Council of the European Union

Brussels, 24 June 2015
(OR. en)

10133/15

Interinstitutional File:
2012/0010 (COD)

LIMITE

DATAPROTECT 106
JAI 487
DAPIX 110
FREMP 141
COMIX 294
CODEC 906

NOTE

From:	Presidency
To:	Working Group on Information Exchange and Data Protectrion (DAPIX)
No. prev. doc.:	7740/15
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 - Chapters I, II and V

In view of the DAPIX meeting on 2-3 July 2015 delegations will find attached Chapters I, II and V of the draft Directive as modified in light of the general approach on the draft General Data Protection Regulation agreed on 15 June 2015, as well as the related recitals.

To facilitate the reading of the document a note with questions relating to these chapters drawn up by the incoming Presidency will be issued.

All changes made to the original Commission proposal are underlined text, or, where text has been deleted, indicated by (…). Where existing text has been moved, this text is indicated in *italics*. The most recent changes are marked in **bold underlining** or where text has been deleted in ~~strikethrough~~. When text has been reverted to the Commission proposal such text is marked in **bold**.

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],

Acting in accordance with the ordinary legislative procedure,

---

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

2 OJ C… , p.

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.

(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]

---

3 OJ L 281, 23.11.1995, p. 31.

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.

(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 …../2012 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.

(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 bod**y**/entit**y** 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. ES found that the recital neither defined nor clarified what was meant with *bodies/entities.* SE found the text in particular the last sentence very prescriptive. **NL and HU supported the recital.**

(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 accident is a criminal offence or not. These can also include the exercise of authority by takin coercive measures[9] such as police activities at demonstrations, major sporting events[10] and riots. [11]

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[12] to safeguard against and prevent threats to public security,[13] 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 of agencies or units dealing with national security issues should not be considered as (…) activities falling under the scope of this Directive.

---

9 **CZ noted that 'coercive measures were not defined in EU law.**

10 Cion feared that activities normally carried out by administrative authorities such as in the area of food safety where authorities controlled if food was poisonous, thereby constituting a criminal offence, would be covered by the Directive and not the Regulation, a situation that would be unacceptable for the Cion.

11 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.'

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

13 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[14].

(13) This Directive allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Directive.

(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**, mechanisms or procedures** 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.

14 RO meant that recital 12 would entail multiple negative consequences for the implementation and wanted police work and domestic processing out of the scope of the Directive. FI scrutiny reservation.

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, such as ~~an~~ activit~~yies~~ concerning national security, ~~**taking into account Articles 3 and 6 of the Treaty on the Functioning of the European Union**~~, nor[15] ~~**data processed by the Union institutions, bodies, offices and agencies, such as Europol or Eurojust**~~ **does it cover** ~~**to**~~ **the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.**

(15a) Regulation (EC) No 45/2001[16] 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 EU …../**XXX**~~**2012.**~~

(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 ~~during~~ **in relation to**[17] criminal proceedings. [18]

---

15 BE asked what would happen with data generated from national security and the police sector, under what regime they would fall. UK meant that the part on national security should be inserted into the body of the text.

16 OJ L 8, 12.1.2001, p. 1.

17 **AT suggestion, supported by IE and SE.**

18 BE reservation of substance and SE scrutiny reservation. IE welcomed recital 15b and wanted the text, in particular the part relating to the independence of the judges to be put into the body of the text. Cion also welcomed the recital on courts.

(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.
19

(16a) Genetic data should be defined as personal data relating to the genetic characteristics of an individual which have been inherited or acquired ~~**as they result from an analysis of a biological sample from the individual in question**~~ **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.[20]

---

19 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.

20 SE expressed concerns with recital 16a because of DNA profiles **used by law enforcement authorities** with the purpose of identifying should **be considered to be 'identifiers' but not as giving any information about an individual's physiology or health.**

(17) Personal data relating to health should include **~~in particular~~** (…) 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 ~~any~~ 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.

(18) Any processing of personal data must be (…) lawful and fair in relation to the individuals concerned, for specific purposes laid down by law.[21] **Individuals should be made aware on risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise his or her rights in relation to the processing. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate and relevant (…) for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. (…). Personal data should only be processed if the purpose of the processing could not reasonably be fulfilled by other means. 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.**

(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[22] 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.

---

21 ES suggested to delete the second sentence since data can be collected for numerous reasons and serve a number of purposes. FR preferred the previous drafting of recital 18.

22 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.

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 not be processed for purposes incompatible with the purpose for which it was collected. In general, further processing for archiving purposes in the public interest or[23] scientific, statistical or historical purposes should not be considered as incompatible with the original purpose of processing. Personal data should be adequate, relevant and not excessive for the purposes for which the personal data are processed. (…). ~~**Personal data which are inaccurate should be rectified or erased**~~. [24]**Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted.**

(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* ~~***public***~~ *authorities (…) should, as far as possible*[25]*, 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.*[26] 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.

---

23 SE, supported by FI, suggested to add a reference to archiving purposes in the public interest.

24 ES, **supported by SE,** suggested removing the last sentence of recital 20. ES meant that requiring that inaccurate data be rectified or erased would make police work ineffective and inefficient since police work consist in receiving and analysing false or incomplete data. SE supported ES and pointed out that the purpose of court proceedings in criminal matters was to establish what is true and false and that judgements cannot be corrected. **SE added that registers could be corrected but not the archives.**

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

26 DE scrutiny reservation on the addition of the new text. BE asked why this text had been added when Article 5 had been deleted. The Chair explained that the principle of accuracy is maintained in the text and that the added text was a reminder thereof.

(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) (…).[27]

(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 quality and reliability of the information processed by the competent (…) authorities. [28]

[27] Deleted since Article 5 was deleted. ES, DK and SE suggested deleting recital 23 since Article 5 was deleted. 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.

[28] UK suggested to delete Article 6 as well as recital 24.

(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. Processing by a competent (…) authority should also be lawful, where the processing is necessary or in order to protect the vital interests of the data subject or of another person, or for the **safeguarding against and the** prevention of ~~**an immediate**~~[29] ~~**and serious**~~ threat**s** to public security[30]. 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)**[31] 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 for example 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**.**[32]

---

29 ES suggested to replace "immediate" because this word is often misinterpreted and replace it with "direct".

30 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." CH considered that excluding *consent* as a legal basis for processing would be an excessive formalism. **CZ said that consent given to the police would not constitute a legal ground for processing because it was not freely given. However, CZ meant that a freely given consent would be exceptional in the framework of the Directive but meant that as regards human trafficking, stalking or a parent on behalf of its child the consent should be taken into consideration.**

31 BE said that consent was sometimes used as a legal basis, *e.g.* in SIS.

32 PT, supported by HU, meant that it was necessary to distinguish between two different kinds of consent, one when consent was required and another when it was not required. DE meant that recital 25 created important problems for the practical work and that it was therefore necessary to clarify this in the body of the text, *e.g.* the situations when consent constituted a legal ground should be set out. UK meant that processing could be legitimate even when consent was missing, *i.d.* consent was not always required. Cion considered that consent could only be used in the context of a law but could not be called consent but something else as operated as an additional safeguard. Cion wanted this to be clearly framed.

(25a) Member States should provide that where[33] Union law or the national law applicable to the transmitting competent (…) authority provides for[34] specific conditions applicable in specific circumstances to the processing of personal data,[35] 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 inform the data subject in case of a limitation to the right of information without the prior approval of the transmitting 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 conditions pursuant to paragraph 1[36] 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.[37]

[33] BE wanted to replace *where* with *when* (as in Article 7.3 suggested by BE).
[34] BE suggested to delete *for*.
[35] BE suggested to add the following text: these conditions are set out in accordance with the Europol handling codes. The Transmitting ...” (as in Article 7.3 suggested by BE).
[36] CH wanted to replace "paragraph 1" with "the first sentence".
[37] CH suggestion.

(26) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights (…) and freedoms, ~~**including genetic data**~~, deserve specific protection **as the context of their processing may create important risks for the fundamental rights and freedoms**. The**se**~~**is**~~ **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 **allowed in** specifical~~**ly**~~ **cases** authorised by a law which provides for (…) appropriate safeguards for the rights and freedoms of the data subjects; 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 is necessary for the prevention of an immediate[38] and serious threat to public security (…)..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 when the data subject has explicitly agreed in cases where the processing of data is particularly intrusive for the persons[39]**.** However, the agreement of the data subject should not provide in itself a legal ground for processing such sensitive personal data by competent **(…)** authorities. [40]

(27) ~~**Every**~~ **The** data subject should have the right not to be subject to a decision which is based solely on automated processing, including profiling ~~**(…),**~~ **which produces legal effects concerning him or her or significantly affects him or her** unless authorised by law and subject to appropriate safeguards for the rights and freedoms of the data subject (…).

---

38 ES suggested to replace "immediate" because this word is often misinterpreted and replace it with "direct".

39 HR wanted to include consent as a separate legal ground for processing.

40 SE meant that the last parts of recitals 25 and 26 were contradictory.

(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* as well as by the police or other law enforcement authorities for the purposes of **~~maintaining law and order and~~ 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.[41]

(46) The Commission 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.

(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.

[41] Since DE suggested to remove Article 33.1(c) it suggested to revise recital 45. DE wanted to remove the text restricting transfer only to public authorities because DE meant that it must be possible to make enquiries to companies for example.

(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**.** 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.

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[42] and serious threat to the public security of a Member State or a third country, or in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences *or the execution of criminal penalties* as well as for the purposes of the safeguarding against and the prevention of public security, or in individual cases for the establishment, exercise or defence of legal claims[43].

---

42 ES suggested to replace "immediate" because this word is often misinterpreted and replace it with "direct".

43 FR referred to judicial redress and meant that transfer to third countries could take place even if the right to judicial redress did not exist in the third country in question.

(49a) 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. [44]

(…)

[44] 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." CH considered that processing of personal data should also be lawful if the data subject has given his or her consent to the transfer of his or her personal data. FR wanted to stress that it was for MS to assess all factors that could constitute appropriate and the need to balance all the factors involved.

CHAPTER I
GENERAL PROVISIONS[45]

Article 1

Subject matter and objectives[46]

1. This Directive lays down the rules relating to the protection of individuals with regard to the processing of personal data[47] by competent[48] (…) authorities[49] for the purposes of the prevention**,** investigation[50], detection or prosecution of criminal offences *or the execution of criminal penalties*[51] or[52] the safeguarding against or the prevention of threats to public security.

[53]

---

45 PL, FI, UK scrutiny reservation on Chapter I.

46 DE deplored the fact that the DPFD's basic philosophy of minimum harmonisation combined with a prohibition on 'data protection dumping' had been lost in this text. Cion explained that this proposal did not seek to attain full harmonisation, but at the same time went beyond the minimum harmonisation of the DPFD. Several Member States (AT, DE, **HU,** NL and RO) stated that the exact nature of the harmonisation (minimum or maximum) the proposed Directive sought to attain was unclear. DE said that it was important that the existing procedural powers were not altered or restricted by data protection rules. DE was of the opinion that the Commission's presentation of the administrative burden was insufficient.

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

48 NL said that the police did not only investigate criminal offences, maintained public order, it also had jobs of administrative nature. NO said that private enterprises could be involved in this area, *e.g.* as processors. Cion said that the Directive was only applicable to competent (public) authorities carrying out activities listed in paragraph and where the same activities were carried out by a private enterprise the Regulation was applicable (see Article 21 and recital 16 in GDPR)this was in line with the Treaty.. The Cion indicated that the DPD was applicable to courts for criminal matters whereas for other courts the Regulation would be applicable.

49 FR suggested the insertion of "the Member States'" before "competent authorities". EL wanted further clarifications of "competent authorities" in order to ensure that investigators and prosecutors were included. Pointing to Article 2(2)(e) in GDPR, EE thought that many bodies would be outside the scope of both the GDPR and the Directive. IT further suggested that specific rules be set out to indicate that private entities (subcontractors, outsourcers, cloud providers and contractors) should be considered joint controllers.

50 NO meant that is was difficult to distinguish between police and criminal investigation in cross-border cases.

51 BE, DE, ES, FI, FR, PL and SE, queried whether this Directive would cover court proceedings (also valid for Article 3(14) and if so to what extent. The Chair explained that courts are covered and that recital 55 had been changed to make this explicit. ES did not want the Directive to cover court activities.

52 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'.

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.[54]

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

[53] FR, supported by FI, NL, NO, CZ and CY and with the acceptance of DE, suggested to replace *internal security* with *public security*. NO suggested to talk about *police tasks* or define the scope negatively so as to exclude administrative tasks. EE and CH did not find that the Directive should cover courts and judicial bodies. **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).**

[54] AT, CH, DE, DK, ES, NL, SE and UK suggestion. CZ supported that MS could provide higher safeguards. Cion welcomed the insertion of the paragraph as long as the free flow of data was not hampered.

(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.[55] [56] [57] [58] [59] [60]

[55] CZ and DE queried whether, *a contrario*, the respect for other existing rules could still limit the exchange of personal data. Reference was made, by way of examples, to the rules contained in the so-called Swedish Framework Decision. Cion stated these rules could still be applied. Cion also clarified that the proposed Directive would not affect Member States' competences to lay down rules regarding the collection of personal data for law enforcement purposes. DE wanted to know if this drafting meant that different levels of data protection can no longer be invoked as an acceptable argument for prohibiting or restricting the transfer of personal data to another MS. SE preferred to delete because it was contrary to the minimi principle in paragraph (1a) but if the paragraph had to stay SE suggested to insert the following text after *Union 'where such exchange is required by Union or national law'*. In contrast, EE saw no problems with paragraph 2.

[56] 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". SE meant that the balance between individuals' integrity and security needed to be ensured and that aspect was not yet sufficiently clear in the current text.

[57] IT and SI queried the interaction with other fundamental rights and referred to the need to protect attorney-client privilege. 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.

[58] DE sugg: p.10 in 14901/2/13 rev 2. Cion meant that new Article 7a covered this.

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

[60] 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 [61]

1. This Directive applies to the processing of personal data by competent (…) authorities[62] for the purposes referred to in Article 1(1).[63]

2. This Directive applies to the processing of personal data wholly or partly by automated means[64], 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.[65]

---

61 BE, CZ, DK, AT, ES, UK considered that the delimitation of the scope of this Directive and the one of the GDPR was not sufficiently clear (*e.g.* when the police is using the same personal data in different situations). UK wanted that the scope be limited to personal data that are or have been transmitted or been made available between MS. EE scrutiny reservation.

62 **DE said that the police, customs and law enforcement authorities should be covered and FR meant that authorities dealing with asylum and immigration should be covered by the GDPR.**

63 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. It requested a thorough analysis of ". CZ pointed to Declaration 21 annexed to the Lisbon Treaty setting out that specific rules may be necessary for the protection of personal data in the fields of judicial cooperation and police cooperation and concluded that national processing of such data should not be covered by the Directive. DE said that data may need to be transmitted for other reasons, *e.g.* a school needed to be informed about young offenders, asylum or data may need to be passed on to concerned persons.

64 HU considered that the distinction of data processing by automated means and other means seemed to run counter to the goal of a consistent data protection legislative framework. 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,".

65 DE scrutiny reservation. DE queried whether files as well as (electronic) notes and drafts are covered by the scope of the Directive. DE considered that if the scope covers all three forms, exceptions are necessary not to overburden the authorities.

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 (…);

~~(aa) in the course of an activity which falls within the scope of Regulation No 1987/2006 (SIS II), Regulation No 767/2008 (VIS) or Regulation No 603/2013 (Eurodac), unless the processing is carried out in application of Regulation No 603/2013 by designated or verifying authorities of the Member States for the purposes of the prevention, detection or investigation of terrorist offences or other serious criminal offences~~.

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

66

66 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. For ES it was important that MS remain competent to legislate on the protection of personal data in matters that could affect national security or impinge on it in some way. If such competence was not set out in the Directive 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. DE pointed to the RO text referring to its suggestion for Article 2.1 in GDPR "and for the purposes of maintaining and assuring the public order" (doc 8208/13).

Article 3

Definitions[67]

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[68], in particular by reference to an identifier such as a name, an identification number, location data, online identifier[69] or to one or more factors specific to the physical, physiological, genetic[70], mental[71], economic, cultural or social identity of that person.[72];

(…)

---

67 DE scrutiny reservation. EL, supported by DK, SE and UK, insisted on the need to ensure consistency between the definitions in this instrument and the GDPR, for IT uniformity of application was also important. FI and HU wanted to review the definitions once they had been more formalised in GDPR. ES meant that some positive progress had been made to align this instrument with GDPR but that *e.g.* controllers was particular for the Directive. Cion also welcomed the alignment with the GDPR. 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.

68 DE wanted to reinsert the reference to "by means reasonably likely to be used" as set out in the Cion proposal should be reinserted into the body of the text. DE asked who should be able to identify the person. FR suggested inserting the following: "If identification requires a disproportionate amount of time, effort or material resources the natural living person shall not be considered identifiable".

69 FI and EE requested clarification of this concept and though that it should be complemented by the words "on the basis of which the data subject can be identified". UK queried whether the proposed definition would prevent law enforcement authorities from releasing personal data from unidentified suspects.

70 FR reservation.

71 FR and RO wanted to know what *mental* meant.

72 FR thought the definition from the 1995 Directive was better. SE queried whether the following data should be listed here: genetic, cultural or social identity of that person. UK thought the definition was not sufficiently technology-neutral. FI suggested to align this definition to the one in the GDPR.

(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[73];

(4) 'restriction of processing' means the marking[74] of stored personal data with the aim of limiting their processing in the future; [75]

(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; [76]

---

[73] DE wanted to add "blocking" instead of restriction.

[74] CH and FR said that the texts uses the word *restriction of processing* but in reality it was about *blocking* and that should be made clear in the text. CH, DE, EE, HU, NO, NL and SI preferred the word *blocking* as is used in DPFD.

[75] RO asked for clarifications on the meaning of *restriction. C*ion explained it thought this term was less ambiguous than the term 'blocking', which is used in the DPFD. DE and SE did not see the need for a new definition. Alternatively, SE and CZ suggested to define the term "marking" instead of "restriction of processing". CZ reservation. DK found the definition unclear. SE wanted to delete "in the future" because the limitation applies from the outset. FR found the definition superfluous and wanted to delete the whole definition

[76] DE, HR and RO wanted to know whether paper-based criminal files (assembled by the police and or courts) were included in the definition. AT meant that it should be clear under which circumstances file in paper format fall under the Directive and referred to recital 15 in DPD.

(6) 'controller' means the competent (…) authority, which alone or jointly with others determines the purposes (…) and means[77] 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[78];

(7) 'processor' means a natural or legal person, **public** authority, agency or any other body which processes personal data on behalf of the controller[79];

[77] Cion considered that the references to *purpose* and *means* was the appropriate solution and ensured consistency with GDPR.

[78] UK though that the distinction between processor and controller was blurred here. ES pointed out that if private sector bodies are included in the scope of the Directive this will impact the definitions of *controller* and *processor*. Cion said that processing would be set out by law and that judges and prosecutors were not controllers because they were bound by the procedure law. SI asked if the prosecutors office was the controller since the individual prosecutor was not a controller. Following up on that, DE while pointing to Articles 11, 12, 15 and 16 which related to controllers required a clarification as to who would carry out these tasks. Cion suggested to clarify that in a recital. CY meant that the definition was moving in the right direction.

[79] PL scrutiny reservation. PL queried what this definition implied for transfers of personal data from the private to the public sector.

(8) 'recipient' means a natural[80] or legal person, public authority, agency or any other body **~~other than the data subject, the controller or the processor,~~** to which the personal data are disclosed[81], **whether a third party or not**;

82

(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;

---

80 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.

81 FR thought this definition was too broad as it would also cover data protection authorities. FR also suggested to include *third parties to whom data are disclosed* as in the definition of recipient in the 95 Directive. 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". In 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".

82 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. The Chair said that since consent was no legal ground for processing it was not necessary to have a defintion of consent. 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. **BE thought that consent could be useful *e.g.* in situations when individuals contact the police to look out for burglars.**

(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 (…) evaluat**e** personal aspects relating to an ~~**individual**~~ **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**;

(…)

[83]

(14) 'competent[84] (…) 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 [85] or any body/entity[86] entrusted by national law[87] to perform public duties or exercise public powers for the **purposes referred to in Article 1(1). ~~purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.~~** [88]

---

[83] 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.**

[84] DE scrutiny reservation.

[85] PL remarked that courts were excluded from this definition. PT thought this definition served little purpose. DK queried whether *e.g.* surveillance authorities were covered by this definition. FI stressed that courts were not covered by this definition. EE said that it had the same concerns as indicated for Article 1.1 and, supported by DE, that, in addition, paragraph 14 did not follow the same logics as in Article 1.1. CZ said that the whole definition was different and that the Directive should be applied to ordinary courts. IE and IT expressed concerns about this paragraph. Cion said that courts and prosecutors should be covered by the Directive.

[86] Cion scrutiny reservation, linked to the authorities being covered by the definition. UK meant that since the definition – extension to other than public authorities- was linked to *public security* in Article 1.1 it was necessary to deal with the two in parallel. FI meant that it was important to separate between on the one hand delegation of tasks by the police and law enforcement authorities to other operators that can be done by delegated laws or special legislation (*e.g.* guarding of prisons to private parties) and on the other hand private actors that cooperate with the police by providing information. FI feared that a grey zone would be created with this definition.

[87] UK, supported by CZ **and IE**, 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.

[88] **UK favoured that private bodies were covered but only under certain circumstances, also in contractual relationships. In the UK creating DNA samples (on scenes of crime and in police custody) was outsourced to private entities. BE was favourable to extend the scope to private bodies and gave the example that road security in BE was carried out be private bodies that collected personal data that they subsequently forwarded to the federal police.**

89

89 DE, RO and SK declared that they accepted the definition since it meant that the purpose of the processing was the relevant point. DE said that there was a difference between a body that helped the police and a body that worked as the police with sovereign powers state authority with powers to use force) then should the Directive be used. BE reservation on private bodies maintaining public order (public security). FI joined BE and did not see a need to extend the scope to private entities. FI , NL and PT scrutiny reservation. Also IE shared BE/FI hesitation to extend the scope to private bodies. IE cautioned against difficulties such an extension and provided an example of an auctioneer who for money laundering reasons was obliged to report to the police in certain cases, this could lead to private bodies being obliged to comply with both the Directive and the GDPR. IE also pointed at recital 16 pf GDPR. IE waiting reservation. CZ thought that no MS would apply the Directive to *e*.g. banks only because they were obliged to report on potential crimes. EE preferred not including private bodies. EE explained that tasks such as airport security and surveillance of football matches had been delegated to private bodies in contracts but these bodies did not carry out public tasks but were placed under the police. EE asked about the large scale implication of such extension. In contrast HU and AT were content to allow for outsourcing to private bodies, HU mentioned such as airport security, transfer of prisoners and surveillance of football matches. For HU the question was if it was necessary to set out minimum rules for contracts with private bodies or allow for MS to decide. In AT certain core tasks of the police could never be outsourced to private bodies. ES asked in what capacity the private bodies would intervene. For ES it was necessary to know if the processing initially was destined for different authorities. PT said that what should trigger the application of the Directive should be the carrying out of a professional activity. For NL it was important that different bodies could cooperate, also administrative bodies *e.g.* tax authorities. BE asked what would happen if a private body processed personal data for a commercial purpose and then that data was used for police purposes, what instrument would be applicable. BE set out another example, a private body that was mandated by the police to process personal data, then the Directive would be applicable from the outset. Following up on that BE suggested to expand on this in the recitals to clarify such issues. The Chair said that it would be necessary to delimit cases where a private body had an obligation to cooperate with the police and the cases where a private body carried out tasks instead of the police. Cion retorted that the GDPR provided a solution to the private bodies, in Article 6.3 and Article 21 in private interest" "compliance with a legal obligation". FD says "established by national law", "established with specific tasks" = GDPR. Cion agreed with IE on the risk of a double regime for certain bodies such as the auctioneer, money laundering and forensic laboratories. Cion noted that another solution could be to have a processor. FI scrutiny reservation.

(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.

90

91

90 CH suggested to add a definition of consent in line with the drafting in Article 4.8 in the GDPR: " 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;" (doc 6828/13) 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". (8916/12) IT opposed the insertion of consent because it meant that consent cannot be the legal basis for processing in the field covered by the Directive.

91 Cion and FI thought that it might be needed to insert a definition on *pseudonymisation* for the sake of investigations.

CHAPTER II [92]

PRINCIPLES

Article 4

***Principles relating to personal data processing*[93]**

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

(a) processed lawfully *and fairly*;[94]

[92] FI, PL, SI, UK scrutiny reservation on Chapter II.

[93] PL scrutiny reservation. AT and DE deplored the apparent absence of the requirement of data minimization. DE thought that a number of important requirements from the DPFD, e.g. the requirement that the data must be processed by competent authorities, purpose limitation, are lost in the proposed Directive. DE further stated that provisions on archiving, setting time limits for erasure and review are missing. SE queried why Article 3(2) DPFD had not been incorporated here. Cion affirmed that it did not intend to lower the level of data protection provided for under the DPFD. EL considered that the same requirements as in Article 5 of the GDPR should be set out. UK considered that the draft Directive should be a minimum standards Directive and in consequence wanted to retain the wording in Article 3 of the DPFD. CH also preferred Article 3.2 of DPFD and AT preferred the text as proposed by Cion. NL and SE suggested to merge Article 4 and 7.

[94] 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*. DE and HR opposed to the reinsertion of *fairly*. IE, supported by SI, saw problems in reinserting *fairly* and pointed to covert police investigations that would not be possible then. SI meant that future proceedings would be influenced and meant that *fairly* had nothing to do in Article 4. CY asked whether it was feasible to ensure fairness. HR meant that *fairly* was inherent to the criminal procedure as a whole so it did not give any added value to the text. HR thought that in the case of transfer of inaccurate or illegal data the person should be notified and inaccurate data deleted or its dissemination ceased. FR and NL and Cion on the other hand welcomed *fairly* and FR saw no problems with police activities if the term was reinserted.

(b) collected for specified, explicit and legitimate purposes and only processed in a way (…) compatible with those purposes[95];

(c) adequate, relevant, and not excessive in relation to the purposes for which they are processed[96];

(d) accurate and, **where necessary~~(…)~~**[97], kept up to date; (…)[98]

(e) kept in a form which permits identification of data subjects[99] for no longer than is necessary for the purposes for which the personal data are processed;[100];

---

95 It was not clear for DE and SE how Articles 4 and 7 were linked, in particular as regards *purpose limitation.* NL meant that the *further processing* was not resolved here. For DE the purpose was for the MS to decide and consequently if another purpose was compatible with the initial one.

96 DE thought the DPFD was clearer. PT also queried about the use of personal data for other purposes.

97 **Reinserted at CZ, DE, DK, ES, IE, HU and UK request and in line with the GDPR. AT and EL supported the deletion.**

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

99 SE, supported by BE, 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.

100 DE queried about rules on archiving on judicial decisions. UK meant that this paragraph undermined future investigations. EE said that this paragraph was problematic for EE; how could personal data be deleted from data collected in criminal proceedings and when could data be archived? EE asked what point in time paragraph (e) referred to. EE meant that future identification was problematic. 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". CH suggested replacing (e) with the following text from Article 4(2) DPFD: "(e) erased or made anonymous when they are no longer required for the purposes for which they were lawfully collected or are lawfully further processed.; "IT wanted to link the period for which data can be kept with the objectives of the Directive and with the purposes for which the personal data was collected. BE suggested to add *or further processed* in the end of the paragraph.

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

(…)

~~1a Personal data shall be erased or made anonymous[101] when they are no longer required for the purposes for which they were lawfully collected or are lawfully further processed[102]. Archiving of those data in a separate data set for an appropriate period[103] in accordance with national law shall not be affected by this provision.~~[104]

[105]

[101] **DE asked what was meant with *made anonymous.* DE scrutiny reservation.**

[102] **NL wanted to delete *further processing.***

[103] **SE meant that the provisions on archiving were to be set out in the GDPR.**

[104] Inserted at the AT and CH request. **DE, IE and UK scrutiny reservation. DE said that archiving should be covered by the GDPR. For DE the question was whether further processing for other purposes should be covered by the GDPR or this Directive and suggested to discuss questions of scope and content horizontally. SE asked how this paragraph and paragraphs ((1)(e) and 3 of Article 4 were linked: they seemed to be duplications. FR doubted the added value of this paragraph: first sentence was redundant because of paragraph (1)(e) and the second sentence did not have its place in Article 4. FR and ES preferred to delete it. CZ found the paragraph superfluous: such paragraph did not exist in GDPR and the sentence on archives could be set out in a recital. Cion did not see any added value of paragraph 1a.**

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

2. Further processing by the same controller[106] for another purpose[107] shall[108] be permitted in so far as:

(a) it is (…) compatible[109] with the purposes for which the personal data was collected; and

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

---

106 **FR** preferred further processing to be prohibited instead of permitted. **FR wanted to delete *by the same controller.* In the same vein UK that said that it could be done not only by the controller but by a processor as well. NL said that the words *by the same controller* raised serious concerns; further processing was often carried out by another controller. IE found that *same controller* was too narrow.**
SE found that the paragraph was too narrow and wanted that *e.g.* the police should be able to inform social authorities of personal data processed by the police in a criminal investigation and which showed that a child was being mistreated (data sent from the police to the social authorities was covered by the Directive whereas the processing by the social authorities should fall under the GDPR).

107 DE and SE appreciated the introduction of text on processing for another purpose. **DE asked if the Directive could be applicable to purposes that were outside the scope of the Directive, and if that was the case it was necessary to discuss the notion of compatible purposes. SE found that it was too limiting if further processing only was allowed for compatible purposes.** DE asked what would happen with data that was processed by the police and then transmitted to a private body and the other way around for example in a case of mistreatment of a child and the police provides the school or social services with the personal data; DE noted that this did not only concern the Directive internally but also in relation to the GDPR. FI and SI supported DE and meant that it was important not to hamper police work and SI thought that information to social services and schools could be subsumed under the police's general tasks. FR supported DE and provided other examples such as transport licenses and election registers. Cion said that further processing across the two legal instruments would create problems and that there were no specific Articles to be used for that. Cion further stated that if a legal obligation to transfer data to the police existed, such transfer would be considered as the initial police processing. For the Cion the crucial point was that there were no gaps in the protection. The Cion said that if the purpose was outside the scope of the Directive the GDPR was applicable, see Article 6.4 that required a legal basis.
DE, supported by AT, FI, suggested that Article 11.2 from DPFD be introduced here (prior consent of the transmitting MS). Cion meant that Article 7(a) covered the situation in Article 11.2 DPFD. DE asked about when a different purpose occurred and suggested that once Article 6(4) of GDPR was agreed, this text should be inserted here.

108 SE meant that further processing is very linked to the national context and should therefore be decided by the MS and therefore suggested to change *shall* to *may.*

109 **CZ wanted to revert to the previous text, and the DPFD, to say *not incompatible.***

(c) processing is necessary and proportionate to that other purpose.[110]

3. *Member States may* [111] *provide that the* same controller[112] *may further process personal data for* archiving purposes in the public interest or [113]*for scientific, statistical or historical purposes*, subject to appropriate safeguards for the rights and freedoms of data subjects*.*[114]
115

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

116

117

110 NL asked about the links between paragraphs 1(b), 2 and Article 7. Cion said that it was necessary to have a legal basis for the further processing. AT could accept paragraph 2 and pointed at Article 11 last part that refers to *anonymous* data.

111 AT, CZ, CY, DE suggestion "shall" was changed to "may".

112 **UK meant that it was too restrictive to refer to the initial controller only. IE scrutiny reservation on *controller;* what controller was supposed to be covered.**

113 SE suggestion as well as for recital 20.

114 UK queried why processing for historical or scientific purposes was different regarding law enforcement from other investigations. CZ supported paragraph 3. DE asked about the relationship between this paragraph and paragraphs 1 and 2, if it was *lex specialis* or if they should be applied cumulatively. **CZ thought that paragraph 3 could be understood as not allowing MS to legislate for other purposes than those set out in paragraph 3. DE found it tricky to construct further processing for other purposes than set out in the Directive and the legal basis for archiving was set out in the GDPR and if the Directive could be used for archiving purposes.**

115 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.

116 DE**,** supported by AT, suggested to insert a new Article 4a (14901/2/13 REV 2). DE noted that data that had been blocked could not be erased. FI expressed a positive view on the DE text, except paragraphs 3(c) and 4 which needed to be further considered.

117 AT suggested to add a new Article 4a along the lines of Article 4a in the EP Resolution (7428/14).

Article 5

Distinction between different categories of data subjects[118]

(…)

Article 6

Verification of quality of data that are transmitted or made available[119]

1. Member States shall provide that the competent authorities shall take all reasonable steps to[120] 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[121] verify quality of personal data before they are transmitted or made available. As far as possible, in all transmissions of data, available information shall be added which enables the receiving competent authority to assess the degree of accuracy, completeness, up-to-datedness and reliability.[122]

---

118 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.

119 BE, CH, IE, RO, SI and UK questioned the added value of the Article. FR and UK said that Article 4(d) set out the same idea. BE and CZ suggested to delete the Article AT in contrast accepted the reinsertion of an Article with that heading. FI thought that an Article on accuracy was needed but was not certain that current Article 6 fulfilled that requirement. **DE saw problems with the lack of consistency with Article 4. CZ asked if cross-border cases were intended.**

120 Introduced at BE request, supported by **CZ,** DE, ES, FR, IE, SI, UK and CH. AT preferred former text.

121 IE suggestion.

122 DE, supported by ES, HR, RO, SE, UK, CH and NO, suggestion to insert parts of Article 8 DPFD.
FR meant that Article 6.1 and Article 4.1(d) were linked and should be dealt with at the same time.

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[123] or restricted in accordance with Article 15.[124]

[123] DE referred to its suggestion for an Article 4a after Article 4 and said that erasure could be made in a small remark.

[124] AT, ES, FI, FR, HU, RO, SE supported the text in 6.2. DE, while accepting to take over text from DPFD raised concerns over non-transmission of *inaccurate and incomplete* data. AT asked if the new text restricted the text.

Article 7[125]

Lawfulness of processing[126]

Member States shall provide that the processing of personal data is lawful[127] only if and to the extent that processing is necessary[128]:

[125] CH, DE and SI scrutiny reservation. DE considered it unacceptable that only the general lawfulness in Article 7 would apply to further processing of data previously transferred within the EU. In its opinion this would mean that data protection law aspects would take precedence over police and/or criminal procedural law. FI wanted to insert this Article after Article 4. ES said that since Article 3 did not define consent it was not clear why this was not addressed in this Article and pointed out that consent was important for alcohol tests for example. ES meant that a reference to consent would give added value to the Article and would provide an additional guarantee. AT, **CZ,** FR, HR, **HU,** UK and CH IE favoured the addition of consent. SI suggested to introduce a recital on consent. DK could consider it. IT and PT questioned the possibility of consent in the field of police work. Cion confirmed that consent was not relevant in the field covered by the draft Directive.CZ suggested to build in consent for processing, *e.g.* victims of stalking could consent to have phone calls tapped. FR meant that consent had to be treated with caution and did not want to have it as an autonomous legal basis for processing. BE meant that consent set out in a law would be acceptable. BE and FR reservation as regards consent. Cion questioned whether consent was necessary beyond what was set out in paragraphs (c) and (d) and stressed that consent should not be an individual ground for processing. Cion agreed that text on consent could be set out for example in a recital clarifying that in some cases consent could be a relevant factor.

[126] BE, DE and FR pointed to the difficulties to delimit the scope of the GDPR and this draft Directive. SE claimed that the Article was too restrictive. UK recommended to delete this Article since the minimum standards set out in the DPFD were both sufficient and appropriate for fundamental rights protection. DE said that it was impossible to agree to this Article until the exact scope of the Directive was decided. DE meant that it was necessary to explain how Article 7 and 4 were to be read, in particular the principle of purpose limitation. FR suggested to remove the Article due to a duplication with Article 4(1)(a). SI said that lawfulness was set out in Article 4 and was therefore dubious about the need of Article 7. FR meant that Articles 7 and 1.1 were contradictory and if the Article 7 had to stay it was necessary to clarify the links between the two Articles. DE meant that deleting Article 7 would not solve any problem and that Article 4 and 7 were linked. **HU suggested a new general discussion on Article 7.**

[127] IE questioned if lawful processing always was fair and wanted to add a new "recital/provision" setting this out.

[128] DK wanted to keep the scope broad enough for competent authorities' processing.

(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 (…)[129] [130] or

(b) (…)[131]

(c) in order to protect the vital interests[132] of the data subject or of another person[133]; ~~**or.**~~[134]

---

[129] DE, supported by RO, meant that is was difficult to attain the purpose of the Directive if the reference was made to national law which was correct since law for the police and criminal as well as criminal procedure law remain a national competence. DE also queried about what would happen to internal EU data processing.

[130] SE asked that the last part be deleted, as in article 4(1)(e)

[131] DE, FI, **IE,** SE and NO wished to reintroduce paragraph (b); for DE to read as follows: " for compliance with a legal obligation or for the lawful exercise of a legal power the controller is subject to". For DE for lawfulness for practical and legal reasons namely that data protection law must follow specialized law on the police and judiciary (which lies within the competence of the Member States) and not the reverse. In DE provisions for the transmission of information from the police or judiciary to other authorities are not set out in law so to cover such cases the reference to *legal power* is necessary. DE was considering whether a material restriction should be inserted in (b) which could be worded as follows: "The statutory provision must pursue an aim which is in the public interest or necessary to protect the rights and freedoms of third parties, must safeguard the essence of the right to the protection of personal data and must stand in appropriate relation to the legitimate purpose pursued by the processing."
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.**

[132] PL questioned whether economic or commercial interests were covered Cion indicated that only life or death situations were covered. SE queried about a definition of "vital" interests, in this Article as well as in Article 8.2 (b). HR suggested to replace *vital interest* with "life and physical integrity" of the data subject because HR meant that data should be processed also when it was necessary for the protection of the physical integrity of any person.

[133] DE scrutiny reservation. DE compared this Article with Article 1.2b of DPFD (protection of fundamental rights and freedoms of natural persons) and asked if Article 7 was the only restriction on MS when processing personal data. DE, supported by CH, also asked whether restrictions in national law would apply to the receiving MS when personal data was transferred/made available to them**.** DE considered it necessary to clarify whether this paragraph overlapped with paragraphs (a) and (b) and if that was the case paragraph (b) could be removed. DE said that if paragraph (b) and (c) were not overlapping it was necessary to determine if the Directive and/or Article 7.1 (c) was not too restrictive for a potential transmission to private parties. IT meant that paragraph (c) should be covered by paragraph (a) and should be attributed to the competence of the authority carrying out the processing.

[134] NL meant that paragraphs (a) and (c) needed revisiting.

135

~~**(d) for the prevention of an immediate and serious threat to public security.**~~

136

Article 7a

Specific processing conditions [137]

1. Member States shall provide that where Union law or the national law applicable to the transmitting competent (…) authority provides specific conditions[138] (...) to the processing of personal data,[139] the transmitting competent authority shall inform the recipient to whom the data are transmitted about such conditions and the requirement to respect them.

---

135 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.

136 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." DE, supported by HU, suggested the insertion of the following: "1a. In the cases referred to in paragraph 1 Member States may also provide that the processing of personal data is lawful if the data subject has consented to the processing." DE meant that Article 8.2 of the EU Charter sets out that personal data can be processed on the basis of consent and that consent-based data processing was essential in prevention projects such as taking blood or conducting DNA testing. DE meant that consent in these cases could be seen as alternatives to a court order.

137 CH, EE, NL, SK, PL, PT and SK scrutiny reservation. FR and SE reservation.DE wanted to delete Article 7a and said that it should be seen in connection with the addition of Article 1(2) (b). FR considered that the text was unclear and that it did not have its place among the Chapter on Principles. HR suggested to add that the data subject's consent could be a valid legal basis for the processing of their personal data. **NL asked about the purpose of the Article.**

138 DE wanted to know what *specific conditions* was.

139 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[140] pursuant to paragraph 1 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[141].

[142]

[140] FI and NL noted that the DPFD uses *restrictions* whereas here it was *conditions*, and therefore wanted to know if it was intended to cover something else.

[141] CH suggestion. to replace the last part of paragraph 2 with the following words. "similar national data transmissions".

[142] 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."

*2a. Member States may[143] set conditions in national legislation[144] for communication[145] of personal data between competent authorities pursuant to Article 1.1, the communication of personal data from a competent authority of a Member State to other public authorities of the same Member State and communication from the competent authority of a Member State to private parties of the same Member State.[146] **[147]***

143 DE suggestion.

144 UK commented that for common law countries the implementation would be difficult if the reference was only to national legislation.

145 **HU asked if *transfer* was meant rather than *communication.***

146 FI, IE and UK scrutiny reservation. HR questioned if paragraph (3a) was compatible with the subsidiarity principle. RO, AT, CH accepted paragraph (3a). NL asked about the links between paragraph (3a) and Article 7a(2) and, supported by UK, if paragraph (3a) had an added value. DE asked about the links between paragraph (3a) and Article 7(1)(a). The Chair explained that CoE Recommendation No. R (87) provides for communication of data and that MS had considered that such a provisions was missing in the Directive. DE meant that the paragraph was drafted too narrowly and noted that communication from a body under the Directive to a body covered by GDPR was excluded. FR **and ES** welcomed the paragraph: FR since it replied to its request in footnote to Article 3(8) on third parties. CZ meant that paragraph (3a) did not make sense especially at this place: paragraph 2 was enough. CZ said that the exchange in paragraph 3a only related to domestic exchange and that for the Victims Directive for example this could be problematic. CZ suggested to delete the paragraph and specify it in a recital. Cion stated that it had difficulties to accept the wording because it represented a lower level than the acquis. NO suggested reverting to Article 13 of DPFD. **NL found that even if paragraph 3a was optional it still created confusion. CZ did not see any added value and cautioned against limitations so as to tie the hands of law enforcement authorities. Cion feared that paragraph 3a would lower the level of protection compared with Article 14 in the DPFD.**
Cion agreed with NO that if the transmission took place between MS, the text of Article 14 in DPFD could be taken over.

147 **Moved from Article 4.**

Article 8[148]

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[149] or sex life[150] shall only be allowed[151] when strictly[152] necessary and

---

148 PL **and SI** scrutiny reservation on Article 8. UK generally preferred the drafting of the DPFD. SE pointed at discrepancies between the definitions in Article 3 on genetic data (and biometric data) and the text set out in Article 8. SE said that criminal science used results from analyses and that it was necessary to define methods for criminal investigation. SE said that law enforcement would be difficult if genetic data could not be used. SE added that distinguishing marks of a person could be covered by *sensitive data*. In conclusion, SE advocated a reviewing of Article 3 and 8 to make them balanced and consistent. Cion said that it was important to maintain the same level of protection as in Directive 1995 without lower the efficiency of the law enforcement authorities.

149 EE asked as an example if setting out that someone was drunk was acceptable or if it was considered as health data.

150 SE was of the opinion that many data was covered by paragraph 1 and that would make it difficult to legislate. PT wanted to reinsert the requirement of need, as in DPFD. PT said that what is sensitive data was not an absolute notion. HR thought that processing concerning health and sex life should be allowed because in cases related to crimes against sexual freedom such personal data would be collected regularly. RO wanted to add "biometric data" to the category with a special character. FR, supported by NL, said that the notions did not correspond to those set out in the 95 Directive, nor in the DPFD or the Charter and opposed the terms used. **DE meant that it was difficult to imagine sexual crimes or terrorism without looking at a person's sex life or religious belief./ were closely linked to sex crimes or terrorism. SI also found that a person's sexual behaviour was an integral part of a sexual criminal offence and that a person's religious belief was relevant for hate crime.**

151 SE and SI welcomed that the prohibition was replaced by a permission whereas AT and FR preferred the prohibition AT because it did not want to lower the level of protection. For FR a prohibition was a stronger protection for fundamental rights and was more in line with the EP position.

152 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." **SE supported FR on personal data supplementing other personal data whereas SI did not find the Eurojust solution satisfactory, nor did DE that did not see why it was better to process such data together with other data. AT said that further exceptions were necessary. DE mentioned that further exceptions for t he public sector were provided for in the GDPR; it seemed that the conditions were stricter in the Directive than in the GDPR; this text was in general difficult to understand. DE suggested to look at the EP text: Article 8(2) did not set out a general prohibition but special requirements for particular offences.**

(a) (…) ~~**the processing**~~ **is** authorised by Union law or Member State law which provides appropriate safeguards[153] for the rights and freedoms of the data subjects; **or**

(…)[154];

~~**In exceptional cases processing of such personal data as referred to in paragraph 1 may be carried out when:**~~

(**b**) ~~**the processing is necessary**~~ to protect the vital interests[155] of the data subject or of another person. ~~**or**~~

~~**(b) the processing (…) is necessary for the prevention of an immediate and serious threat to public security**~~.

156

---

153 AT, DE and NL required examples of safeguards and EE, HR, FR, IT, NL and RO asked for a clarification of what *safeguards* was. IT meant in this context that recital 26 could be modified to address this problem, suggesting text on procedural guarantees, technological or security safeguards.

154 SI and NL scrutiny reservation. CH considered the list of exceptions not sufficiently long, *e.g.* consent was missing. In contrast, PT considered that the list of exceptions was too long. CH also considered that Article 7(d) could be added to Article 8.2. DE considered it worth reflecting whether Article 8 could not be formulated as an anti-discrimination provision, like Article 21 of the EU Charter of Fundamental Rights. DK preferred the drafting of Article 6 in DPFD. Cion declared itself willing to reconsider the list of exemptions.

155 SE and SK required clarifications of the notion of "vital interests". CZ wanted to replace *vital* with *essential*. DE FR and SE meant that *vital interest* was too narrow. HR suggested to replace *vital interest* with "life and physical integrity" so that data would be processed also when it was necessary for the protection of the physical integrity of any person".

156 DE suggested to insert a paragraph (d) with the following wording: "(d) the data subject has consented to the processing". DE considered that the provision was too narrow, especially if the DE suggestion in paragraph 1 was not accepted. ES, supported by CH, DK, HU, IE and HR suggested to insert a paragraph with the following wording: "(d) the data subject has given his explicit consent". CZ suggested a new paragraph with the following wording: "data which the data subject has published him/herself or agreed to by the data subject." UK supported that processing would be acceptable if the data subject has consented or it had manifestly made public. BE suggested to insert a new paragraph with the following wording: "(d) the processing relates to data which are manifestly made public by the data subject." AT meant that points (a) and (b) did not cover all exceptions. Cion said that it would consider these suggestions.

Article 9

*(…)**Automated individual decision making**(…)*[157]

1. Member States shall provide that a decision based solely[158] **on automated processing, ~~on~~ including,** profiling**,** which produces an adverse legal effect[159] 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 (…).[160]

1a. Profiling shall not be based on special categories of personal data referred to in Article 8(1), unless Article 8(2) applies and appropriate safeguards for the rights and freedoms of the data subjects are in place.

---

157 RO suggested to move this Article to Chapter III. Scrutiny reservation FI, DE, ES, IT and SI

158 FR asked for the deletion of the word "solely".

159 EE asked who would assess the adverse legal effect and how.

160 **DE pointed to Article 7 in the DPFD and that it was without human intervention and wanted at least to add *by automated means.* UK supported DE and did not want to undermine what is core police work; if solely would be deleted this would cause serious concern. CZ also agreed with DE to use Article 7 of the DPFD. EL meant that the current text did not sit well with criminal law.**

CHAPTER V

TRANSFER[161] OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS[162]

[161] FR found it necessary to define *transfer*.

[162] AT, BE, CH, CZ, CY, DE, DK, EE, FI, FR, IT, NL, NO, PL, PT, RO, SI, SK and UK scrutiny reservation on Chapter V. DE and UK meant that it was difficult to have a clear view as long as the scope was not decided. ES and DE, FI reservation on Chapter V. DE questioned whether the core concept in Chapter V was appropriate. DE saw four main problems with Chapter V: (1) the structure of the Chapter including if main rules and exceptions were set out properly (2) lack of provisions for transfer to private bodies (3) what happens if the data are used for other purposes (4) general problems regarding third countries and the standing of consent. For DE it was important that data could be transferred for other purposes than prosecution of criminal offences. DE also asked how Chapter V was linked to Articles 4 and 7. On comment 4, Cion replied that the protection of personal data was a fundamental right but not an absolute right and that the derogations in Article 36 are derogations for the level of protection and not for the transfer itself. Cion replied that the provisions on transfer to private parties in DPFD only regulated transfers within the MS. Cion said that the main purpose was to protect personal data which might require the adducement of appropriate safeguards. As to point 2 of the DE comments, Cion asked why the police would want to send personal data to private parties in other MS. On point 3, Cion replied that for such a case the GDPR would be applicable. As regards consent the Cion reiterated that only *a freely given and informed* consent could constitute a legal basis for processing and that it was therefore not relevant in the law enforcement sector . DE, supported by FI, wanted it to be possible to transfer data to private bodies/entities, for cybercrime this was important. NL, SE and SI agreed with DE on the need for a solution on transfer to private parties in third countries. SE mentioned *e.g.* transfer of non sensitive data to parties who are affected by a case, such as convocations to meetings, hearings of witnesses or hearing of evidence in the individual case or sending an ip address to identify an account and last but not least information about sexual abuse of children and on foreign fighters. SE noted that the DPFD only covered cross-border data but that the Directive does cover domestic processing and that it should be possible to transfer data to private parties in third countries. Cion meant that in such cases requests for mutual assistance would be used and no direct contact would take place. As regards consent the SE stressed that administrative rules must not make transfer to third countries and international organisations more difficult. FI wanted that the content of Article 14 of DPFD (transmission to private parties in MS) should be covered in the future as well. FR and BE meant that it was necessary to link Chapter V and Article 60. BE said that its scrutiny reservation was linked to the uncertainty of the role and statute of international organisations in general and Interpol in particular. It was important for BE that the MS could continue to cooperate as they do now. For CZ swift and efficient international information exchange was an important precondition for the protection of fundamental rights by preventing and combating crime. ES raised concernes about the competences assumed by the Commssion in this chapter, which may directly or indirectly affect to security issues that belong to Member States, ES thererfore considered that the potential political impact of Article 34.5 should be carefully assessed. FR was in favour of maintaining the adequacy procedure but meant that is was necessary to preserve the procedures in Articles 35 and 36 since they would be most used by the MS allowing them to continue to exchange data with third countries, due to the low number of adequacy decisions taken on basis of Directive 95/46 and the absence of such a procedure in the DPFD. FR meant that Article 35 should be viewed as enabling MS to maintain exchange with third countries channels with third countries in the absence of adequacy decisions. FR said that it could be necessary to exchange data with third countries not offering an adequate level of protection and that the operational needs required to allow such exchanges must be continued to be carried out. AT wanted that the sequencing of the transfer in Chapter V be made clear; *i.d.*positive adequacy decision, if no adequacy decision the need for the MS to assess the safeguards offered and in the third place a transfer in the individual case in exceptional circumstances. AT also wanted it to be clarified which possible appropriate safeguards within the meaning of Article 35 could result in a

Article 33

General principles for transfers of personal data [163]

1. Member States shall provide that any transfer of personal data by competent (…) authorities (…) to a third country, or to an international organisation[164], including further onward transfer to another third country or international organisation, may take place only if:[165] [166]

transfer despite a negative adequacy decision. SE wanted that Chapter V be simplified and that it must be clear how the different Articles were related to each other, *e.g.* must the conditions in Article 33 be complied with for transfers based on Articles 34 and 35 and when Article 36 was applied. SE asked whether the possibilities to transfer data were not too limited in the draft text, *e.g.* transfer of data for judicial administratice proceedings with a direct link to combating crime, not even after consent from the initial MS.

163 PT wanted to see more safeguards in Article 34. The Chair indicated that the equivalent Article had been deleted in the GDPR. DE said that the Article did not set out criteria for striking the right balance between data protection and investigation and prosecution of crime.. EE, PL, SE, SI and UK welcomed DE comments about the right balance between data protection and combating crime. SE asked how the different Articles in Chapter V were linked and AT how Chapter V fitted into the overall scheme. SE found the possibilities for transfer to be too limited, requiring that the conditions set out in Article 33 had to be fulfilled also when applying Article 34-36 went too far. SE found the hierarchy between the Articles not clear enough. CZ considered the Article too vague and confusing, and the following problems would arise: Data transfers to victims (or supportive organizations) were probably prohibited, which would be contradictory to the Victims Directive 2012/29/EU; Data transfers to Interpol and international tribunals were put in doubt (the wording "international organizations" was stricter than that of Article 13 DPFD, which spoke about *bodies);* Purposes (a) were excessively limited (appropriate reference to "maintenance of public order" must be included and further purposes must be examined); a possibility to impose a deadline for the Member State from which personal data originated to give its prior authorization should be considered); AT wanted that it be ensured that the third State used the data only for the isolated case for which the data were transferred, and that subsequent transfer and/or use for other purposes required the consent of the transferring State and - if the data originally came from another Member State - of the "State of origin" of the data. Cion said that it was important that Article 33 set out the structure an general principles for transfer to third countries. CZ preferred Article 13 in DPFD to Article 33 and wanted it deleted.

164 FR asked about the relationship between this Directive and those organisations' specific rules on data protection.

165 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

166 ES considered that the text "may take place only if" needed to be redrafted.

(a) the transfer is necessary for the prevention, investigation, detection or prosecution of [167] criminal offences […] *the execution of* [168] *criminal penalties* or [169] the [170] safeguarding against and the prevention of threats to public security; and,

(b) (…)

[167] 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.

[168] 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.

[169] DE asked whether paragraph (a) could be used outside the purpose of police work, for example in the context of asylum or immigration law. CZ supported that the asylum and immigration law be covered by the Directive. The purpose must be set out in the Directive according to DE.

[170] BE suggested to replace *and* with *or* and add the following paragraph "(b) the transfer is necessary for the prevention of criminal offences and in maintaining public order and security for major events, in particular for sporting events or European Council meetings; and" The suggestion comes from Article 14 of the Council Decision 2008/615/JHA Prüm Decision. DE suggested to remove paragraph 1(a) to avoid that the relationship with Article 7 was unclear.

(c) the controller in the third country or international organisation[171] is an authority[172] competent for the purposes referred to in Article 1(1)[173]; and

(d) in case personal data are transmitted or made available from another Member State,[174] that Member State has given its prior authorisation[175] to the transfer[176] in compliance with its national law [177] and

[171] NL asked how paragraph (c) tied in with international organisations in criminal prosecution.. Cion accepted to clarify the meaning of *international organisation.* FI thought that paragraphs (c) and (e) needed to be fine tuned. FI suggested to use *intergovernmental organisation* in accordance with the Vienna Convention on the Law of Treaties.

[172] DE, , suggested to delete paragraph (c) and, supported by BE, revise recital 45 so as not to rule out the possibility for judicial authorities and the police to share information with private parties, this is in particular important for cybercrime. BE noted in this context that the Europol Regulation (general approach in June 2014) (10033/14, Article 2(g) contained a definition of *private parties.*

[173] SE said that this paragraph raised great concern for bodies prosecuting crimes which work with Google and Facebook, it also created problems for courts of law, *e.g.* when they need to hear witnesses abroad or serve a writ or other deeds abroad. CZ wanted to add other bodies such as for example victims and organisations supporting victims. DE, NO and SE meant that paragraph (c) was too narrow.

[174] EE said that it sometimes was difficult to know that data had arrived from a third country.

[175] DE understood "prior authorisation" to cover authorisations given for transfers within the EU or generally and meant that this should be set out in recital 49a, as was the case in recital 24 in DPFD.

[176] AT wanted to add "including further onward transfer," after *transfer* to make clear that the consent in also necessary for subsequent transfer.

[177] 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 [178] or in the absence of an adequacy decision pursuant to Article 34 or of appropriate safeguards in accordance with Article 35, where derogations for specific situations apply pursuant to Article 36.

[179]

[178] ES queried whether paragraph (e) did not contradict Article 36 whereas CH, FR, UK suggested to insert a reference to Article 36. NL asked about cooperation agreements with third countries for *i.d.* investigation but that the data could be used in the third country for other purposes than those set out in paragraph (e). NL suggested to insert *consent* to be able to use the data for all purposes. 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).

[179] DE 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).

2[180]. 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 [181] for the prevention of an immediate[182] and serious threat to public security of a Member State or a third country or to essential interests[183] 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.[184]

---

180 Moved from Article 36a

181 UK preferred "necessary" to "essential".

182 ES and UK suggested to replace "immediate" because this word is often misinterpreted and replace it with "direct" that is not only temporal. Cion pleaded for *immediate* because it was the language used in the acquis.

183 BE asked about the meaning of *essential interest* and whether a common definition existed.

184 AT wanted it to be clarified that a MS could have ruled out such transfer beforehand.

Article 34

Transfers with an adequacy decision [185]

1. Member States shall provide that a transfer[186] of personal data to a third country or a territory or one or more specified sectors within a third country[187] or an international organisation[188] may take place where the Commission has decided in accordance with Article 41 of Regulation (EU) **…./20~~12~~ XXX** or in accordance with paragraph 3 of this Article

---

185 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. SK suggested to copy Article 13 of DPFD. CH said that in case the GDPR should not constitute an integral part of the Schengen acquis, CH would not be bound by its provisions. However, in order to avoid restrictions in data exchange, CH should continue to be considered a Schengen country regarding the exchange of data between EU MS and CH in the entire area of Schengen and Dublin cooperation. This includes data exchange under the Schengen and Dublin cooperation to which the Data Protection Directive does not apply. DE had doubts if Article 34 corresponded with reality. DE further did not support the Cion's role regarding adequacy decisions. UK supported DE that it was better that the adequacy decision were taken by the MS rather than Cion. DE said that Article 60 and Article 34 were contradictory. FR wanted a clarification concerning the procedure for adopting an adequacy decision, will it be the same as the current system, *i.e* Article 31 of Directive 1995, and who can refer a matter to the Cion. In reply to FI why a specific Article on adequacy was needed in addition to the Chapter V of GDPR, Cion replied that it was an enabling tool if the general provision did not suffice when a country adequacy was not possible and that the sector specific approach was used more frequently now. Cion mentioned PNR and TFTP as ad hoc sui generis sectoral approaches. FR found that such approach was not the most relevant.

186 BE and FR suggested to talk about "any transfer or set of transfer".

187 SE asked if not the area covered by the Directive was a single sector. Cion said that countries are different it might be that in one country only one public authority has the adequate level of protection or only the federal level but not the state level.

188 FR thought that the *international organisations* could be deleted in this paragraph.

that the third country or a territory or specified sector[189] within that third country, or the international organisation in question ensures an adequate level of protection[190]. Such transfer shall not require any specific authorisation. [191]

[189] The term processing sector was changed to specified sector in Chapter V of GDPR, as agreed at the Council in June 2014. FR asked for example if a State could not be subject of an adequacy decision whereas one of its entities might be, or that an international organisation might ensure an adequate level in one sector but not in another.

[190] For SE it was important that the procedure to adopt a Decision on an adequate level of protection was not made too complicated. (FI wanted that adequacy decisions must be made swifter than currently.) FR asked about the meaning of the last sentence of paragraph 1. NL pointed to the low number of countries being considered as having an adequate level of protection by the Cion and meant that a heavy procedure was being created. NL wanted Cion to explain how this procedure would be used for the police and judiciary sectors.

[191] BE asked whether the individual MS could require additional requirements. PL meant that since law enforcement authorities would need to react quickly to protect *e.g.* fundamental rights, if there was a general decision by the Cion that would not be possible. 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.

2[192] Where no decision adopted in accordance with Article 41 of Regulation (EU) ~~…./2012~~ **XXX** exists, the Commission[193] shall[194] assess the adequacy of the level of protection, ~~**giving consideration**~~ **in particular taking into account of** ~~**to**~~ 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;

(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[195]; and

---

192 BE reservation on Article 34(2) because it should be based on the GDPR and not on police cooperation or cooperation in criminal matters.

193 RO meant that it was necessary to involve the EDPB at this stage.

194 DE suggested to replace *may* with *shall* because it seemed excessive and undesirable that the Cion had to assess the level of protection of all countries in the world and if the Cion found that a country did not have an adequate level of protection it would entail political tensions, DE therefore found it better to leave it to the Cion to decide whether or not to assess the level of protection.

195 Cion scrutiny reservation.

(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 ~~**and decissions …Article 25(6)**~~.

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. ~~***At the appropriate time,***~~ ***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.[196]

8. (…)

[196] LV thought that such lists could be published on MS websites. Cion could accept this. CZ thought that there should be a provision requiring the Member States to either publish their adequacy decisions or report them to the Commission. RO did not want the list to contain the countries whose level of protection were not considered adequate (black list) but wanted the Cion to look over and update the list periodically.

Article 35

Transfers by way of appropriate safeguards[197]

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[198] have been adduced in a legally binding and enforceable[199] instrument [200]; or

[197] EE asked what would happen after the transfer. CZ and FR meant that the MS must be able to conclude bilateral and multilateral agreements. BE asked if INTERPOL Rules on Processing of Data ensure an adequate level of protection, BE hoped that a pragmatic approach would be taken on this issue.

[198] 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),"

[199] DE raised concerns, supported by CY, about *enforceable* and found that it was a too high requirement and wanted more flexibility.

[200] LV, RO, SE and SI asked clarifications on "a legally binding instrument". Cion replied that bilateral legally binding agreements were covered. BE asked whether the general regulations of Interpol would be covered here. CZ suggested to add "such as an agreement concluded by Member State" before *or* to recognize the powers of the individual MS to conclude agreements in this area.

(b) the controller (…) has assessed all the circumstances[201] surrounding [202] the transfer of personal data [203] and concludes that appropriate safeguards exist with respect to the protection of personal data[204]. Such an assessment may take into account the existing cooperation agreements between Europol and/or [205] Eurojust[206] and third countries which allow for the exchange of personal data.[207]

[201] FI suggested that the *circumstances* to be taken into account at the assessment be clearly specified in the Article. Another option according to FI would be to stipulate in line with Article 13.3 of DPFD that the safeguards have been deemed adequate by the MS concerned according to its national law.

[202] DE suggested adding "the individual case of" after *surrounding.*

[203] 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)."

[204] AT scrutiny reservation on Article 35.1(b). UK thought that it was not clear whether every single processing operation needed safeguards or whether it was more general. 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.

[205] MT suggestion.

[206] HR welcomed the insertion of the reference to Eurojust and Europol. Cion said that the scope of the Europol and Eurojust on the one hand and this Directive was different and that it might be misleading to refer to such texts but said however that the wording could be modified to refer to these two instruments.

[207] NL, RO, CH, BE were happy with the new text, ~~BE except the reference to DPFD~~. DE and FI 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.

208

2. (…)

Article 36

Derogations for ~~transfer in~~ specific situations

1. (…)***I****n 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 categoryof transfersof 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[209]

(b) the transfer is necessary to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides; or

208 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".

209 NL asked about the differences between paragraphs (a) and (b).

(c) the transfer of the data is necessary [210] for the prevention[211] of an immediate[212] and serious threat to public security of a Member State or a third country; or

(d) the transfer is necessary in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences,*the execution of criminal penalties* or the safeguarding against and the prevention of threats to public security; or[213]

(e) the transfer is necessary[214] in individual cases[215] for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection or the safeguarding against and the prevention of threats to public security or prosecution of a specific criminal offence or the execution of a specific criminal penalty. [216]

[217]

[218]

---

[210] UK suggestion.

[211] CZ said that paragraph (c) should refer to all purposes in Article 1.1, not only prevention.

[212] ES suggested to replace "immediate" because this word is often misinterpreted and replace it with "direct".

[213] CZ asked what documents would be needed for *e.g.* an EAW being transferred to Interpol. Cion said that *prevailing public interest* is what was intended, this requires that it fulfils the necessity and proportionality tests. Cion suggested to add "if proportionate and necessary" to ensure alignment with

[214] CZ wanted to replace *necessary* with *essential* as in paragraph (c) or *required* because the meaning of necessary was unclear.

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

[216] DE asked what would happen if data was transferred to an entity/body that pursued other purposes than the ones pursued in the Directive; Article 36.1(e) could *e.g.* be used for civil proceedings. BE feared that paragraph (e) was too narrow.

[217] DE, supported by CZ, suggested adding a paragraph (f) with the following wording: "**(**f) the transfer is necessary in individual cases for compliance with a legal obligation or for the lawful exercise of a legal power the controller is subject to." The text from DE was the same as for deleted Article 7(1)(b). CH suggested 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".

[218] DE, supported by SK, suggested adding a paragraph (2) with the following wording: "2. Personal data shall not be transferred, if in the individual case the data subject has protectable interests, especially data protection interests, in the exclusion of the transfer, which override the public interest in the transfer set out in paragraph 1."

2. Personal data shall not be transferred, if in the individual case the data subject has protectable interests, especially data protection interests, in the exclusion of the transfer, which override the public interest in the transfer set out in paragraph 1."[219]

Article 36a

(…)

Article 37

Specific conditions for the transfer of personal data

Article 38

International co-operation for the protection of personal data

(…)

---

219 DE suggestion. FR reservation on the paragraph in its present wording. IE, AT, PT scrutiny reservation. RO supported the text. HR supported the insertion of the paragraph. CY and PT scrutiny reservation. CZ, FI, SI and CH asked to what situations this paragraph was applicable. FI asked if the paragraph was an exception. EE found the text too restrictive and could not support it. DE said that its suggestion for paragraph (2) was to be seen in the light of its opinion that Article 36 should be a way for transfer on equal footing with the other Articles in Chapter V. DE was also concerned that the CoJ would see Article 36 as an exception and therefore interpret it narrowly. DE gave the following example of when the paragraph could be used: when *e.g.* a crime in the concrete case will lead to a death penalty then transfer of data should not take place. FR, supported by UK, meant that the language was too vague and broad and did not see that the paragraph could be used. UK was particularly concerned about the reference to protectable interests and meant that the paragraph could stand in the way for transfer. UK also asked who would decide on its use. UK, wanted to delete the paragraph.CH meant that the paragraph seemed to be addressed to the data subject not to the MS. Cion rather liked the paragraph but meant that it was necessary to fine tune the wording. Cion meant that it could be a useful addition but that it concerned the whole structure and in light of the general approach on the GDPR it could not remain in the text.