subject in an intelligible and easily accessible form, using clear and plain language. The information shall be provided by any appropriate means, including **(...)** ~~**where appropriate,**~~ electronically **(...)** As a **general** rule the controller shall provide the information in the same form as the request **(...) .**

3. Member States shall provide that the controller takes all reasonable steps **(...)** to facilitate the exercise of data subject rights under Articles 12 and 15 (…).[106]

4. **(...)**

5. Member States shall provide that the information provided under Article 10a **(...)** and any communication under Articles 12, 15 and 29 shall be provided (…) free of charge[107]. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character (…), the controller may refuse to act on the request. In that case, the controller shall[108] bear the burden of demonstrating the manifestly unfounded or excessive character of the request (…)[109].

---

[106] DE wanted to delete paragraph 3,

[107] SE informed that data subjects had to pay a fee if they asked to have a lot of information but received information once a year free of charge. DE and NL scrutiny reservation. DE believed that the access rights of data subjects should not be undermined in fact by unreasonably high fees. NL asked whether it was reasonable to provide information *free of charge.* SE preferred the previous version of paragraph 5. DE noticed that the wording was different from the one in the DPFD. IE, UK supported to replace "free of charge" with "without an excessive charge".

[108] DE, BE suggested to add "state the reasons for the refusal" and delete the end of the sentence starting with "bear the burden…"

[109] DE, BG worried about the costs involved and referred to Article 17 in the DPFD where the wording is "without excessive expense". CZ, NL also preferred the text in the DPFD. CZ suggested to revert to simple principles, cf. Article 17 in DPFD, *at reasonable intervals.*

5a. Where the controller has reasonable doubts concerning the identity of the individual making the request referred to in Articles **10a (2),** 12 and 15, the controller may request the provision of additional information necessary to confirm the identity of the data subject.[110]

Article 10a[111]

Information to the data subject

1. Member States shall make available to the data subject at least the following information:
   (a) *the identity and the contact details of the controller*; the controller shall also include the contact details of the data protection officer *if any*;
   (b) *the purposes of the processing for which the personal data are intended*;
   (c) ~~**(…)**~~[112]
   (d) ~~(…)~~[113]
   (e) *the right to lodge a complaint* ***with*** ~~***to***~~ *a supervisory authority* (…).

2. Member States shall provide **by law** ~~**further specifications on the necessary**~~ information **in addition to paragraph 1**, **which is necessary** to be **given** to the data subject, in particular ~~**data concerning children and**~~ **where the data are** collected without the knowledge of the individual.

3. Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to paragraph 2 (…)*the extent that, and as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the individual concerned:*

(a)to avoid obstructing official or legal inquiries, investigations or procedures;

(b)to avoid prejudicing the prevention, detection, investigation or *prosecution of criminal offences or the execution of criminal penalties;*

(c)to safeguard *public security;*

---

110 EE found that paragraph 5a needed to be strengthened. SE found it important that the data subject could identify him/herself in an appropriate manner.

111 Cion scrutiny reservation on the introduction of Article 10a and the deletion of Article 11, 11a and 11b.

112 FI, NL wanted to reinsert paragraph (c).

113 NL asked to reinsert (d).

*(d)*_to_ safeguard _national security;_

*(e)*_to_ safeguard _the rights and freedoms of others._

114

115

---

114 DE suggested to insert an additional paragraph 1a containing general grounds for limiting the rights of information as follows: "1a. Member States may provide that the provision of information may be dispensed with temporarily, wholly or partly**.**
(a) if the data subject is already in possession of the information or voluntarily waives the right to the information;
(b) if the personal data are not collected from the data subject, the processing is explicitly subject to statutory regulations and the controller makes a general representation of the information referred to in paragraph 1 generally available in writing and electronically; this exception shall not apply to the collection of data in secret from the data subject;
(c) if further personal data would first have to be collected in order to provide the information;2
(d) if the effort involved in weighing the interests of the data subject in receiving the information and that required in providing the information would be disproportionate;3
(e) if this is obviously not appropriate due to special circumstances or would significantly endanger or interfere with the performance of law enforcement tasks."
IE suggested adding two new exemptions: "to protect the well-being and safety of others, in particular children. The purpose of this exemption is to ensure that the police can refuse to provide information in relation to recipients/categories of recipients of personal data where they consider it necessary to provide information to health professionals/authorities or social workers in child welfare cases; and where the provision of such information proves impossible or would involve a disproportionate effort (based on Article 14a.4 (b) of the Regulation).

115 CH, AT suggested to complete Article 11b with the same wording as in Article16 (2) DPFD: "3. When personal data have been transmitted or made available between Member States, each Member State may, in accordance with the provisions of its national law referred to in paragraph 1, ask that the other Member State does not inform the data subject. In such case the latter Member State shall not inform the data subject without the prior consent of the other Member State."

Article 11

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

(...)

Article 11a

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

(...)

Article 11b

Limitations to the rights of information

(...)

Article 12

Right of access for the data subject [116]

1. Subject to Article 13, Member States shall provide for the right of the data subject to obtain from the controller at reasonable intervals and free of charge confirmation as to whether or not personal data concerning him or her are being processed and where such personal data are being processed to obtain access to such data and the following information: **[117]**

(a) the purposes of the processing;**[118]**

(b) (…)**[119]**

(c) the recipients **~~or categories of recipients~~** to whom the personal data have been **(...)** disclosed, in particular the recipients in third countries or international organisations;

(d) (…) the envisaged period for which the personal data will be stored or the rules applicable to calculating this period;

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

(f) the right to lodge a complaint **~~to~~ with** a supervisory authority (…);

---

116 DE, ES, SI scrutiny reservation. EL wanted to limit the scope of Article 12. UK wanted to see clarifications as to whether judges' notes would be covered by the right of access. In reply to UK, the Cion said that judges' notes could be covered by Article17. SE thought DK found that Article 12, entailed a considerable burden on controllers. DE said that the scope was considerably different to Article 17 in DPFD and asked the reasons for this extension. HR meant that the right of access should be limited to the right of notification of whether personal data of a specific person was processed by the authority and for what purpose. HR also said that the information should be provided at the request of the person concerned. DE, supported by PT, SK and UK, considered that the real issue was the scope of access, whether it was to electronic files or to paper files. Cion replied that according to Article 2.2 paper files were covered if they formed part of a filing system and that paper files constituted a filing system, see also the definition in Article 3.5. According to Cion the Charter did not make a difference between paper and processing by automated means. DE meant that the scope of the obligation would be considerable if paper files were included in the scope; the number of pages to go through.

117 ES thought that the independence of the judiciary was at stake. Support from AT, DK and UK. FI wanted to add that the right to obtain information depended on a request from the data subject made within a certain timeframe, like in DPFD. DK noticed that the right of access had been extended compared to DPFD and that the proposal increased the burden on the police, also financially. UK considered that Article 17.1 in DPFD was more acceptable.

118 CZ wanted to delete paragraph (a).

119 FI meant that paragraph (b) should be reinserted.

(g) **communication of the personal data undergoing processing and of any available information as to their source;**

~~**(h) the appropriate safeguards pursuant to Article 35 where personal data are transferred to a third country or to an international organisation.**~~

1a. **(...)**

~~**2. (...). Subject to Article 13, Member States shall provide for the right of a data subject to obtain from the controller, on request and without an excessive charge, a copy of the personal data undergoing processing. The right to obtain a copy(...) shall not apply where such copy cannot be provided without disclosing personal data of other data subjects or confidential data (...)**~~

2a. **(...)**

Article 13

Limitations to the right of access[120]

1. Member States may adopt legislative measures[121] restricting, wholly or partly, the data subject's right of access to the extent that such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the individual concerned:[122]

(a) to avoid obstructing official or legal inquiries, investigations or procedures;

(b) to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) to safeguard public security;

(d) to safeguard national security; [123]

(e) to safeguard the rights and freedoms of others. [124]

2. **(...)**

---

[120] DE, BE reservation in substance. BE explained that in BE limitations are not on a case by case basis but are set out as total legal exceptions. FR wished to introduce the possibility of an indirect access and noted that DPFD did not forbid indirect access. DK mentioned that Article 52 in the Charter sets out the limitations and deemed it important that the limitations did not become the rule. ES and HU argued that Article 13 did not solve its problem concerning the independency of the judiciary that ES had mentioned in relation to Article 12. SE wanted criminal intelligence to be listed in paragraph 1 allowing to restrict the data subject's access. UK joined SE and required more flexibility allowing for tailoring of the national systems. For UK Article 13 should only contain minimum standards. CZ was of the opinion that the scope of Article 13 depended on the particular situation in a particular state. NL considered that it should be possible to deny access on behalf of the MS that provided the information. DE thought that other exceptions could be added to the list. UK was broadly in agreement with the Article. Cion said that restrictions should be allowed only when it was really necessary and that the principle was direct access.

[121] HR meant that it should be set out in law and not in legislative measures.

[122] CZ asked to add another subparagraph to paragraph 1 relating to children involved in household violence.

[123] FI asked that the changes to the draft Regulation on restrictions (Article 21) be mirrored here.

[124] FI suggested reverting to the text in Article 17.2(e) in the DPFD. CZ wanted to add "and of the data subject" in the end of the paragraph to cover cases of domestic violence for example.

3. In cases referred to in paragraph 1 **(...)**, Member States shall provide that the controller informs the data subject in writing **~~(...)~~** of any refusal or restriction of access, **~~of~~ and** the reasons for the refusal or the restriction. **~~and of the possibilities of lodging a complaint to the supervisory authority or seeking a judicial remedy.~~** This shall not apply (…) where the provision of such information would undermine a purpose under paragraph 1. [125] **Member States shall provide that the controller informs the data subject of the possibilities of lodging a complaint ~~to~~ with ~~the~~ a supervisory authority or seeking a judicial remedy.**

4. Member States shall ensure that the controller documents **~~the grounds for omitting the communication of~~** the factual or legal reasons on which the decision is based. [126]

Article 14

Additional modalities for exercising the right of access

(…)

[125] DE, CH and CZ saw problems with this paragraph because the data subject can draw conclusions on the basis of a motivated refusal. UK meant that it is implicit in paragraph 3 that the reply is negative. In the UK the reply can be "neither confirm nor deny" since a negative reply also contains information. Cion stressed that this paragraph did not interfere with the MS national criminal procedures. AT, CH, IT suggested a new drafting for paragraph 3 as follows: "3. In cases referred to in paragraphs 1 and 2, or when, in fact, no data on the person requesting the information is processed, Member States shall provide a neutral reply, instead of giving a reason in substance, stating that "no data are being used which are subject to the right to information". In addition, an information on the possibilities of lodging a complaint to the supervisory authority **or, where applicable the seeking of a** judicial remedy shall be given." BE said that in BE the data subject must address him-or herself to the supervisory authority to have access to information and that the data subject is not informed about refusal/restriction of access.

[126] BE feared that the Article could lead to the harmonisation of the criminal procedure. BE said that since there is not direct access in BE the controller did not keep documents.

Article 15

Right to rectification, erasure and restriction of processing [127]

1. Member States shall provide for the right of the data subject to obtain from the controller without undue delay the rectification of personal data relating to him or her which are inaccurate.[128] *Having regard to the* **(...)** *purpose of the processing concerned* (…) Member States shall provide that the data subject has the right to obtain completion of incomplete personal data, including by means of providing a supplementary statement.

---

127 DE, ES, PT and SI scrutiny reservation. EE reservation. DE considered that the Article increased the administrative burden. CZ, SI and FR preferred the text of Article 18 in DPFD. UK wanted to see recital 21 be incorporated in the body of the text. EE thought that the Article was too far reaching and that it was necessary to set out the type of data that could be rectified as well as the reasons and justifications for the request to rectify. UK meant that only facts and not personal assessments could be rectified. DE considered that the overall relationship between Articles 4(d), 15(1) and 15(1a) was unclear. DE queried why Article 15 differed from Article 18 of DPFD. DE meant that the accuracy or inaccuracy of statements could not be determined at the level of data protection law but is the main purpose of investigations and the criminal proceedings. DE thought that what the Directive should set out was mere blocking and not the obligation to erase. HR suggested that rights set out in the Article only be carried out *ex officio*, otherwise the effectiveness of the criminal proceedings could be compromised. SE wanted to see *blocking* as well to take into consideration legislation on archives which have requirements on keeping information. FR meant that flexibility should be given to authorities regarding the purposes pursued. BE said that Article 15 did not correspond to the BE system where it was the DPA that asks for rectification, erasure and restrictions of processing. SE meant that restriction was more of a temporary measure than blocking which exists in DPFD and that SE did not approve of the change of terminology. SE further said that it is forbidden in the SE Constitution to erase personal data. UK meant that recital 15 was helpful and that the text therefore could be added to the Article. FR wanted to insert a reference to indirect access in the different paragraphs. DE asked when data should be erased respectively restricted and meant that authorities should not erase only because a time limit had expired, also because it was difficult to erase retained data; it should be enough to block the data. DE pursued that it was very expensive for authorities to erase data it should be enough to block/restrict data and this had to be set out in the Directive. For DE it was very important that the Directive did not require 100 % erasure.

128 FI and UK were concerned about witness testimonies. DE, supported by SE, CZ, saw the problem of rectification as a problem of substance rather than of data protection. SE thought that rectification only concerned "dry rectification of obvious facts" and wanted to clarify the Article with this in mind. DE found it important that data that were inaccurate could be corrected.UK voiced concerns over *who* defined "inaccurate" and asked what type of data could be rectified.

1a. *Member States shall provide for the obligation of the controller to erase personal data without undue delay and of the right of the data subject to obtain from the controller the erasure of personal data (…) concerning him or her without undue delay where the processing does not comply with the provisions adopted pursuant to Articles 4,* **(...)** *7 and 8 of this Directive*[129]*, or where the data have to be erased for compliance with a legal obligation to which the controller is subject.*[130]

1b. ~~**Member States shall provide for the right of the data subject to obtain from the controller the restriction of the processing of personal data where their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data, or where they are required by the data subject for the establishment, exercise or defence of legal claims.**~~[131] **If the accuracy of an item of personal data is contested by the data subject and its accuracy or inaccuracy cannot be ascertained, restriction of the processing of that data item may take place.**

[132]

[129] ES meant that the reference to Articles 4, 7 and 8 was too broad.

[130] DE suggested to delete the paragraph because it meant that the obligation to erase should be dealt with separately in Article 16, as in the Cion proposal.

[131] DE, HR, CZ suggested to delete paragraph 1b because data whose accuracy was contested by the data subject could not be blocked in criminal proceedings or proceedings for the purpose of threat prevention. CH suggested to reword paragraph in the following way: "1b. Member States shall provide for the right of the data subject to obtain from the controller the **blocking of the processing of personal data where their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the dat**a."

[132] CH wanted to add the following paragraph: "1bb. Member States may/shall provide that in case where the accuracy of an item of personal data is contested by the data subject and its accuracy or inaccuracy cannot be ascertained, referencing of that item of data may take place. Personal data shall be blocked instead of erased if they are required by the data subject for the establishment, exercise or defence or legal claims." CH explained that the addition of paragraph (1bb) was necessary in order to make sure that activities of public authorities should not be jeopardized in any way.

2. Member States shall provide that the controller informs[133] the data subject in writing ~~(…)~~ of any refusal of rectification, erasure or restriction of the processing, **and of** the reasons for the refusal. ~~**and the possibilities of lodging a complaint to the supervisory authority or seeking a judicial remedy**~~. [134] **This shall not apply (…) where the provision of such information would undermine a purpose under Article 1 (1) to the extent that such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the individual concerned. Member States shall provide that the controller informs the data subject of the possibilities of lodging a complaint ~~to~~ with ~~the~~ a supervisory authority or seeking a judicial remedy.**

[133] UK believed that the controller's ability to refuse the request was not sufficiently set out and would prefer text similar to prefer text similar to Article 13.1 and a clear stipulation that the controller may refuse if complying would prejudice the prevention, detection, investigation, or prosecution of crime or in negatively impact public security in other ways. In order to limit the obligation to communicate the refusal UK suggested inserting the following text: "This shall not apply where the provision of such information would undermine a purpose under Article 1". For UK a "neither confirm nor deny" provision vital. FR supported the UK and found the obligation to systematically motivate a refusal went too far.

[134] UK thought that it was not always appropriate to indicate why a rectification had been carried out and feared that it could jeopardize an ongoing investigation. CH also wanted to delete paragraph 2.

3. Member States shall provide that in the cases referred to in paragraphs 1, 1a and 1b the controller shall notify the recipients and that the recipients shall rectify, erase or restrict[135] the processing of the personal data under their responsibility.[136]

137

[135] DE wanted to delete "erase and restrict".

[136] DE wanted to add the following text to the end of the sentence: "if these measures are important for the recipient or necessary to protect the data subject's rights." DE scrutiny reservation. DE meant that despite its addition it was necessary to decide whether the provision should be further lifted. DE said that the broad legal definition of recipients could create problems for the application of Article 15(3).

[137] BE suggested, supported by IE, CH, BG, FR, CZ, DK, HU, a new Article 15a as follows: "*Article 15a* **Limitations to the right to rectification, erasure and restriction of processing**

1. Member States may adopt legislative measures delaying, restricting or omitting the right to rectification, erasure and restriction of processing of the data subject pursuant to Article 15 to the extent that, and as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the individual concerned:

   (a) to avoid obstructing official or legal inquiries, investigations or procedures;

   (b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences, the execution of criminal penalties or the prevention of danger;

   (c) to protect public security;

   (d) to protect national security;

   (e) to protect the rights and freedoms of others.

2. Member States may determine categories of data processing which may wholly or partly fall under the exemptions of paragraph 1.

Article 15a[138]

Verification by the supervisory authority[139] [140]

1. Member states shall provide for the right of the data subject to request, in cases referred to in Article 13[141]***, that the supervisory authority checks the lawfulness of the processing.***[142]

1a. In cases referred to in Article 13 (3) and Article 15 (2) Member States may adopt measures providing that the rights of the data subject may also be exercised through the competent supervisory authority.

2. Member State shall provide that the controller informs the data subject of the right to request the intervention of the supervisory authority pursuant to paragraph 1.

3. When the right referred to in paragraph 1a is exercised, the supervisory authority shall inform the data subject at least that all necessary verifications or a review by the supervisory authority have taken place. and of the result as regards the lawfulness of the processing in question.

---

138 Moved from Article 14

139 BE and FR reservation in substance. FR, UK scrutiny reservation. DE wanted to delete Article 14 and SI would not oppose it if other delegations wanted it. FR expressed doubts about the utility of the Article. SE meant that Article 14 set out self-evident elements and contained too many details but could accept the Article if the SA could decide him or herself what measures should be taken.

140 RO considered that the title of the Article should be changed to "Right to lodge a complaint to the national supervisory authority". Support from FI, AT and SE.

141 BE suggested to add references to Article 15.

142 BE wanted to remove paragraph 1. BE meant that the MS could organise an indirect access via the DPA who would inform the data subject that a control has been carried out.

Article 16

Right to erasure

(…)

Article 17

Rights of the data subject in criminal investigations and proceedings[143]

Member States may provide that the exercise of the rights (…) referred to in Articles **(...)** 10a, 12 and 15 is carried out in accordance with national ~~procedural~~ law[144]where the personal data are contained in a judicial[145] decision or record[146] or case file processed in the course of criminal investigations and proceedings. [147]

---

[143] IE reservation of substance on the application of the Article on courts and tribunals. SE asked for an analysis of the application to courts and tribunals. In contrast CZ and SE welcomed the changes, CZ meant that the Article could also be removed. PT found Article 17 superfluous. Cion said that Directive 95 applies to civil courts but not to criminal proceedings. SE and SK fears about the mixing of criminal procedure law and data protection. SE meant that reference could be made to Article 14 as well. DE feared a creeping harmonisation of the criminal procedure law. SE considered that the Article clashed with national criminal procedure law and that the exceptions set out were not sufficiently broad. SE said that courts had information that did not form part of the judgement or the minutes of the process.

[144] IE reservation of substance on the insertion of *procedural law*. IE meant that *national procedural law* narrows the scope. ES scrutiny reservation on the notion *national procedural law*. SK found that *national procedural law* would create problems for criminal law. SI meant that *national procedural law* could be dealt with in the recitals.

[145] HU, BG suggested to add "police and public prosecutorial" after *judicial decision* and DE asked if prosecutors' *decisions were covered as well.* HR supported the addition of *police* after decision.

[146] HU, BG wanted to add "documents, registry and decisions of police and public prosecutors".

[147] AT, SI and PL queried the need of the Article if the purpose was, according to the Cion, only to set out modalities. On the opposite, NO considered the Article necessary and that it should be applicable to both the police and the judiciary. DE shared NO view and commented that Article 4.4 in the DPFD contained a similar provision. CZ, NL, SE preferred the wording of the DPFD. SE thought that the scope had become broader than in the DPFD. EE considered that the Article had become more ambiguous and wanted it to be clearer. HU wanted to cover decisions by the police, the public prosecutor and criminal proceedings. ES also wanted to include police proceedings as it was not always easy to know when one kind of proceedings finished and another started. DE supported this view. FI meant that at least the words "and proceedings" should be deleted.

CHAPTER IV

CONTROLLER AND PROCESSOR[148]

SECTION 1

GENERAL OBLIGATIONS

Article 18

Obligations of the controller [149]

1. Member States shall provide that, taking into account the nature, scope, context and purposes of the processing as well as the likelihood and severity of risk for the rights and freedoms of individuals, the controller implements appropriate measures and be able to demonstrate that the processing of personal data is performed in compliance with the provisions adopted pursuant to this Directive.

1a. Where proportionate in relation to the processing activities[150], the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies[151] by the controller which specify the application of the data protection rules adopted pursuant to this Directive.[152]

2. (…)

---

148 PT scrutiny reservation on Chapter IV.

149 IT scrutiny reservation on Article 18.

150 RO thought that the words *proportionate in relation to the processing activities* were too vague and did not leave room to ensure conformity with the stipulations of the Directive.

151 In view of Article 19, RO, BG asked for a clarification of the term *policies*, DE too and what significance it had for *measures* referred to in paragraph 1 and 1a. CZ, also asked for clarifications on what was meant with *policies* CZ considered it superfluous and that it therefore should be deleted.

152 DE, FR, IE suggested to remove the last part of paragraph 1a as well as in recital 38.

Article 19[153]

Data protection by design[154] ***and by default*** [155]

1. *Having regard to available technolgy*[156] *and the cost of implemention and taking into account* ~~**of**~~ the *nature, scope*, context and purposes of the processing as well as the likelihood and severity of the risks for rights and freedoms of individuals, Member States shall provide that, the controller shall implement ~~**appropriate**~~ technical and organisational measures ~~**and procedures**~~ appropriate to the processing activity being carried out and its objectives, such as pseudonymisation, in such a way that the processing will meet the requirements of provisions adopted pursuant to this Directive and protect the rights of data subjects.

153 DE and RO scrutiny reservation on Article 19. Cion explained that the reasons to maintain the Article were the same as in the GDPR and that the principles were necessary, that they applied to all stages in the processing and not only to automated processing.

154 FR, BE meant that since the concept of *privacy by design* was incompatible with the data processing existing at the entry into force of the Directive it would be necessary to insert a provision indicating that the existing processing operations created and implemented in accordance with the legislation in force before the entry of this proposal would be maintained.

155 FR reservation. UK, supported by RO, supported the principle in Article 19 and considered that the text must be flexible and considered that the text would be better placed in the recitals. UK further considered that the purpose should not be to set out "the state of the art" because it could be expensive. SE also supported the principle. SE did not consider it appropriate to legislate directly but that such principles should be set out in a recital. SI expressed doubts about the whole Article 19 and suggested to delete it since it was not appropriate for police and judicial cooperation. SI scrutiny reservation. EE generally supported the idea of data protection by design and by default. DE also wanted to see a more flexible text. With a reference to Article 2.2 and recital 15, DE considered that the Directive covered this all way. DE suggested to set out in Article 19 what can be achieved "insofar as possible", since this would make the Article more flexible.

156 FR scrutiny reservation on the term "available technology".

2. Member States shall provide that the controller shall implement **appropriate measures** ~~**mechanisms**~~, in particular for automated processing, for ensuring that, by default, only **(...)** personal data which are necessary[157] for each specific purpose of the processing are processed; this applies to the amount of (…) data collected, the extent of their processing, the period of their storage and their accessibility.[158]

Article 20

Joint controllers

(1) Member States shall provide that where two or more controllers jointly determine the purposes and means of the processing of personal data, they are joint controllers. They shall in a transparent manner **(...)** determine their respective responsibilities for compliance with the provisions adopted pursuant to this Directive, in particular as regards ~~**the procedures and mechanisms for**~~ **the** exercising **of** the rights of the data subject [159]and their respective duties to **provide** the information referred to in Article 10a **(...)**, unless and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. **(...)** Member States ~~**shall**~~ **may** designate which of the joint controllers ~~**shall**~~ **can** act as single point of contact for data subjects to exercise their rights.

1a. **(...)** Without prejudice to Article 17, Member States shall provide that the data subject may exercise his or her rights under the provisions adopted pursuant to this Directive in respect of and against each of the controllers.[160]

---

157 ES and PL suggested to replace *necessary* with *appropriate* to provide more flexibility and said that the wording of Article 4.1 (c) was better. Cion said that necessary related to the minimisation principle. Cion further said that the proportionality of cost was the guidance and that cost could also be set out in paragraph 2.

158 DE, SE and CZ considered that proportionality should be addressed in paragraph 2 as well. CZ suggested to add a reference to "the state of the art and the cost" in paragraph 2 as well.

159 IE suggested to delete the last part of the paragraph from 'and their respective duties…' because the text was too detailed.

160 IE suggest to delete the paragraph because the text was too detailed.

Article 21

Processor

1. Member States shall provide that the controller shall use only (…) processors providing sufficient guarantees to implement appropriate technical and organisational measures (…) in such a way that the processing will meet the requirements of the provisions adopted pursuant to this Directive (…).

1a. Member States shall provide that the processor shall not enlist another processor without the prior specific or general written consent of the controller. In the latter case, the processor should always inform the controller on any intended changes concerning the addition or replacement of other processors, thereby giving the opportunity to the controller to object to such changes.

2. Member States shall provide that the carrying out of processing by a processor shall be governed by a legal act under Union or Member States law, including a contract, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the rights of the controller and stipulating in particular that the processor shall act only on instructions[161] from the controller (…).[162]

3. (…)

[161] DE preferred to use "within the scope of" rather than "on instructions from".

[162] SI scrutiny reservation.

Article 22

Processing under the authority of the controller and processor[163]

(…)

Article 23

Records of categories[164] ***of personal data processing activities***[165]

1. Member States shall provide that each controller **(...)** shall maintain a record[166] of all categories of personal data processing activities (…) (...) under its responsibility. This record shall contain (…) the following information:

(a) *the name and contact details of the controller and any joint controller* (…) **(...),** and data protection officer, if any;

(b) the purposes of the processing;

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

(**ca**) a description of the categories of personal data concerning ~~**the**~~ data subject**s**;

(d) where applicable, the categories of transfers of personal data to a *third country or an international organisation* (…)*;*

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

---

163 Cion reservation on deletion, referring to Article 21 of DPFD.

164 UK sought clarification on what category or type of record was required by the Article, *e.g.* was it necessary to list every single type of processing or was it enough to keep categories such as *defendant data* and *witness data?* BE, supported by DE, PT, BG and RO, asked what was meant with *categories* and noted that no explication was provided in the recitals. DE noted that this wording did not correspond to the wording in DPFD or Article 28 in GDPR and that the provision was stricter and that DE said no to these stricter rules.

165 SI and PT scrutiny reservation. FR meant that the notion *processing* activities was too large and that it was necessary to frame it. RO asked what the data in this Article may contain and who would check whether this record was properly documented. DE noted that Article 23 and especially Article 24 derogated from the documentation obligation in Article 10 of DPFD and Article 28 of GDPR. DE further considered that the terminology in both Articles remained vague and therefore problematic.

166 UK asked what kind of records/categories were intended.

(f) where possible, a general description of the technical and organisational security measures referred to in Article 27(1).

2. (…)

2a. Member States shall provide that each processor shall maintain a record of all categories of personal data processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting; ~~and of the controller's representative, if any~~;

(b) the name and contact details of the data protection officer, if any;

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

(d) (...)

(e) (...)

(f) where possible, a general description of the technical and organisational security measures referred to in Article 27(1).

2b The records referred to in paragraphs 1 and 2a shall be in writing, including in an electronic or other non-legible form which is capable of being converted into a legible form.

3. *On request*, the controller and the processor shall make the record available to the supervisory authority.

Article 24

Logging[167]

1. Member States shall [168]ensure that logs are kept of at least the following processing operations *in automated processing systems*[169]: collection, alteration, consultation, disclosure, combination or erasure.

[167] DE, UK scrutiny reservation. NO reservation. ES feared that the Article would cause administrative burden and suggested to remove the Article. DE, BE considered that the obligation to keep record created a disproportional bureaucracy. PT raised concerns regarding the proportionality of the obligation and the administrative burden it would entail. IT saw the need for having a policy on records keeping.
DE noted that Article 23 and especially Article 24 derogated from the documentation obligation in Article 10 of DPFD and Article 28 of GDPR. DE further considered that the terminology in both Articles remained vague and therefore problematic. DE suggested the following new wording for Article 24: "1. In automated processing systems all transmissions of personal data shall be logged or documented for the purposes of verifying the lawfulness of the data processing, self-monitoring and proper data integrity and security. 2. Logs or documentation prepared under paragraph 1 shall be communicated on request to the competent supervisory authority to monitor data protection. The competent supervisory authority shall use this information only to monitor data protection and ensure proper data processing as well as, data integrity and data security." DE concluded that it had not yet finished its deliberations as to whether the obligation to document is to be introduced for all transmissions or only in automated processing systems. SE said that logging related to possibility to trace and security of information and that the Article therefore should be better placed after Article 27. IT meant that is was an important Article, compared with Article 10 DPFD and for Prüm. NL had doubts about the purpose and meant that the Article seemed more linked to documentation. AT asked what would happen if the data was not subject to automatically registration.

[168] ES suggested to move the words *as far as possible* to after the "The MS shall".

[169] Cion, AT and FI reservation on the restriction of *automated processing systems.*

The logs of consultation and disclosure shall show: [170](…) the reason, the date and the time of such operations and, as far as possible[171], the identification of the person who consulted or disclosed personal data. [172]

2. The logs shall[173] be used (...) for **(...)** verification of[174] the lawfulness of the data processing, self-monitoring and for ensuring data integrity and data security.

Article 25

Cooperation with the supervisory authority

(…)

[170] RO wanted to insert "at least" between *show* and *the purpose*, so that MS would have the possibility to provide for extra options to be shown in logs in order to thoroughly document the processing operation.

[171] FR, MT, CZ, BE and ES wanted the phrase *as far as possible*, to be moved to the start of paragraph 1.SK and SE wanted to remove the words *as far as possible.* FR, supported by IE, suggested the following drafting for Article 24: " As far as possible, Member States shall ensure that records are kept of at least the following processing operations: collection, alteration, consultation, disclosure or erasure in automated processing systems. The records of consultation and disclosure shall show in particular the date and time of such operations and the identification of the person who carried out such operations."

[172] UK thought that such records might entail disproportionate costs and burdens and suggested a reference to proportionality and the cost involved.

[173] FR asked to replace *shall* with *may.*

[174] SE suggested to replace *for the purposes of verification of* with *to provide the possibility to establish.*

Article 26

Prior consultation of the supervisory authority[175]

1. Member States shall ensure that the controller or the processor consults[176] the supervisory authority prior to the processing of personal data which will form part of a new [177]filing system[178] to be created[179] where:

(a) special categories of personal data referred to in Article 8 are to be processed;

(b) the type of processing, in particular where using new technologies, mechanisms or procedures, involves high risk for the (…) **(...)** rights and freedoms (…) of data subjects.[180]

1a. **~~In the case of a processing referred to in Article 7~~ (...)** Member States shall ensure that the supervisory authority is consulted during the preparation of proposals for legislative or regulatory measures which provide for the processing of personal data referred to in paragraph (1).[181]

2. Member States may provide that the supervisory authority establishes a list of the processing operations which are subject to prior consultation pursuant to paragraph 1.

---

175 Scrutiny reservation for UK, DE, ES, SI. SE reservation.

176 FR wanted to know the value of the consultation, was it a simple consultation or were legal consequences attached to it.

177 DE, supported by CZ, IE and PL, suggested inserting "automated" before *filing system* because non-automated files and filing systems did not pose a threat justifying prior consultation of the SA.

178 SE and UK asked why a new filing system triggered the consultation of the SA.

179 FR would like the phrase *a new filing system to be created* to be replaced with *processing.*

180 DE, supported by CZ, IE and PL, wanted it to be clarified that the consultation should take place only for automated processing.

181 CZ and UK scrutiny reservation. SE found that the SA should not be consulted when new legislative proposals were prepared because such proposals were national legislation so in line with the subsidiarity principle this was up to the MS to legislate but if the Directive would be covering domestic processing it would be acceptable.

3. Member States shall provide that where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 does not comply with the provisions adopted pursuant to this Directive, in particular where risks are insufficiently identified or mitigated, the supervisory authority shall within a maximum period of 6 weeks[182] following the request for consultation give advice to the data controller, in writing. This period may be extended for a further month, taking into account the complexity of the intended processing. [183] Where the extended period applies, the controller or processor shall be informed within one month of receipt of the request of the reasons for the delay.[184]

SECTION 2

DATA SECURITY

Article 27

Security of processing

1. Having regard to available technology and the costs of implementation and taking into account the nature, scope, *context* and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of individuals, Member States shall provide[185] that the controller and the processor implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (…).

---

182 SE and PT scrutiny reservation on the time limit.

183 FR voiced concerns about the new paragraph 3, because its usefulness and implementation remained unclear. FR considered that the time limit should be extended to two months. SI meant that this paragraph was too prescriptive and wanted its removal.

184 DE suggested adding a paragraph for urgent cases as follows: "4. Member States may provide that the controller or processor may consult the supervisory authority without undue delay after the processing referred to in paragraph 1, if otherwise serious disadvantages for the purposes mentioned in Article 1 (1) are expected".

185 FR suggested to replace *provide* with *ensure* since this article establishes an obligation to achieve a result, which is, moreover, incompatible a priori with the limits imposed later in the text in relation to technical developments and the cost of their implementation. Support from AT referring to Article 22 in DPFD.

2. In respect of automated data processing, each Member State shall provide that the controller or processor, following an evaluation of the risks[186], implements measures designed to[187]:

(a) deny unauthorised persons access to data-processing equipment used for processing personal data (equipment access control);

(b) prevent the unauthorised reading, copying, modification or removal of data media (data media control);

(c) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);

(d) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);

(e) ensure that persons authorised to use an automated data-processing system only have access to the data covered by their access authorisation (data access control);

(f) ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment (communication control);

(g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data were input (input control);[188]

(h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control);

(i) ensure that installed systems may, in case of interruption, be restored (recovery);

---

186 FR expressed concerns about the concept of the *evaluation of the risk* and believed that this evaluation should be obligatory only for the processing of the most sensitive types of data, as is the case in the GDPR.

187 FR stated that a better alignment between paragraph 2 and Article 3(9) defining *personal data breach*, where the concepts of *accidental or unlawful destruction, loss* were worded differently. FR also pointed out that the list of security measures did not seem appropriate for all types of processing, nor for all architectures, and that it did not guarantee the technological neutrality of the Directive. FR believed that the specification of the scope of this provision should be kept to a minimum and that the list should be indicative. FR suggested that the list currently given in Article 27(2) should instead be set out in a recital, for instance at the end of the new recital 37b, to provide examples of such measures.

188 FR pointed out that the reference should be made to Article 24(1) in order to harmonise traceability obligations, rather than create a new obligation here.

(j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported (reliability) and that stored personal data cannot be corrupted by means of a malfunctioning of the system (integrity).

3. (…)[189]

Article 28

Notification of a personal data breach to the supervisory authority[190]

1. Member States shall provide that in the case of a personal data breach which is likely to result in a high risk for the rights and freedoms of data subjects**, (...)** the controller notifies, without undue delay (…) and, where feasible, not later than 72 hours after having become aware of it, the personal data breach to the supervisory authority (…). The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours.

1a. The notification referred to in paragraph 1 shall not be required if a communication of the data subject is not required under Article 29(3)(a) **and (b). ~~to (c).~~** [191]

2. The processor shall alert and inform the controller without undue delay after having become aware of a personal data breach.

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

(a) describe the nature of the personal data breach,

(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;

(c) (…)

(d) describe the likely consequences of the personal data breach identified by the controller,

---

189 Cion reservation on deletion of paragraph 3.

190 DE, NO, BG, FI and SI entered scrutiny reservations. DE found it necessary to ensure that the notifications and their handling by the supervisory authorities endanger neither the legitimate interests of third parties nor police and judicial interests. Cion reservation: consistency with the e-Privacy Directive should be kept. UK was concerned that there may be cases where it could prejudice on-going, sensitive investigations if a law enforcement agency is required to communicate the breach to the DPA.

191 NL scrutiny reservation. NL wanted to delete paragraph 1a since it could undermine paragraph 1. SI wanted to delete the paragraph. AT reservation. Cion meant that the paragraph could dilute the obligation to notify and therefore suggested to further develop recital 42 to take account of this.

(e) describe the measures taken or proposed to be taken[192] by the controller to address the personal data breach; and

(f) where appropriate, indicate measures to mitigate the possible adverse effects of the personal data breach.

3a. Where, and in so far as, it is not possible to provide the information referred to in paragraph 3 (d), (e) and (f) at the same time as the information referred to in points (a) and (b) of paragraph 3, the controller shall provide this information without undue further delay.

4. Member States shall provide that the controller documents any personal data breaches referred to in paragraph 1, comprising the facts surrounding the breach, its effects[193] and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. **(...)**

194

---

192 FR believed that the obligation to propose measures to address any negative consequences of the breach should be mitigated by the insertion of *where appropriate* after *taken.*

193 FR wanted that the obligation to describe the nature of the data breach be formulated in a more realistic manner and therefore asked for the phrase *identified by the controller* to be added after *its effects*.

194 HR wanted to insert a new paragraph 4a with the following wording: "(4a) Competent authority monitors the protection of personal data at the request of the respondents, on a proposal from a third party or ex officio." DE suggested to insert the following new paragraph because the obligation to incriminate oneself could be problematic in terms of fundamental rights "4a. In the event that proceedings must be brought against a controller or processor on account of a violation of duty which necessitates the measures under Articles 28 or 29, Member States may provide that the measures taken by the controller and processor under Article 28 and 29 may not be used in these proceedings."

5. (…)
6. (…)

195

195 BE, HU suggested inserting an Article 28a with the following heading "Communication of the data breach to the concerned Member States' controllers" and the following text:
"1. Member States shall provide that in the case of a personal data breach which is likely to severely affect the rights and freedoms of data subjects, the controller from a MS where the breach happened notifies, without undue delay (...) the personal data breach to the controller of the MS from which the data are originated or have been transferred to (...).
2. The notification referred to in paragraph 1 shall not be required if a communication of the data subject is not required under Article 29(3)(a) and (b).
3. The notification referred to in paragraph 1 shall at least describe the nature of the personal data breach, the likely consequences of the personal data breach identified by the controller, and the measures taken or proposed to be taken by the controller to address the personal data breach. (...)
4. Member States shall provide that the controller from the MS where the breach happened documents any personal data breaches referred to in paragraph 1, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the controller of the MS from which the data are originated to take the first measure in order to limit the breach. The documentation shall only include the information necessary for that purpose".

Article 29

Communication of a personal data breach to the data subject[196]

1. Subject to paragraphs 3 and 4 of this Article, Member States shall provide that when the personal data breach is likely to result in a high risk for the rights and freedoms (…) of the data subject **(...)** the controller shall **(...)** communicate the personal data breach to the data subject without undue delay. **[197]**

---

196 CZ, DE, EE, FI, NO, SI scrutiny reservations. ES and PT suggested to delete Article 29, ES because it represented a risk for the security and PT because the communication should be indirect in criminal proceedings. SI objected to the deletion and stated that it could be necessary for the right of defence (judicial right). NL also saw a problem informing the data subject of a breach and was generally hesitant to the need to notify the data subject. FR wondered if it was necessary to notify only the supervisory authority. Support from ES, NL. DE also cautioned against bureaucracy. Cion reservation: consistency with the e-Privacy Directive should be kept. UK urged strongly for an exemption to this in situations where communicating the breach to the data subject might prejudice an investigation. CY also raised concerns about the interference with ongoing investigations. FR, supported by CH, asked that the communication provided for in this article be limited to data subjects who have the right of information over their personal data. FR also believed that this article, like those relating to data subjects' rights in Chapter III, should establish the principle of the absence of notification, except:
where the personal data affected by the security breach relate to a data subject with the right of information, in cases which do not fall within the restrictions of data subjects' rights allowed by our proposal for Article 10; and where the security breach is particularly harmful to the data subject's rights and freedoms. FR therefore suggested the following drafting for Article 29:
"Article 29
Communication of a personal data breach to the data subject

1. The communication of a personal data breach to the data subject may be delayed, restricted or omitted on the grounds referred to in Article 10.
2. When the communication of a personal data breach is not restricted or omitted according to paragraph 1 and subject to paragraphs 3 and 4 of this Article, Member States shall provide that when the personal data breach is likely to severely affect the rights and freedoms (…) of the data subject, the supervisory shall, after the notification referred to in Article 28, communicate the personal data breach to the data subject without undue delay.
3. The communication to the data subject referred to in paragraph 2 shall describe the nature of the personal data breach (…).
4. The communication (…) to the data subject referred to in paragraph 2 shall not be required if:
   (a) the controller (…) has implemented appropriate technological protection measures, and those measures were applied to the personal data affected by the personal data breach in particular those that render the data unintelligible to any person who is not authorised to access it; or
   (b) the controller has taken subsequent measures which ensure that the data subjects' rights and freedoms are no longer likely to be severely affected; or
   (c) it would involve disproportionate effort, in particular owing to the number of cases involved. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner."

197 NL reservation.

2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach ~~(…)~~ and shall contain at least the information referred to in Article 28(3) (b)(e) and (f).

3. The communication (…) to the data subject referred to in paragraph 1 shall not be required if:

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

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

(c) it would involve disproportionate effort, in particular owing to the number of cases involved. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.[198]

4. The communication to the data subject referred to in paragraph 1 may be delayed, restricted or omitted on the grounds referred to in Article 10a (3).

199

200

---

198 SE asked if it was acceptable to require communication to the data subject when there was no obligation to notify him or her (29.3(c)). In the same vein FR and BE that meant that it was enough to inform only the data subject that had the right to be informed and not all data subjects. BE added that with the indirect access the data subject never knows.

199 BE and NL suggested inserting a new paragraph 5 with the following wording: "Member States may determine by law categories of data processing which may wholly or partly fall under the grounds referred to in paragraph 4".

200 BE and NL suggested inserting a new paragraph with the following wording: "Member States shall provide that where the data breach involves personal data that have been transmitted by another Member State, the information, meant in Article 28(3), will be communicated to this Member State without undue delay".

SECTION 3

DATA PROTECTION OFFICER [201]

Article 30

Designation of the data protection officer[202]

1. Member States may[203], or where required by *Union law* **(...)** shall, provide that the controller or the processor designates a data protection officer.

2. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 32, particularly the absence of any conflict of interests. **[204]**

3. A single data protection officer may be designated for several competent **(...)** authorities, taking account of their organisational structure (…) and size. [205]

4. *Member States shall provide that the controller or the processor ensures that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.*

---

201 PT wanted to delete the whole section 3 because a DPO would not be bound by the professional secrecy and should not have access to all information. Introducing a DPO in PT law would entail constitutional problems.

202 DE, EE, and SI scrutiny reservations. DK asked whether "shall provide ..." could refer to collective agreements as well Referring in particular to paragraphs 2 and 3, PL preferred not having so many details on the designation of a DPO. BE wanted to add an Article setting out that rules on professional secrecy should be applicable to the DPO.

203 Cion reservation on replacing the mandatory DPO by an optional DPO. DE, AT, BG and NL supported that the designation of a DPO should be mandatory since it was important to have harmonised rules on this. Cion stated that if the designation of a DPO was voluntary it would be necessary to harmonise the tasks. ES informed that in the context of the examination of the Regulation it had defended a voluntary DPO and did so for the Directive as well.

204 PL wanted to delete paragraph 2.

205 PL wanted to delete paragraph 3 because it considered that the Directive only should contain overarching rules and it should be left the MS to set out the details.

5. *The controller or processor shall ensure that the data protection officer is provided with the means to perform (…) the tasks referred to under Article 32 effectively and can act in an independent manner with respect to the performance of his or her tasks (…).*

206

Article 31

Position of the data protection officer

(…) **207**

Article 32

***Tasks of the data protection officer*[208]**

Member States shall provide that the controller or the processor entrusts the data protection officer (…) with the following tasks:

(a) to inform and advise the controller or the processor **(...)** ~~**who are processing personal data**~~ of their obligations in accordance with the provisions adopted pursuant to this Directive and other Union or Member State data protection provisions (…);

(b) to monitor compliance with provisions adopted pursuant to this Directive, with other Union or Member State data protection provisions and with (…) the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities**,** awareness-raising and training of staff involved in the processing operations and the related audits;

---

206 BE, supported by BE, suggested the inserting of a paragraph 6 as follows: "The data protection officer shall,
both during and after his/her term of office, be subject to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties".

207 DE suggested adding the following text: "The data protection officer shall suffer no disadvantage through the performance of his duties."

208 EE, NO, SI scrutiny reservations. NO, SE and EE considered the Article too detailed.

(c) (…)

(d) (…)

(e) (…)

(f) (…)

(g) to monitor the responses to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, to co-operate with the supervisory authority at the latter's request or on the data protection officer's own initiative;

(h) to act as the contact point for the supervisory authority on issues related to the processing of personal data, including the prior consultation referred to in Article 26, and consult, (…) as appropriate, on any other matter (…).

209

209 FR asked for the insertion of an additional point to be added to the list of tasks to provide that the data protection officer should produce an annual report to submit to the controller.

CHAPTER V
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS[210]

Article 33

General principles for transfers of personal data

1. Member States shall provide that any transfer of personal data by competent (…) authorities (…) to a third country, or to an international organisation, including further onward transfer to another third country or international organisation, may take place only if:[211]

(a) the transfer is necessary for the purposes set out in Article 1 (1)[212][213][214]; and,

(b) (…)

(c) the controller in the third country or international organisation is an authority competent for the purposes set out in Article 1(1)[215]; and

(d) in case personal data are transmitted or made available from another Member State, that Member State has given its prior authorisation to the transfer[216] in compliance with its national law [217] and

---

210 AT, BE, CZ, CY, DE, DK, EE, FI, FR, IT, NL, NO, PL, RO, SI, SK, ES and UK scrutiny reservation on Chapter V.

211 DE suggested to add the following text after "only if" "in addition to the conditions under Article 7" for the sake of legal clarity, including the paragraph 1a (consent by the data subject) suggested by DE

212 AT suggested to add “a specific” before criminal offence in order to clarify that transfer may only take place in a specific case and not as a routine transfer.

213 AT suggested to add “a specific” before criminal penalty in order to clarify that transfer may only take place in a specific case and not as a routine transfer.

214 DE suggested to remove paragraph 1(a) to avoid that the relationship with Article 7 was unclear.

215 BE reservation on the insertion of 'Article 1(1) in the whole of Chapter V.

216 AT wanted to add “including further onward transfer,” after *transfer* to make clear that the consent in also necessary for subsequent transfer.

217 AT suggested to insert another principle after point (d) that transfers may take place only if and insofar as provided for in national law.

(e) the Commission has decided pursuant to Article 34 that the third country or international organisation in question ensures an adequate level of protection or in the absence of an adequacy decision poursuant to Article 34, where appropriate safeguards are adduced or exist pursuant to Article 35. [218] **(…).** [219]

2[220]. Member States shall provide that transfers without the prior authorisation by another Member State in accordance with point (d) shall be permitted only if the transfer of the personal data is necessary for the prevention of an immediate and serious threat to public security of a Member State or a third country or to essential interests of a Member State and the prior authorisation cannot be obtained in good time. The authority responsible for giving prior authorisation shall be informed without delay.

3. Member States shall provide that in the absence of an adequacy decision pursuant to Article 34 or of appropriate safeguards in accordance with Article 35, a transfer may only take place where derogations for specific situations apply pursuant to Article 36 and the conditions laid down in points (a), (c) and (d) of paragraph 1 **and, as the case may be, ~~and~~** in paragraph 2 of this Article are complied with.

---

218 FI, supported by BE, meant that, in line with Article 34, a territory or specified sector within a specific third country should be mentioned in paragraph (e).

219 DE, supported by AT, NL, PL and CY, suggested to insert a paragraph 2 with the following wording: "(2) Member States shall provide that the recipient shall be informed of any processing restrictions and be notified that the personal data may be used only for the purposes for which they are transferred. The use for other purposes shall be allowed only with the prior authorisation of the transmitting member state and, in case personal data had been transmitted or made available from another member state to the transmitting member state, the prior authorisation of the other member state too, or in cases where the requirements of Article 36a are fulfilled". DE had taken this text from removed Article 37 because it found it important as it is a general principle for transfer to third countries, however the part on *reasonable steps* had been deleted. DE found it also important that use for other purposes could only be carried out with the consent of the transferring MS, maybe also the MS from where the data originated (like in Article 33.1 (d).

220 Moved from Article 36a

Article 34

Transfers with an adequacy decision [221]

1. Member States shall provide that a transfer[222] of personal data to a third country or a territory or one or more specified sectors within a third country or an international organisation may take place where the Commission has decided in accordance with Article 41 of Regulation (EU) XXX or in accordance with paragraph 3 of this Article that the third country or a territory or specified sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any specific authorisation. [223]

2. Where no decision adopted in accordance with Article 41 of Regulation (EU) XXX ~~exists~~ **applies**, the Commission shall assess the adequacy of the level of protection, in particular taking into account the following elements:

   (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, data protection rules (…)including concerning public security, defence, national security and criminal law as well as (…) security measures, including rules for onward transfer of personal data to another third country or international organisation, which are complied with in that country or by that international organisation; as well as the existence of effective and enforceable data subject rights and effective administrative and judicial redress for data subjects (…) whose personal data are being transferred;

---

221 DE scrutiny reservation. DE, supported by SK, meant that transfers under Article 34-36 should be considered as being on equal footing and not that Article 35 and 36 be exceptions to Article 34.

222 BE, CZ and FR suggested to talk about "any transfer or set of transfer".

223 DE meant that since *authorisation* could lead to misunderstandings it should be deleted and the following wording be added: " additional assessment in respect of the level of data protection. Decisions taken by the Commission under sentence 1 shall not result in an obligation of Member States to transfer data". With this wording DE also wanted to make clear that there is no obligation to transfer data.

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility (…) for ensuring and enforcing compliance with the data protection rules including adequate sanctioning powers for assisting and advising (…) data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States[224]; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

2a. The European Data Protection Board shall give the Commission an opinion for the assessment of the adequacy of the level of protection in a third country or international organization, including for the assessment whether a third country or the territory or the international organization or the specified sector no longer ensures an adequate level of protection.

3. The Commission after assessing the adequacy of the level of protection, may decide, within the scope of this Directive that a third country or a territory or one or more specified sectors within that third country or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority(ies) mentioned in point (b) of paragraph 2. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 57(2).

4. (…)

4a. The Commission shall monitor the functioning of decisions adopted pursuant to paragraph 3 **(…).**

[224] Cion scrutiny reservation.

5. The Commission may decide within the scope of this Directive that a third country or a territory or a specified sector within that third country or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2, and may, where necessary, repeal, amend or suspend such decision without retro-active effect. The (…) implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2), or, in cases of extreme urgency, in accordance with the procedure referred to in Article 57(3).

5a. **(…)** *The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.*

6. Member States shall ensure that where a decision pursuant to paragraph 5 is taken, such decision (…) shall be without prejudice to transfers of personal data to the third country, or the territory or the specified sector within that third country, or the international organisation in question pursuant to Articles 35 and 36 (…).

7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and specified sectors within a third country and international organisations in respect of which decisions have been taken pursuant to paragraphs 3~~, 3a~~ and 5.

8. (…)

Article 35

Transfers by way of appropriate safeguards

1. (…)*In the absence of a decision pursuant to paragraph 3 of Article 34*, Member States shall provide that ~~**a controller or processor may**~~ **a** transfer **of** personal data to a third country or an international organisation **may take place** where:

   (a) appropriate safeguards with respect to the protection of personal data[225] have been adduced in a legally binding ~~**and enforceable**~~[226] instrument; or

   (b) the controller (…) has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with respect to the protection of personal data[227]. Such an assessment may take into account the existing cooperation agreements between Europol and/or Eurojust and third countries which allow for the exchange of personal data.[228]

   [229]

2. (…)

---

225 DE meant that it was important that the criteria in Article 34(2) be applied as well and suggested adding the following text after *personal data* "taking account of the criteria set out in Article 34 (2),"

226 DE raised concerns, supported by CY, BG, ES, IT, IE, SE, HR, DK, UK and CH, about *enforceable* and found that it was a too high requirement and wanted more flexibility.

227 AT scrutiny reservation on Article 35.1(b). HU, supported by NL, requested the deletion of Art. 35 para 1. b) HU because it believed that it was not an appropriate safeguard if the controller may, on his own, asses the circumstances before transferring the data. HU meant that the assessment prior to the transfer should be linked to objective criteria; as an alternative solution, HU suggested the insertion of prior authorisation by the SA in the receiving country.

228 DE scrutiny reservation on paragraph (1)(b). Cion scrutiny reservation on paragraph (1)(b) linked to the fact that to it was not aware of any adequacy decision taken on the basis of Article 13 of DPFD.

229 ~~FR suggested adding a subparagraph (c) with the following wording: "the transfer is necessary in the framework of a police or judicial cooperation in criminal matters, provided that the legal basis for such cooperation includes data protection provisions".~~

Article 36

Derogations for (…)specific situations

1. (…)*In the absence of an adequacy decision pursuant to Article 34 or appropriate safeguards pursuant to Article 35*, Member States shall provide that, a transfer or a category of transfers of personal data to a third country or an international organisation may take place only on condition that:

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

   (b) the transfer is necessary to safeguard legitimate interests of the data subject ~~**relating to the purposes set out in Article 1 (1**~~) where the law of the Member State transferring the personal data so provides; or

   (c) the transfer of the data is necessary for the prevention of an immediate and serious threat to public security of a Member State or a third country; or

   (d) the transfer is necessary in an individual case for the purposes set out in Article 1 (1); or

   (e) the transfer is necessary in an individual case~~s~~[230] for the establishment, exercise or defence of legal claims relating to the purposes set out in Article 1 (1). [231]

[230] UK, supported by BE, CZ and CH, feared that *individual cases* could be interpreted narrowly and therefore suggested to delete these words and explain in the recitals.

[231] CH suggested, supported by BE, ES and CZ, inserting a paragraph (f) with the following text: "(f) the data subject has given his or her consent to the transfer of his or her personal data for one or more specific purposes." (this could be used when the transfer is in the interest of the victim). FR suggested a paragraph (f) with this wording: "The transfer is necessary to safeguard legitimate prevailing interests, especially important public interests".

2. Personal data shall not be transferred if the transferring competent authority determines that (…)**fundamental** rights **and freedoms ~~or legitimate interests~~** of the data subject concerned override the public interest **(…)** in the transfer set out in points (d) and (e) of paragraph 1.[232]

Article 36a

(…)

Article 36a~~a~~[233]

Transfer of data to ~~private parties~~ **recipients and public authorities established in third countries**

1. By way of derogation to Article 33 (1) (c) and without prejudice to any international agreement referred to in paragraph 2, Union or Member States law may provide that the competent authorities may, in individual and **(…)** specific cases, transfer personal data directly to **~~private parties~~ recipients and public authorities** established in third countries only if the other provisions of this Directive are complied with and the following conditions are fulfilled:
   (a) the transfer is essential and strictly necessary for the performance of a task of the competent authority as provided for by Union or Member State law for the purposes (…)set out in Article 1(1); and
   (b) **(…)**[234]
   (c) **(…)**[235]
   (d) the transferring competent authority determines that no **fundamental** rights **~~or legitimate interests~~ and freedoms** of the data subject concerned override the public interest necessitating the transfer in the case at hand.

2. An international agreement referred to in paragraph 1 shall be any bilateral or multilateral international agreement in force between Member States and third countries in the field of judicial co-operation in criminal matters and police co-operation. **~~to the extent that such agreements are compatible with Union law.~~**

---

232 IE, AT, FR, LT, PT, CY scrutiny reservation. UK wanted to delete the paragraph.
233 FR, FI, SK, UK, AT and Cion scrutiny reservation.
234 AT wanted to keep paragraph (1) (b).
235 FI, AT and NL wanted to keep paragraph (1) (c).

Article 37

Specific conditions for the transfer of personal data

Article 38

International co-operation for the protection of personal data

(…)

CHAPTER VI

INDEPENDENT SUPERVISORY AUTHORITIES

SECTION 1

INDEPENDENT STATUS

Article 39

Supervisory authority

1. Each Member State shall provide that one or more independent public authorities are responsible for monitoring the application of the provisions adopted pursuant to this Directive.

1a. Each supervisory authority shall contribute to the consistent application of this Directive throughout the Union. (…) For this purpose, the supervisory authorities shall co-operate with each other and the Commission[236] in accordance with Chapter VII.

2. Member States may provide that a supervisory authority established (…) under Regulation (EU)/ XXX **may be the supervisory authority referred to in this Directive and** assumes responsibility for the tasks of the supervisory authority to be established under paragraph 1 of this Article.

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which (…) shall represent those authorities in the European Data Protection Board.

[236] SE and UK wanted to delete the reference to the Cion.

Article 40

Independence

1. Member States shall ensure that each supervisory authority acts with complete independence in performing the tasks and exercising the powers entrusted to it.
2. (…) Member States shall provide that the member or **(…)** members of **(…)** each supervisory authority, in the performance of their tasks and exercise of their powers in accordance with this Directive, remain free from external influence, whether direct or indirect and neither seek nor take instructions from anybody.
3. (…)[237]
4. (…)[238]
5. (…) Member States 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 tasks and exercise of its powers including those to be carried out in the context of mutual assistance, co-operation and active participation in the European Data Protection Board.
6. (…) Member States shall ensure that each supervisory authority must have its own staff which shall ~~be appointed by and~~ 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 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.

[237] Cion reservation against deletion. DE and FR also preferred to reinstate paragraph 3, but DE wanted to use the singular or plural for the members.

[238] Cion reservation against deletion. DE also preferred to reinstate paragraph 4 but using the singular or plural for the members.

Article 41

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 either by the parliament and/or the government or the head of **S**tate of the Member State concerned or by an independent body entrusted by Member State law with the appointment by means of a transparent procedure.
2. The member or members shall have the qualifications, experience and skills required to perform their duties and exercise their powers.
3. (…)[239]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 **law, ~~concerned.~~**
4. (…)[240]
5. (…)[241]

[239] Cion scrutiny reservation against deletion.
[240] Cion scrutiny reservation against deletion.
[241] Cion scrutiny reservation against deletion.

Article 42

Rules on the establishment of the supervisory authority

1**.** Member State**s** 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**;**

(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 be no less than four years, except for the first appointment after entry into force of this Directive, 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) (…)

1a. *Member States shall provide that* 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.

Article 43

Professional secrecy

(…)

SECTION 2

TASKS AND POWERS

Article 44

Competence

1. Member States shall provide that each supervisory authority shall be competent ***on the territory of its own Member State*** to perform the tasks and exercise (…) the powers conferred on it in accordance with this Directive. ~~**on the territory of its own Member State**~~.

2. Member States shall provide that the supervisory authority is not competent to supervise processing operations of **(…)**[242] courts when acting in their judicial capacity. [243] [244] **Member States may provide that the supervisory authority is not competent to supervise processing operations of other independent judicial authorities when acting in their judicial capacity.**

---

242 CH preferred the wording of recital 55, CH, AT, BE, IT suggested to replace *independent judicial bodies* with "national courts or other judicial authorities".

243 ES suggested adding “and other matters assigned to bodies or authorities of the judiciary related to their judicial capacity.” ES meant that such wording was necessary to ensure the independence of the judiciary enshrined in the Constitutions of the MS, so that all treatments related to the judicial capacity fell outside the administrative control, and remained within the judiciary.

244 DE and HU scrutiny reservation. SI considered that the prosecution office and the police should be put on equal footing with the judiciary and be excluded for the SA supervision..

Article 45

Tasks

1. Member States shall provide that each supervisory authority shall on its territory:

(a) monitor and enforce the application of the provisions adopted pursuant to this Directive and its implementing measures;

(aa) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data;

(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 data subjects' rights and freedoms with regard to the processing of personal data;

(ac) promote the awareness of controllers and processors of their obligations under the provisions adopted pursuant to this Directive;

(ad) upon request, provide information to any data subject concerning the exercise of his or her rights under the provisions adopted pursuant to this Directive and, if appropriate, co-operate with the supervisory authorities in other Member States to this end;

(b) deal with complaints lodged by data subject, or body, organisation or association representing **and duly mandated by a data subject ~~in accordance with Article 50~~,** 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 where further investigation or coordination with another supervisory authority is necessary;

(c) check the lawfulness of data processing pursuant to Article **15a~~14~~**, and inform the data subject within a reasonable period on the outcome of the check or on the reasons why the check has not been carried out;

(d) 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 the provisions adopted pursuant to this Directive;

(e) conduct investigations on the application of the provisions adopted pursuant to this Directive **(…)**, including on the basis of a information received from another supervisory or other public authority, **(…) (…);**

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

(g) **(…)**

(h) give advice on processing operations referred to in Article 26;

(i) contribute to the activities of the European Data Protection Board.

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. Member States shall provide that 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. **Member States shall provide that** ~~**W**~~**w**here requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may refuse to act on the request [245]. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 46

Powers

(1) Each Member State shall provide by law that its supervisory authority shall have ~~**at least the following**~~ *investigative* powers, **such as:**

~~**(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 notify the controller or the processor of an alleged infringement of the provisions adopted pursuant to this Directive;**~~

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

~~**(ac) 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.**~~

(1a) Each Member State shall provide by law that (…) its supervisory authority shall have corrective powers such as, **for example (…)**

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions adopted pursuant to this Directive;

[245] CH suggested to add *can charge a fee* and to delete the last sentence.

(b) **(…)**

~~**(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Directive;**~~

(d) to order the controller or processor to bring processing operations into compliance with the provisions adopted pursuant to this Directive, where appropriate, in a specified manner and within a specified period; in particular by ordering the rectification, restriction or erasure of data pursuant to Article 15;

(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.**~~

(1b) Each Member State shall provide by law that its supervisory authority shall have the ~~**following**~~ (…) advisory powers:

~~**(a)**~~ to advise the controller in accordance with the prior consultation procedure referred to in Article 26; **and**

~~**(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;

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.

(b) **(…)**

(c) **(…)**

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

Article 47

Activities report

Member States shall provide that each supervisory authority draws up an annual[246] report on 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.

[246] DE wanted the reports to be done every second year.

CHAPTER VII

CO-OPERATION

Article 48

Mutual assistance[247]

1. Member States shall provide that supervisory authorities provide each other with mutual assistance in order to implement and apply the provisions adopted pursuant to this Directive (…) 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 (…) inspections and investigations.

2. Member States shall provide that a supervisory authority takes all appropriate measures required to reply to the request of another supervisory authority without undue delay and no later than one month after having received the request. ~~**Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.**~~

~~**2a.**~~[248] ~~**Member States shall provide that the request for assistance shall contain all the necessary information, 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.**~~

2b.[249] Member States shall provide that a supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless:

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

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

---

247 SI reservation. DE and FR scrutiny reservation.

248 NL scrutiny reservation

249 NL scrutiny reservation

3. 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 2b, it shall explain its reasons for refusing the request.

3a. Supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means. **~~, using a standardised format.~~**

3b. 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.

3c.[250] 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 3a. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2).

250 NL scrutiny reservation

Article 49

Tasks of the European Data Protection Board

1. The European Data Protection Board established by Regulation (EU)…./ XXX exercise the following tasks in relation to processing within the scope of this Directive:

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

(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 the provisions adopted pursuant to this Directive and issue guidelines, recommendations and best practices (…) in order to encourage consistent application of those provisions;

(ba) draw up guidelines for supervisory authorities concerning the application of measures referred to in paragraph 1, 1b and 1c of Article 46;

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

(d) give the Commission an opinion on the level of protection in third countries or international organisations;

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

(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.

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 57(1) and make them public.
4. The Commission shall inform the European Data Protection Board of the action it has taken following opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.

CHAPTER VIII

REMEDIES, LIABILITY AND SANCTIONS

Article 50

Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, Member States shall provide that every data subject shall have the right to lodge a complaint with a single **(...)** supervisory authority, **~~in particular~~ namely** in the Member State of his or her habitual residence, **~~place of work~~** or place of the alleged infringement **(…)**(…) if the data subject considers that the processing of personal data relating to him or her does not comply with provisions adopted pursuant to this Directive.

1a. Member States shall provide that if the complaint is not lodged with the supervisory authority that is competent pursuant to Article 44 (1), the supervisory authority to which the complaint has been lodged shall transmit it to the competent supervisory authority.

1b. Member States shall provide that the supervisory authority with which the complaint has been lodged provides further assistance upon the request of the data subject.

2. **(…)**[251]

2a. **~~The competent supervisory authority~~ ~~with which the complaint has been lodged shall inform the complainanton the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article~~ ~~51.~~ The data subject shall be informed on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 51.**

3. (…) [252]

[251] Moved to Article 53(1).
[252] Moved to Article 53(2).

Article 51

Right to an effective judicial remedy against a supervisory authority

1. Without prejudice to any other administrative or non-judicial remedy, Member States shall provide for the right of a natural or legal person to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them**.**

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority competent in accordance with Article 44 **(1)** does not deal with the complaint [253](…) or does not inform the data subject within three months or any shorter period provided under Union or Member States law on the progress or outcome of the complaint lodged under Article 50.

3. Member States shall provide that proceedings against a supervisory authority shall be brought before the courts[254] of the Member State where the supervisory authority is established.

Article 52

Right to an effective judicial remedy against a controller or processor[255]

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority under Article 50, Member States shall provide for the right of data subjects to an effective judicial remedy if they consider that their rights laid down in provisions adopted pursuant to this Directive have been infringed as a result of the processing of their personal data in non-compliance with these provisions.

---

253 SE meant that according to the subsidiarity principle it was not possible to introduce a right to judicial remedy when a SA has failed to act, since this would mean a harmonisation of MS procedural rights, paragraph 2 should therefore be deleted or redrafted or that it be explained in recital 60.

254 SE suggested to put a full stop after *courts.*

255 UK said that in the UK after the lodging of a complaint to the SA the SA would look at the complaint once more, *i.e.* not a court of law and that it seemed as if the Article tried to harmonise the MS administrative procedures which was problematic. AT indicated, as it had done when the GDPR had been discussed, that the AT Constitution did not allow for parallel proceedings which the Article seemed to provide for.

Article 53

(...)Representation of data subjects[256]

1. **Member States shall provide that the** data subject shall have the right to mandate a body, organisation or association, *which has been properly constituted according to the law of a Member State and whose statutory objectives include the protection of data subjects' rights and freedoms with regard to the protection of their personal data, to lodge the complaint on his or her behalf* and to exercise the rights referred to in Articles 50, 51 and 52 on his or her behalf.[257]

~~**2. Member States may provide that any body, organisation or association referred to in paragraph 1, independently of a data subject's mandate (…), shall have in such Member State the right to lodge a complaint with the supervisory authority competent in accordance with Article 50 and to exercise the rights referred to in Articles 50, 51 and 52 it considers that the rights of a data subject have been infringed as a result of the processing of personal data that is not in compliance with the provisions adopted pursuant to this Directive.**~~[258]

3. (…)

Article 54

(…)Right to compensation and liability

1. Member States shall provide that any person who has suffered ~~**material or immaterial**~~ damage as a result of (…) a processing operation which is not in compliance with the provisions adopted pursuant to this Directive shall have the right to receive compensation from the controller or the processor for the damage suffered. [259]

---

256 PT wanted to delete the whole Article.

257 AT asked that it be clarified in a recital that this paragraph did not run counter the AT obligation to be represented by a lawyer in higher courts in AT.

258 Deleted at the request of BG, CZ, EL, ES, FI, FR, IE, LT, SI and UK. In contrast AT was positive to this right.

259 FI, supported by AT, IE, IT and CH, preferred the text of DPFD "or other competent authorities in the MS". EL meant that something was missing in the paragraph, namely *an illegal act* and referred to Article 14 Eurodac Regulation.

2. **(…)** Any controller **(…)** involved in the processing shall be liable for the damage caused by the processing which is not in compliance with the provisions adopted pursuant to this Directive,**(…).** A processor shall be liable for (…) the damage caused by the processing only where it has not complied with obligations in the provisions adopted pursuant to this Directive specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. ~~**A controller or the processor shall be exempted from liability in accordance with paragraph 2, (…) if (…) it proves that it is not in any way responsible (…), for the event giving rise to the damage**~~.

4. ~~***Where more than one controller or processor* or a controller and a processor are *involved in the same processing* and, where they are, in accordance with paragraphs 2 and 3, responsible for any damage caused by the processing, (…) each controller or processor shall be held (…) liable for the entire damage.**~~

~~**5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage in accordance with the conditions set out in paragraph 2.**~~

Article 55

Penalties[260]

Member States shall lay down the rules on penalties, applicable to infringements of the provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive. **[261]**

260 DE, ES, RO scrutiny reservation on Article 54, RO in relation to *national law*. CH, and EE reservation. Cion stated that Article 55 existed in the Regulation as well and was a standard provision.

261 FI preferred the text of DPFD.

CHAPTER IX

(…) IMPLEMENTING ACTS

Article 56

Exercise of the delegation

(…)[262]

Article 57

Committee procedure

1. The Commission shall be assisted by the committee established by Article 87 of Regulation (EU) XXX. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.
3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

[262] Cion scrutiny reservation against deletion.

CHAPTER X
FINAL PROVISIONS

Article 58

Repeals

1. Council Framework Decision 2008/977/JHA is repealed **with effect from the date referred to in Article 62(1).**
2. References to the repealed Framework Decision referred to in paragraph 1 shall be construed as references to this Directive.

Article 59

Relationship with previously adopted acts of the Union for judicial co-operation in criminal matters and police co-operation

The specific provisions for the protection of personal data in acts of the Union adopted in the field of judicial co-operation in criminal matters and police co-operation **(…)** adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive remain unaffected. [263]

[263] DE scrutiny reservation.

Article 60

Relationship with previously concluded international agreements in the field of judicial co-operation in criminal matters and police co-operation[264]

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to the entry into force of this Directive and which are in compliance with Union law applicable prior to the entry into force of this Directive shall remain [265]~~**in force until amended, replaced or revoked**~~ **unaffected. To the extent that such agreements are not compatible with Union law, Member States are required to take all appropriate steps to eliminate any incompatibilities.**

---

264 Cion reservation. CH, SK and DE scrutiny reservations. For the UK and CZ Article 60 as it was drafted here was unacceptable. SI said that DPFD was more acceptable and that the text contained no element of flexibility.

AT meant that the aim should still be to adapt as soon as possible agreements that do not conform to the provisions of the Directive. AT suggested that intermediate solutions be set out in a recital.

265 DE suggested to reword Article 60 as follows: "International agreements involving the transfer of personal data processed by competent authorities for the purposes referred to in Article 1(1) to third countries or international organisations which were concluded by Member States prior to the entry into force of this Directive shall remain unaffected. To the extent that such agreements concluded by Member States are not compatible with this Directive, the Member State or States concerned shall make appropriate efforts to eliminate the incompatibilities established." DE aligned the first sentence to Article 59 and clarified that existing agreements did not need to be renegotiated. SI could accept reverting to Article 26 in DPFD or the DE suggestion. BE and CZ supported "unaffected." ES, PL supported the deletion of the second sentence of the Article.

Article 61

Evaluation

1. The Commission shall evaluate the application of this Directive.

2. The Commission shall review within five years after the entry into force of this Directive other acts adopted by the European Union which regulate the processing of personal data **by the competent authorities** for the purposes set out in Article 1 (1) including those acts adopted by the Union referred to in Article 59, in order to assess the need to align them with this Directive and make, where appropriate, the necessary proposals to amend these acts to ensure a consistent approach on the protection of personal data within the scope of this Directive. [266]

3. The Commission shall submit reports on the evaluation and review of this Directive pursuant to paragraph 1 to the European Parliament and the Council at regular intervals. The first reports shall be submitted no later than four years after the entry into force of this Directive. Subsequent reports shall be submitted every four years thereafter. The Commission shall submit, if necessary, appropriate proposals with a view of amending this Directive and aligning other legal instruments. The report shall be made public.

[266] DE wanted to add a sentence in the end of paragraph 2 to clarify that the same minimum standards must apply to the EU bodies as to the Member States: "The Commissions proposals shall ensure that the data protection provisions applicable to institutions, bodies, offices and agencies of the European Union within the scope of Article 1(1) at least correspond to the standard set by this Directive."

Article 62

Implementation

1. Member States shall adopt and publish, by [date/ two years[267] after entry into force] at the latest, the laws, regulations and administrative provisions[268] necessary to comply with this Directive. They shall forthwith notify to the Commission the text of those provisions. They shall apply those provisions from xx.xx.201x [date/ two[269] years after entry into force].

   When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 63

Entry into force ~~and application~~

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

Article 64

Addressees

This Directive is addressed to the Member States.

---

267 For DE, ES, FI, NL, CZ, SK, RO and SE two years was too short. CZ, DE and RO preferred three or four years, BE five years and FR three years.

268 BE and AT asked an explanation of what was meant with *regulations and administrative provisions.*

269 DE, NL, SI, IT, DK, FI wanted that the provisions be applicable four years after the entry into force.