Council of the European Union

Brussels, 19 November 2014

Interinstitutional File: 2012/0010 (COD)

15659/1/14 REV 1

LIMITE

DATAPROTECT 171
JAI 894
DAPIX 173
FREMP 211
COMIX 617
CODEC 2277

NOTE

From:	Presidency
To:	Working Group on Information Exchange and Data Protection (DAPIX)
No. prev. doc.:	11109/14 DATAPROTECT 95 JAI 541 DAPIX 90 FREMP 128 COMIX 327 CODEC 1504
No. Cion prop.:	5833/12 DATAPROTECT 6 JAI 41 DAPIX 9 FREMP 8 COMIX 59 CODEC 217
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

I. Introduction

1. At its meeting on 29 September DAPIX discussed the first two Chapters of the draft Data Protection Directive. The Presidency had decided to have an open discussion about principles and difficulties.

2. At its next meeting devoted to the Directive, Chapter V on international transfer was on the agenda. The equivalent Chapter of this Chapter in the General Data Protection Regulation (GDPR) had been agreed by the JHA Council in June 2014. At this meeting the delegations made clear that it was difficult to discuss this matter as long as the scope was not clearly set out in the text.

3. For these reasons the Presidency has decided to revert to the question of the scope of the Directive at its next meeting. Other issues in the first two Chapters will also be discussed at the same meeting.

4. The purpose of this note is to explain the main changes that the Presidency is suggesting for the two Chapters. All changes in the Annex are indicated in **bold and underlined** for new text, parenthesis for deletions and *italics* for text that has been moved within the text.

Subject matter and objectives

5. The first and most important change is Article 1 and new recital 11a.

6. Delegations have raised concerns that the replacement of the 1995 Directive with a Regulation and the Framework Decision from 2008 with a Directive will make it difficult to have all activities of the police and other law enforcement authorities in the performance of their institutional tasks covered by one single instrument. To this end the EL Presidency presented a text introducing the possibility to also have a reference to the need to safeguard public security linked to the initial scope of the Directive (prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties) by the words "and for these purposes". The reference to public security rather than to public order (as required by some delegations) was introduced due to the difficulty of finding a common understanding of the latter. In the course of the discussion some delegations have asked for the deletion of *for these purposes* in Article 1 of the Directive. The Commission has opposed that because it would impinge on the scope of the Regulation and lead to legal uncertainty.

7. During the last meeting the German delegation in particular has suggested a wording taken from Article 72 TFEU that reads as follows:

"1. This Directive lays down the rules relating to the protection of individuals with regard to the processing of personal data by competent (…) authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties as well as by the police or other law-enforcement services for the purposes of maintaining law and order and the safeguarding of internal security." (14105/14).

8. In order to have a clear view and find a satisfactory way forward, the Presidency puts forward these three options for consideration:

- 1. Keep the reference to "safeguarding public security" and maintain "for these purposes", or
- 2. keep the reference to "safeguarding public security", delete “for these purposes” and clarify what must be implied by “public security” by adding the new 11a recital, or
- 3. take on board the above-mentioned German suggestion, with the need to better clarify what the wording "law and order" is meant to include/exclude and in particular, as far as the concept of "internal security" is concerned, in order to avoid overlapping with tasks assigned to intelligence services in order to protect the security of the State from internal threats.

8. DE has suggested changes to the scope of the GDPR so that what is added to the scope of the Directive will find a correspondence in the definition of the scope of the Regulation.

9. In case option 2 is preferred, the Presidency is proposing to add a new recital 11a clarifying what is meant with public security, in order to make clear that this concept includes most of the police institutional tasks. In the recital, the Presidency introduced language from the Treaty - police and law enforcement services- and specified that the Directive would apply to the processing by the police and law enforcement services for the purposes of safeguarding of public security. The notion of public security has been narrowed down in the new recital, notably to make clear that activities of the intelligence services for the purposes of safeguarding national security are excluded from the scope.

The new recital 11a reads as follows:

"(11a) The activities carried out by the police or other law enforcement services, which are mainly focused on the prevention, investigation, detection or prosecution of criminal offences also include safeguarding public security (such as activities carried out by the police and other law enforcement services in the Member States aimed at preventing real and severe threats to fundamental interests of the society at large protected by the law and which may lead to a criminal offence). This Directive should therefore also apply to activities carried out by the police or other law enforcement services for the purposes of safeguarding public security while excluding activities carried out by intelligence services for the purposes of safeguarding national security which are outside the scope of union law. [Those activities of safeguarding public security, insofar as t hey are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences, may include activities which go beyond the scope of Chapter 4 or 5 of Title V of Part Three of the Treaty on the Functioning of the European Union (*i.e* judicial cooperation in criminal matters and police cooperation)][1]."

Definition of competent authority

The Presidency has maintained the definition from the previous text. This definition allowed for private bodies under certain conditions to be covered by the Directive. Some delegations raised concerns that this definition risked to create a too broad scope and wanted clarification for example on the applicable framework in cases such as where banks and financial institutions that, e.g for money laundering purposes, were obliged to inform the police of certain flux of money would be covered by the Directive. The Presidency has therefore modified recital 11 to explain that such operations should not be covered by the Directive.

Definition of international organisation

As agreed when Chapter V was discussed on 27 October 2014, a definition of international organisation was introduced. This definition is the same as the one in the GDPR. However, in line with the Europol Regulation, *Interpol* has been added to this definition.

[1] The last sentence of the recital 11a is necessary if the words "for these purposes" are deleted.

Article 4

In reaction to delegations queries as to why further processing in general and further processing for historical, statistical or scientific purposes were set out in different Articles, the Presidency brought the paragraph on further processing for historical, statistical or scientific purposes from Article 7 to Article 4 on principles of processing.

The responsibility for further processing lies with the controller, as is set out in Article 4(4).

For further processing for the historical, statistical or scientific purposes, the text has been brought in line with the Article 3(2) of Framework Decision from 2008 to indicate that competent authorities may further process personal data for such purposes.

A paragraph 2a has been added, dealing with transfer to other competent authorities or private bodies.

Article 5

Article 5 on different categories of data subjects has been deleted following requests from delegations. Since Article 5 was building on the principle of accuracy set out in Article 4, some text from the corresponding recital now appears in recital 21 on the different categories of data, in line with similar text present in the Europol and Eurojust legal framwork.

Article 6

At the request of many delegations the Presidency has reverted to the drafting in the Framework Decision from 2008 setting out that the competent authorities shall take all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted rather than ensuring the same.

(Article 8 second part has been slightly redrafted.)

Article 35

The Presidency has extended the list of situations in which transfers may take place despite the absence of an adequacy Decision. It has added that the controller could use agreements between Europol and Eurojust and third countries as well as assessments made according to Framework Decision from 2008 as basis for transfers.

Article 36

The Presidency finds it important that for the case of conflict between data protection interests and other interests such as the public interest to prevent and solving crime an appropriate balance must be struck. A paragraph has therefore been added that sets out that this balancing must take place.

Article 35 and 36

At the request of some Member States the Presidency has deleted the requirement that transfers must be recorded and that the records must be available for the supervisory authority. The intention is to redraft Article 23 to cover the situations in Articles 35 and 36.

Article 60

The last sentence has been deleted. The Presidency considered that this text was superfluous since the obligation to eliminate incompatibilities is already set out in the TFEU.

In the light of the above, delegations are invited to

(a) agree which of the three options they would prefer to further develop.
(b) discuss the changes to Article 4
(c) agree to the definition of competent authorities together with the explanation in the recital that not all bodies having a legal obligation to assist the police will be covered by the Directive.
(d) agree to the new drafting of Article 6
(e) discuss the addition to Article 35(1)(b)
(f) express themselves on the need for the paragraph on the balancing of interests.

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, and the free movement of such data[2]

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[3],

Acting in accordance with the ordinary legislative procedure,

---

2 ES, HU, IT, LV, PT, SI, UK scrutiny reservation on the whole text. FI scrutiny reservation since FI meant that the GDPR should be dealt with first.

3 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, [and for these purposes], safeguarding of public security or the execution of criminal penalties 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[4] 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.

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

(6) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters[5] 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 **[**and for these purposes**,]** (…) safeguarding of public security or the execution of criminal penalties 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. [6]

(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.

---

5 OJ L 350, 30.12.2008, p. 60.

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

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

(11) Therefore a distinct Directive should meet the specific nature of these fields and lay down the rules relating to the protection of individuals with regard to the processing of personal data by competent **(…)** authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences [and for these purposes,] (…) safeguarding of public security, or the execution of criminal penalties.[7] Such competent authorities may also include any bod**y**/entit**y** entrusted by national law to perform public duties or exercise public powers for the purposes of prevention, investigation, detection or prosecution of criminal offences, **[**and for theses purposes**]** the safeguarding of public security 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,[and for these purposes] safeguarding of public security, 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 processes those personal data further 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]

---

7 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."

8 FI scrutiny reservation and SE reservation. ES found that the recital neither defined nor clarified what was meant with *bodies/entities.* SE meant that the scope of the Directive should be set out in the body of the text. SE found the text in particular the last sentence very prescriptive. SE opposed the deletion of the text in square brackets in Article 1.1 and 3.14 and therefore requested the removal of parts of recital 11.

(**11a) The activities carried out by the police or other law enforcement services, which are mainly focused on the prevention, investigation, detection or prosecution of criminal offences also include safeguarding public security (such as activities carried out by the police and other law enforcement services in the Member States aimed at preventing real and severe threats to fundamental interests of the society at large protected by the law and which may lead to a criminal offence). This Directive should therefore also apply to activities carried out by the police or other law enforcement services for the purposes of safeguarding public security while excluding activities carried out by intelligence services for the purposes of safeguarding national security which are outside the scope of Union law. [Those activities of safeguarding public security, insofar as they are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences, may include activities which go beyond the scope of Chapter 4 or 5 of Title V of Part Three of the Treaty on the Functioning of the European Union (*i.e* judicial cooperation in criminal matters and police cooperation)]**[9]**.**

(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 [and for these purposes] safeguarding of public security or the executions of criminal penalties. 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.[10]

(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.

---

9 The last sentence of the recital 11a is necessary if the words "for these purposes" are deleted.

10 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

(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. 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 activity[11] concerning national security, taking into account Articles 3 and 6 of the Treaty on the Functioning of the European Union, nor [12] to data processed by the Union institutions, bodies, offices and agencies, such as Europol or Eurojust. [13]

(15a) Regulation (EC) No 45/2001[14] 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 …../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 criminal proceedings. [15]

---

11 FR suggested to change "activity" into "such as *activities* …"

12 FR suggested to add the following text: "nor does it cover 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". 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.

13 AT did not find recital 15 clear.

14 OJ L 8, 12.1.2001, p. 1.

15 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. [16]
[17]

(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, in particular by chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained.[18]

(17) Personal data relating to health should include in particular (…) data pertaining to the health status of a data subject, (…) including any information on, for example, a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as for example from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.

---

16 Cion welcomed the redrafting of recital 16 ensuring consistency between GDPR and the Directive.

17 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.

18 SE expressed concerns with recital 16a because of DNA profiles with the purpose of identifying should not be allowed to be used in the future.

(18) Any processing of personal data must be (…)lawful and fair in relation to the individuals concerned, for specific purposes laid down by law.[19]

(19) For the prevention, investigation and prosecution of criminal offences [and for these purposes], (…)[20]safeguarding of public security, it is necessary for competent (…) authorities to (…) process personal data, collected in the context of the prevention, investigation, detection or prosecution of specific[21] criminal offences beyond that context to develop an understanding of criminal phenomena and trends, to gather intelligence about organised criminal networks, and to make links between different offences detected.

19a In order to maintain security of the processing and to prevent processing in breach of this Directive, personal data should be processed in a manner that ensures an appropriate level of security and confidentiality, 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 historical, statistical or scientific 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. [22]

---

19 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.

20 BE wanted to add the following text: "and the prevention of danger".

21 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.

22 ES 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.

(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, 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.* In particular in judicial proceedings, statements containing personal data are based on the subjective perception of individuals and are in some cases not always verifiable. Consequently, the requirement of accuracy should not appertain to the accuracy of a statement but merely to the fact that a specific statement has been made.

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

(23) (…).[23]

(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. [24]

[23] 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.

[24] 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 offence, [and for these purposes,] safeguarding of public security, or the execution of criminal penalties. 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 prevention of an immediate[25] and serious threat to public security.[26]. 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)**[27] 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**.**[28]

---

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

26 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.

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

28 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[29] Union law or the national law applicable to the transmitting competent (…) authority provides for[30] specific conditions applicable in specific circumstances to the processing of personal data, [31] 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[32] 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.[33]

[29] BE wanted to replace *where* with *when* (as in Article 7.3 suggested by BE).
[30] BE suggested to delete *for*.
[31] 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).
[32] CH wanted to replace "paragraph 1" with "the first sentence".
[33] 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. This 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 specifically[34] 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[35] 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[36]**.** However, the agreement of the data subject should not provide in itself a legal ground for processing such sensitive personal data by competent **(…)** authorities. [37]

(27) Every data subject should have the right not to be subject to a decision which is based solely on profiling (…), unless authorised by law and subject to appropriate safeguards for the rights and freedoms of the data subject (…).

---

34 ES did not see the need to "specifically" to refer to authorisation by law and therefore suggested to delete it.

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

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

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

Whereas:

(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 , [and, for these purposes], safeguarding public security, or the execution of criminal penalties, 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. [38]

(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.

[38] 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.
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[39] 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 [and for these purposes], safeguarding of public security or the execution of criminal penalties, or in individual cases for the establishment, exercise or defence of legal claims.

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

(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. [40]

(72) Specific provisions with regard to the processing of personal data by competent (…) authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences [and for these purposes] safeguarding of public security or the execution of criminal penalties in acts of the Union which were adopted prior to the date of the adoption of this Directive, regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, should remain unaffected. The Commission should evaluate the situation with regard to the relationship between this Directive and the acts adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, in order to assess the need for alignment of these specific provisions with this Directive.

[40] 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.

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

[41] CH suggested adding ",as far as possible,".

CHAPTER I

GENERAL PROVISIONS[42]

Article 1

Subject matter and objectives[43]

1. This Directive lays down the rules relating to the protection of individuals with regard to the processing of personal data[44] by competent[45] **(…)** authorities[46] for the purposes of[47] the

---

42 PL, FI, UK scrutiny reservation on Chapter I. SI critical to Chapters I and II. Cion scrutiny reservation on the text in bold in Chapters I and II.

43 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, 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. DE, NL and UK entered scrutiny reservations on the whole Directive. BE entered a substance reservation on Article 1(1) FI found that Article 1.1 did not clearly set out whether court activities were covered by the Directive. BE and UK reservation of substance.CY scrutiny reservation on Article 1(1) NO meant that the police authorities should be allowed to apply only one instrument.

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

45 NL said that the police did not only investigate criminal offences, maintained public order, it also had jobs of administrative nature. FR supported BE, ES and UK. FR thought that a recital should be added to clarify this. NO said that private enterprises could be involved in this area, *e.g.* as processors. Cion said that the DPD 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). The Cion indicated that the DPD was applicable to courts for criminal matters whereas for other courts the Regulation would be applicable FI meant that adding *public order and security* would facilitate the implementation of the Directive and the Regulation.

46 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. EE meant that "public authorities" created a misunderstanding if both the Regulation and Directive are applicable. 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. If the private nature of such private entities was predominant provisions should ensure that they are governed by the GDPR, potentially with safeguards considered necessary under Article 21 of the Directive.

47 Cion stated that the notion of "public" had moved from the GDPR to the Directive and that the Cion was against applying the Directive to private bodies since that was against the logic of the Treaty.

prevention[48], investigation[49], detection[50] or prosecution[51] of criminal offences [and for these

[48] FR wished certain activities carried out by the special administrative police aiming at prevention of an offence or unrest against national security to be covered by the Directive. DE wanted that threat prevention by the police be covered by uniform provisions.

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

[50] PL suggested to add "of crime and perpetrators".

[51] FI wanted that "prosecution" be clarified in particular to know whether courts and prosecutors are covered by this Article and if so to what extent. The Chair explained that courts are covered and that recital 55 had been changed to make this explicit. For EE "prosecution" covered both the pre-trial and trial phase and the same law applied in EE so where was the borderline for the Directive? FI wanted to a clarification of the exact coverage of the Directive in respect of *prosecution* and courts.

purposes,] [52],

[52] DE welcomed putting "for these purposes" within square brackets for three reasons: GDPR was not fitted for police work, secondly difficult delimitations were avoided and thirdly it allowed the MS to create a uniform framework for the police as regards data protection. CZ also raised concerns about the GDPR being used by omission. Once the text in square brackets was deleted, DE asked how the idea of *safeguarding public security* could be reformulated and hinted to the RO suggestion in doc 8208/13.DE suggested the following text to set out the scope: "This Directive lays down the rules relating to the protection of individuals with regard to the processing of personal data by competent (…) authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties as **well as by the police or(and) other law-enforcement services** for the purposes of maintaining law and order and the safeguarding of internal security. The underlined text should be added to the list of areas in Article 2 (e) of the GDPR upon which the that Regulation will not apply. The corresponding recital should read: "DE said that the wording came from Articles 72.2 and 87.1 from TFEU.BE, CZ, ES, FR, NL, RO supported the deletion of the text in square brackets and said that the most important was that the police was subject to only one single data protection instrument. EE also meant that the law enforcement services should only be covered by one instrument. HU also welcomed the deletion of the text in square brackets. In contrast SE that wanted to keep the text in square brackets. Cion indicated that the are different legal acts in the EU today, *e.g.* civil justice, migration, money laundering and trafficking where the MS have both law enforcement authorities and the police being responsible on the basis of Directive 1995. Cion also pointed at Articles 6.3 and 21 of GDPR which provide the MS with the flexibility to specify the general rules in the GDPR. For the Cion it was important to maintain a high level of protection as well as to cover all EU policies; no issue should fall outside the scope of both instruments. BE contested that it was not yet certain what the text of the GDPR would look like and that being the situation BE preferred including the police in the Directive. BE said that if *public security* was changed into *public order* the text was acceptable. NL thought that even administrative police work such as issuing permits for fire arms were linked to the criminal area and should therefore be covered under the same instrument. ES supported the NL suggestion to cover administrative police in the Directive whereas AT was sceptical to it. FI appreciated the text suggested by DE, in particular to use the terminology of *law enforcement services* as this concept is used for border controls, customs and in the Prüm Decision. PT appreciated the use of Treaty language in the DE suggestion and CZ the reference to *law enforcement authorities*. In contrast SE that wanted to see the Directive being used only for law enforcement purposes and compared with the **DPFD**. SE meant that only law enforcement activities required special rules. HU wanted to see a strict scope, only covering Title V, Chapters 4 and 5. UK wanted to know if the deletion of the text in square brackets and public security was excluded from the scope of the GDPR meant that the Directive applied to all public sector activities. DE gave the example of the police being called to a house where a dead body has been found, if there has been a murder, *i.d.* a criminal offence the Directive would be applicable whereas if it is a natural death the Regulation would be applicable. A missing person is another example, this uncertainty would decide if the Directive or Regulation would be applicable. This situation was not satisfactory according for DE and EE. ES found it useful to discuss whether private security activities were covered and noted that only processing operations carried out by private security operators having a public purpose could be covered by the Directive. ES stated that it was necessary to look at the tasks and the function that were carried out and not by whom. Support from FR. DE further said that problems arise due to the fact that the 95 Directive will be replaced by a Regulation having for consequence that MS would not be allowed to transpose all the provisions from this Directive and GDPR into national law taking account of the national situation/context. ES and DE asked about "civil protection, and whether it was covered. For EE it was not clear to what authorities the Directive would be applied when they performed an activity not as their sole/predominant task. EE asked if for example law enforcement authorities would be covered and what about environmental offences. EE and CH did not find that the Directive should cover courts and judicial bodies. BE, supported by CZ, DE, RO, wanted to delete "for these purposes"; CZ meant that public order should be maintained for other reasons than prevention etc of criminal offences.

safeguarding of public[53] security[54] or the execution of criminal penalties[55]

[53] ES asked whether *citizens* security was covered with this drafting.

[54] SE meant that public security was a difficult notion and too broad a notion, especially if private bodies would be included in the scope. RO preferred *public order* but said that it could be flexible on that but then *public order* had to go out of the GDPR. FR and EE preferred *public order* and ES *public security*. Cion indicated that *public* security ia a known EU term and therefore more familiar than other concepts. For Cion the maintenance of the text in square brackets and the links to *public security* were important to keep. FR and ES and SI reminded that the Directive would apply to the judiciary as well. AT scrutiny reservation on *public* security and meant that although it had been used previously AT was uncertain if the meaning was the same. RO asked for clarifications of the notion of *public security* since in RO the notion of public order exists but no public security. In the same vein ES said that *public* security had a particular meaning within the ES Constitution and that it would be difficult to translate it for ES. RO meant that maintaining public security was a purpose in itself. FI supported the use of *public security*. BE, CY, EE and NL preferred to keep *public order* rather than *public security*, for *BE* because it meant that public security differs from MS to MS. UK found the notion of public security uncertain. FR preferred *public order* because it fitted into its national law. DE, supported by PT, meant that many MS seemed to have problems with the notions *public order* and *public security* and as a consequence the scope became unclear. Cion preferred *public security* because it was a well-known notion in the acquis and was an autonomous definition.

[55] BE, DE, ES, FI, FR, PL and SE, queried whether this Directive would cover court proceedings (also valid for Article 3(14). ES did not want the Directive to cover court activities. RO, supported by CZ, wanted to add "and ensuring public order and security". BE wanted to ensure that both arms/branches of the police were covered by the Directive. BE also wanted to insert a recital with the following wording: "the criminal character of the offences in Article 1 is not decided by the Member States' national law but by the European Court of Human Rights which specifies that the criminal character depend on the following criteria; the severity of the potential crime that the person concerned risks to meet/face". EL wanted to know whether the processing of personal data in criminal records was included. RO suggested to exclude police activities linked to the operational side of the activity regardless of how they are classified in the MS national legislation. RO further considered that the maintenance of public order/risk represented a significant part of police work and that there were no clear distinction between the scope of GDPR and the Directive. RO meant that this had negative repercussions on other aspects of public order. Since the Directive will apply to domestic processing DE wanted to know what was meant with domestic data processing. IT asked for clarifications on the notion of competent authorities for the purposes …penalties " in order to precisely define the scope of the Directive and the interaction between the Directive and the Regulation. IT said that since it was difficult to distinguish tasks relating to those activities from purely administrative tasks it was necessary that the Directive and the GDPR be as consistent as possible. AT was in favour of extending the scope to the maintenance of public order as long as they fall within the ambit of EU law and therefore suggested the following addition to paragraph 1 after penalties and having deleted the text in square brackets "Public authorities in the sense of the Directive are the authorities established in the respective Member State, insofar as they are competent for the prevention, investigation, detection or prosecution of criminal offences or for the execution of criminal penalties." NL thought that focus should be on crime prevention. DE suggested the following text for Article 1(1): " This Directive lays down the rules relating to the protection of individuals with regard to the processing of personal data by competent (…) authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties as well as for the purposes of maintaining law and order and the safeguarding of internal security by the police or other law-enforcement services. (see 14105/14 for further explanations).

1a. This Directive shall not preclude Member States from providing higher safeguards than those established in this Directive[56] for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent **(…)** authorities.[57]

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

[56] SE and DE welcomed the new Article 1.1a but thought that a full stop could be put after "Directive".

[57] 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 is neither restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data. [58] [59] [60] [61] [62] [63]

[58] 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 meant that the meaning of paragraph 1.2(b) and its effect for MS needed to be clarified. SE, supported by CH, DE, RO said that Article 1.1a and 1.2(b) seem to contradict each other. In contrast, EE saw no problems with paragraph 2.

[59] 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.

[60] 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.

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

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

[63] 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 [64]

1. This Directive applies to the processing of personal data by competent (…) authorities for the purposes referred to in Article 1(1). [65]

2. This Directive applies to the processing of personal data wholly or partly by automated means[66], 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.[67]

---

[64] 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.

[65] 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 ". by the MS when carrying out activities which fall within the scope of Union law" as set out in Article 16 TFEU. DE, supported by AT, suggested to add in the end of the sentence: "Article 1(1) and their transmission by competent public authorities for other purposes." 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.

[66] 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,".

[67] 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[68]; (…)[69] [70];

[68] AT, ES and IT thought this required clarification. ES and IT referred to the difficulties of distinguishing between criminal intelligence and national security intelligence operations. IT referred to specific case of personal data collected in the context of foreign security (CFSP) operations, which might be transferred to law enforcement authorities. IT asked for clarification as to what activities carried out by which bodies are considered outside the scope of Union law, possibly including an indicative list. Cion, supported by UK, thought it was not expedient to define the concept of national security in secondary legislation as this concept is used in the TEU. DE meant that at least public security requirements were needed. FR suggested to insert the following: "by the MS when carrying out activities under chapter 2 of title V of the TFEU." FR considered also that it was necessary to change recital 15 in line with what was already done in GDPR. AT suggested the following addition to paragraph 3(a) " such as an activity concerning national security, or an activity which is not governed by legislative measures in the area of judicial or police cooperation based on Title V Chapters 4 and 5 (Art. 82 – 89) TFEU". The Chair said that it was clear by the definition that the EU Treaties were excluded and that it was not necessary to set out all excluded areas. AT wanted that the content of "EU law" was clarified. NO said that as a non-member of the EU national security was not covered and that should be set out explicitly.

[69] DE meant that the deletion of "national security" was contra productive and that it was better to reinsert the text of the initial proposal relating to national security. Support from AT, FI, EE, NO and UK, for FI even despite recital 15. FI scrutiny reservation on its deletion.

[70] FR suggested to add the following point (aa) to paragraph 3: " (aa) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union;". The FR wording used the wording as in GDPR, and recital 15 should be changed accordingly.

(b) by the Union institutions, bodies, offices and agencies[71].

[72]

[71] Many MS (CZ, DE, EE, ES, FI, LV, PT, RO, SE) queried why these bodies and agencies had been excluded from the scope of the Directive. AT thought the data protection regime of these bodies and agencies should be governed by a separate instrument. AT therefore suggested to add "such as Europol or Eurojust". Cion confirmed that it would, at a later stage, table a proposal to amend Regulation 45/2001 in order to align the data protection regime for Union institutions, bodies, offices and agencies align the data protection. DE thought this exclusion was difficult to reconcile with the Cion's stated aim of full harmonisation. BE reservation. The Chair explained that Europol, Eurojust and Prüm have their own regime of data protection. HU and RO asked how consistency between Europol, Eurojust and Prüm and GDPR and DPD could be ensured. Cion said that even if the text "Union institutions … agencies" was deleted the Directive could not apply to such bodies because a Directive can only apply to MS. Concerning consistency when proposing changes to Directive No 45/2001 the Cion would look at that. IT wanted that the relationship between Article 2(3)(b) and Article 59 be made clear.

[72] 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[73]

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[74], in particular by reference to an identifier such as a name, an identification number, location data, online identifier[75] or to one or more factors specific to the physical, physiological, genetic[76], mental[77], economic, cultural or social identity of that person. [78];

(…)

---

[73] 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.

[74] 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".

[75] 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.

[76] FR reservation.

[77] FR and RO wanted to know what *mental* meant.

[78] 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, combination (…)[79] erasure or (…)[80];

(4) 'restriction of processing' means the marking[81] of stored personal data with the aim of limiting their processing in the future; [82]

(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; [83]

---

79 HU opposed the deletion of *restriction*.

80 FR reservation because of the broad scope of the definition. FR wanted to know if the mere presence of personal data implied automatic processing. DE wanted to reinsert *destruction* and add "blocking" instead of restriction. HU opposed the deletion of *destruction.*

81 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.

82 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

83 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[84] 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[85];

(7) 'processor' means a natural or legal person **(…)** [86] authority, agency or any other body which processes personal data on behalf of the controller[87]

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

[85] 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.

[86] Cion suggestion.

[87] 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[88] 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[89];
[90]

(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[91];

---

88 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.

89 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".

90 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.

91 Cion explained this definition featured already in the E-Privacy Directive. AT asked to clarify whether these breaches were limited to technical security breaches (Article 27) or also covered other personal data breaches. FR reservation: queried why the reference to third parties had been deleted. DK found the definition unclear. HU suggested the following changes to the definition: delete "security" and replace with "*the provisions of this Directive* leading to *any unlawful operation or set of operations performed upon personal data such as"* …because data breaches were not only linked to security breaches.

(10) 'genetic data' means all personal data, (…) relating to the genetic characteristics of an individual that have been inherited or acquired[92], resulting from an analysis of a biological sample from the individual in question[93];

(11) (...)[94];

(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[95];

[92] AT suggested to delete the text from *acquired.* For AT it was important that the genetic data was protected from the beginning of its existence. AT suggested an alternative(preferred) wording: "10. 'genetic data' means all personal data, of whatever type, concerning relating to the genetic characteristics of an individual that have been inherited or acquired, in view *of* an analysis of a biological sample from the individual in question which are inherited or acquired during early prenatal development"

[93] FR reservation. AT scrutiny reservation. AT worried that 'genetic data' and "biometric data" receive special protection. DE suggested adding "non coding DNA sequences are not regarded as genetic data". NO, SI wanted to delete the paragraph.

[94] PL remarked that biometric data could be used both to verify and to identify persons. CH, DE, SI and SE suggested to remove paragraph 11. CH and SE said that the Directive did not contain any other provision on processing of *biometric data*. Cion could accept to delete the definition.

[95] FR thought that the level of protection afforded to personal data should be proportionate to the importance thereof. CZ, DK, SE and UK thought the definition was too broad. Cion scrutiny reservation.

[(12a) 'profiling' means any form of automated processing of personal data intended to create or use a personal profile by evaluating personal aspects relating to an individual;[96]]

(…)

[97]

[96] Cion reservation. DE scrutiny reservation. FR, supported by NL, RO, suggested to use the definition in the CoE recommendation from 2010 on profiling. SI wanted either to use the definition in GDPR or the one in the CoE recommendation.

[97] 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.

(14) 'competent[98] (…) authority' means [99]any (...) public authority competent in each Member State for the prevention, investigation, detection or prosecution of criminal offences, [and for these purposes[100]],[101] safeguarding of public security or the execution of criminal penalties [102] or any body/entity[103] entrusted by national law[104] to perform public duties or exercise public powers for the purposes of prevention, investigation, detection or prosecution of criminal offences [and for these

---

98 DE scrutiny reservation.

99 DE thought that it might ne necessary to reword paragraph 14 once Article 1(1) had been agreed.

100 RO and UK suggested to delete *for these purposes.*

101 SE reservation to the deletion of the text in square brackets and that the Directive would be applicable also to private bodies. FR and RO supported SE on linking this question and the text in square brackets in this paragraph and Article 1.1. SE said that its position also meant that large parts of recital 11 would need to be removed.

102 Cion scrutiny reservation, linked to the authorities being covered by the definition. 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. IT thought that the definition could be improved by saying for example: "authority on which national legislation confers the competence to …" or "institutionally competent to…". BE suggested to add "and the prevention of danger." 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.

103 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.

104 UK, supported by CZ, 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.

purposes]safeguarding of public security or the execution *of criminal* penalties; [105]

[105] 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.

(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,[106] **, as well as Interpol.**

[107]

[108]

[106] Text from the GDPR as agreed by the JHA Council in June 2014. Addition of Interpol following DAPIX on 27.10.14

[107] CH suggested to add a definition of consent in line with the drafting in Article 4.8 in the draft 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.

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

CHAPTER II [109]

PRINCIPLES

Article 4

Principles relating to personal data processing[110]

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

(a) processed (…)lawfully and fairly;[111]

(b) collected for specified, explicit and legitimate purposes and only processed[112] in a way (…) compatible with those purposes[113];

---

[109] FI, PL, UK scrutiny reservation on Chapter II.. SI critical to Chapters I and II.

[110] 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. SE wanted that Articles 4 and 7 be elaborated together, maybe by transferring Article 7.2 to Article 4. SE raised concerns as regards the delimitation between the Directive and GDPR. SE asked what instrument would apply to courts dealing with (civil) torts arising from a criminal case. SE meant that Article 4 and Article 7.2 should be dealt with together

[111] 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 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.

[112] EE meant that *further processing* was the most complicated in this Article.

[113] 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.

(c) adequate, relevant, and not excessive in relation to the purposes for which they are processed[114];

(d) accurate and, where necessary[115],, kept up to date; (…)[116]

(e) kept in a form which permits identification of data subjects[117] for no longer than is necessary for the purposes **for which they are processed**;[118];

(ee) processed in a manner that ensures appropriate security of the personal data[119].

(…)

[120]

---

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

[115] EL, NL suggested to delete "where necessary".

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

[117] 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.

[118] DE queried about rules on archiving on judicial decision. 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. SE found that the scope for further processing was narrowed down with the addition of the reference to Article 1.1 and suggested to delete that reference. Also UK raised concerns about the reference to Article 1.1 and meant that it would cause difficulties for future investigations. Cion on the other hand accepted paragraph (e). SE suggested to replace the end of the paragraph with the words "for which they are processed", Cion accepted this wording.

[119] DE asked whether paragraph (ee) was purely declaratory or if it went further, if so it should be made clear.

[120] AT suggested the insertion of a new paragraph 1a with the following wording: "1a. Personal data shall be erased or made anonymous when they are no longer required for the purposes for which they were lawfully collected or are lawfully further processed. Archiving of those data in a separate data set for an appropriate period in accordance with national law shall not be affected by this provision." In addition AT pleads for the re-introduction of provisions along the lines of Article 4.3 and 4 of DPFD.

2. Further processing for another purpose[121] **according to paragraph 1(b)** shall be permitted in so far as: (a) it is not incompatible with the purposes for which the **personal** data was collected; (b) the competent authorities are authorised to process such **personal** data for such purpose in accordance with the applicable legal provisions; and (c) processing is necessary and proportionate to that other purpose. [122]

2a. To this end Member States shall set conditions in national legislation for communication 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.

[121] DE and SE appreciated that the introduction of text on processing for another purpose. 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 and noted that this did not only concern le 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 further 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.

[122] BE asked about the relationship between paragraph 2 and Article 7.2 and suggested to add the text from Article 7.2 to Article 4. BE archives. 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. HR welcomed the new text.

*3. Member States may [123] provide that the **competent authority** may,[124] further process personal data for historical, statistical or scientific purposes, subject to appropriate safeguards for the rights and freedoms of data subjects.*[125]

[126]

[123] AT, CZ, CY, DE suggestion "shall" was changed to "may".

[124] SE suggested to delete the reference to the purposes in Article 1.1.

[125] UK queried why processing for historical or scientific purposes was different regarding law enforcement from other investigations. In the same vein, IE asked how historical purposes could fall within the scope of Article 1.1. SE said that the reference to Article 1.1 made it impossible to use for statistical purposes, SE therefore suggested to delete that reference. UK shared the view that data in law enforcement should not be treated differently when it came to the purposes set out in Article 7.2 and the reference should therefore be deleted. FR wanted to delete paragraph 2. SE wanted to see *archives* mentioned explicitly. AT could accept paragraph 2 and pointed at Article 11 last part that refers to *anonymous* data. DE was critical to the reference to Article 1.1 since it meant that the use of police data for historical, statistical and scientific purposes was not the normal field of use but meant that such use should be set out in the Directive and not in GDPR. FI meant that the reference worsened the situation for data for historical/statistical and scientific purposes. Cion declared itself willing to look for solutions.

[126] HU suggested to add a new paragraph to Article 7 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."

4. The controller shall be responsible for compliance with paragraph 1, 2 **and 3**. [127]

[128]

[127] DE asked whether the amended text was meant to change the content. FR noted that the controller could not be responsible for further processing if it was not the controller him/herself who carried out the processing. To solve the problem, FR suggested to insert "by the data controller" after *processing* in the first line in paragraph 2. Cion accepted the FR suggestion.

[128] BE, CZ, EE, IE, NL, NO and UK wanted to insert a paragraph 3 with the following text from Article 3(2) DPFD: "3. Further processing for another purpose shall be permitted in so far as: (a) it is not incompatible with the purposes for which the data was collected; (b) the competent authorities are authorised to process such data for such purpose in accordance with the applicable legal provisions; and (c) processing is necessary and proportionate to that other purpose. The competent authorities may also further process the personal data transmitted by the competent authorities of other Member States for historical, statistical or scientific purposes, provided that Member States provide appropriate safeguards, such as making the data anonymous." CH supported the text until (c) and the text "to that other purpose". CH noted that the reference in paragraph (3) would in consequence be to "paragraphs "1 and 2". EE support for further processing for statistical purposes. FR favoured the insertion of a reference to historical/statistical or scientific purposes but queried about the links to Article 7.2 and wanted to ensure duplication of provisions. The Chair pointed to recital 20 concerning statistical purposes. Cion agreed with BE and FR also concerning the links to Article 7.2. SE supported the inclusion of the reference to "historical, statistical or scientific" purposes. IE wanted to add provisions permitting further processing in line with article 3.2 in DPFD; "competent authorities are authorised to process such data for other purpose in accordance with the applicable legal provisions" and "processing is necessary and proportionate to that other purpose".

129 DE suggested to insert a new Article 4a with the following wording:

"Article 4a

Rectification, erasure and blocking

1. Personal data shall be rectified if inaccurate
2. Personal data shall be erased or anonymised if they are no longer required for the purposes for which they were lawfully collected or for which they are lawfully being processed
3. Personal data shall not be erased but merely blocked if[129]

(a) there is legitimate reason to assume that erasure would impair the data subject's legitimate interests;

(b) they have been stored for the purposes of backing up data or data protection supervision[129], or

(c) the erasure would be technically feasible only with a disproportionate effort, for instance on account of the special nature of the storage

4. Without the consent of the data subject blocked data may only be processed for the purpose which prevented their erasure. They may, in individual cases, also be processed if, after weighing all the circumstances, the public interest in processing overrides the interest of the data subject standing in the way of the processing; in particular they may be processed, if this is essential for discharging the burden of proof 5.Appropriate time limits shall be established for the erasure of personal data or for a periodic review of the need for the storage of the data. Procedural measures shall ensure that these time limits are observed. ".

DE noted that data that had been blocked could not be erased. FI expressed a positive view on the DE text, in particular paragraphs 3(c) and 4.

130 AT suggested to add a new Article 4a along the lines of Article 4a in the Droutsas report:

"Article 4a

Access to data initially processed for purposes other than those referred to in Article 1(1)

1. Member States shall provide that competent authorities may only have access to personal data initially processed for purposes other than those referred to in Article 1(1) if they are specifically authorised by Union or Member State law which must meet the requirements set out in Article 7(1a) and must provide that:

(a) access is allowed only by duly authorised staff of the competent authorities in the performance of their tasks where, in a specific case, reasonable grounds give reason to believe that the processing of the personal data will substantially contribute to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

(b) requests for access must be in writing and refer to the legal ground for the request;

(c) the written request must be documented; and

(d) appropriate safeguards are implemented to ensure the protection of fundamental rights and freedoms in relation to the processing of personal data. Those safeguards shall be without prejudice to and complementary to specific conditions of access to personal data such as judicial authorisation in accordance with Member State law.

2. Personal data held by private parties or other public authorities shall only be accessed to investigate or prosecute criminal offences in accordance with necessity and proportionality requirements to be defined by Union law by each Member State in its national law, in full compliance with Article 7a."

Article 5

Distinction between different categories of data subjects[131]

(…)

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

Article 6

Verification of quality of data that are transmitted or made available[132]

1. Member States shall provide that the competent ~~(…)~~ authorities shall **take all reasonable steps to**[133] 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 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.[134]

2. If it emerges that that incorrect **personal** data have been transmitted or the data have been unlawfully transmitted, the recipient must be notified without delay. **In such case the personal** data must be rectified, erased or restricted **in accordance with Article 15**. [135]

---

132 HR found the text confusing and suggested dividing it in two parts. BE, CH, 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. IE, supported by SE, suggested to use language from DPFD; IE questioned the need to have the Article at all. AT in contrast accepted the reinsertion of an Article with that heading. NL noted that the text was more tightly drafted than in DPFD and seemed more binding. NL asked to whom the Article was addressed. ES considered that the competent authorities and not the MS were the addressees of the obligation CZ could accept the DE suggestion for cross-border cases. ES asked why paragraph 8.2 of DPFD was not inserted. FI thought that an Article on accuracy was needed but was not certain that current Article 6 fulfilled that requirement. NO wanted it to cover also domestic processing. Cion declared that they were not against the text of Article 8 DPFD.

133 Introduced at BE request. DE, ES, FR, IE, SI, UK and CH supported the text.

134 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.

135 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.

Article 7[136]

Lawfulness of processing[137]

1. Member States shall provide that the processing of personal data is lawful[138] only if and to the extent that processing is necessary[139]:

[136] 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, FR, HR and IE favoured the addition of consent. SI suggested to introduce a recital on consent. 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 reservation on consent. 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. 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.

[137] 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 are to be read, in particular the principle of purpose limitation. FR suggested to remove the Article due to a duplication with Article 4(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.

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

[139] CH, IE and UK wanted to provide for consent from the data subject, DK could consider it. IT and PT questioned the possibility of consent in the field of police work. FR reservation as regards consent. Cion confirmed that consent was not relevant in the field covered by the draft Directive. 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, based on Union law or Member State law[140], for the purposes set out in Article 1(1); or

(…) [141]

(c) in order to protect the vital interests[142] of the data subject or of another person[143]; or[144]

---

[140] 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.

[141] DE, FI, 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.

[142] 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.

[143] 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 to 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.

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

145

(d) for the prevention of an[146] immediate and serious[147] threat to public security[148].

149

150

[145] 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.

[146] IE asked whether it was possible to prevent an immediate threat and suggested, supported by HR, to replace "immediate" with "direct". CY, DE, DK, RO and UK suggested to delete "immediate", CY and RO to delete "serious" as well. DE considered that having both "immediate" and "serious" made the scope too narrow. CZ and SE suggested to replace "immediate" with "essential". ES suggested to replace "immediate" because this word is often misinterpreted and replace it with "direct" which is not temporal. For UK all threats to public security were important. Cion said that the text was standard wording in the acquis.

[147] IE meant that paragraph 1(d) was too narrow and therefore suggested to delete *immediate and serious* or to replace these words with *direct.*

[148] DE scrutiny reservation. DE said that the police must be able to take action even in the absence of imminent danger therefore "immediate and serious" should be deleted. SI reservation. BE wanted to know if this was a reference to classical police work or something else. SI considered that Article 7 could be seen as limiting police work. SI suggested to add a new paragraph (e) "similar tasks might be added for additional tasks". NL thought that paragraphs (c) and (d) might be superfluous since these tasks are an obligation of the state. AT meant that what would not be covered by paragraph (d) would be covered by paragraph (a).

[149] 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.

[150] HU suggested to add a new paragraph to Article 7 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."

151

Article 7a

Specific processing conditions ***152***

1. Member States shall provide that where[153] Union law[154] or the national law applicable to the transmitting competent **(…)** authority provides[155] specific conditions[156] (...) [157] to the processing of personal data,[158] the transmitting public authority shall inform the recipient to whom the data are transmitted about such conditions and the requirement to respect them.

2. Member States shall provide that the transmitting competent **(…)** authority[159] does not apply conditions[160] 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 [161].

162

---

151 BE suggested to create a Chapter IIA.

152 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. CH, EE, NL, SK, PL, PT and SK scrutiny reservation. FR and SE reservation. HR suggested to add that the data subject's consent could be a valid legal basis for the processing of their personal data.

153 BE suggested to replace *where* with *when.*

154 NL asked what was meant with EU law.

155 BE suggested to delete *for.*

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

157 NL asked to what *specific circumstances* referred.

158 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.

159 NL said that the notion of *transmitting authorities* was deviated from the language in the DPFD.

160 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.

161 CH suggested to replace the last part of paragraph 2 with the following words. "similar national data transmissions". For CH it was important that national transfers and Schengen transfers be regulated by the same conditions, CH therefore suggested to use the same formulation as in DFPD Article 12(2).

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

Article 8[163]

Processing of special categories of personal data

1. (…) [164] 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[165] or of data concerning health[166] or sex life[167] shall only be allowed[168] when strictly[169] necessary and (…) *the processing authorised by Union law or Member State law which provides appropriate safeguards*[170] *for the rights and freedoms of the data subjects.*

---

163 PL scrutiny reservation on Article 8. CZ, DK, SE and UK preferred the drafting of DPFD that was not formulated as a prohibition. DE found that an absolute prohibition on processing data in paragraph 1 was too far-reaching and impractical. UK generally preferred the drafting of the DPFD. DK meant that it was necessary to bring clarity to the text and further considered that it did not make sense to have a prohibition. 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 Article 8 had been aligned to Article 8 of the 95 Directive, *i.d.* as a prohibition and that it was important to maintain the same level of protection as in that instrument without lower the efficiency of the law enforcement authorities.

164 DE, supported by IE, wanted to replace "prohibit" with "restrict".

165 AT scrutiny reservation on genetic data. HR considered that it was necessary to further analyse the processing of genetic data. SI saw problems with genetic data as was the case in the GDPR.

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

167 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. DE, supported by PT, was against an absolute prohibition to process sensitive data. PT said that what is sensitive data was not an absolute notion. DE wanted to add "to the extent which is strictly necessary" at the end of the sentence. 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.

168 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.

169 SE reservation on *strictly* because it wanted to verify the consequences of this qualifier.

170 AT, DE and NL required examples of safeguards and EE, HR, 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.

(…)[171];

In exceptional cases **processing of such personal data as referred to in paragraph 1 may be carried out** when[172]:

(a) the processing is necessary[173] to protect the vital interests[174] of the data subject or of another person[175]; or

(b) the processing (…) is necessary for the prevention of an[176] immediate and serious[177] threat to public security [178]or

[179]

[171] SI and NL scrutiny reservation. CH considered the list of exceptions not sufficiently long, *e.g.* consent is missing or health. 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.

[172] SE asked whether *in exceptional cases* represented a stronger protection or an exception. HR found the drafting of this part of the Article imprecise.

[173] NL and SI inquired why "strictly" had disappeared from the text compared to Article 6 in DPFD. DE meant that it was still unclear what was meant with *appropriate safeguards*.

[174] 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".

[175] DE thought that paragraph 2(b) was too narrowly focused especially if the DE suggestion for paragraph 1 was not accepted.

[176] ES and UK wanted to replace "immediate" with "direct" and EE to delete it.

[177] IE meant that paragraph 1(d) was too narrow and therefore suggested to delete *immediate and serious* or to replace these words with *direct.*

[178] FR considered that points (a) and (b) could be deleted because they only confuses matters and that the reference to national law and EU law in the *chapeau* was enough.

[179] 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 suggested to insert a paragraph with the following wording: "(d) the data subject has given his explicit consent". Support from CH, DK, HU, IE and HR . 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]

[(…) Profiling (…)[180]

1. Member States shall provide that a decision based solely[181] on profiling which produces an adverse legal effect[182] for the data subject or severely affects[183] him or her (…) shall be prohibited unless authorised by Union or Member State law[184] to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject (…).]

_____

[180] RO suggested to define "profiling" and move the Article to Chapter III, support from CZ, EE, IT, FI, SI, SE to define "profiling". DE, ES, IT, SI entered scrutiny reservations. SE serious doubts about the Article. Cion reservation. DE meant that it was necessary to determine if Article 9 in its current form is covered by the legislative competence of the EU. CZ said that since there was no final agreement on the text on profiling in the GDPR it was not possible to decide the text for the Directive.

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

[182] EE asked who would assess the adverse legal effect and how.

[183] SI wanted to remove *severely affect* .

[184] FR wanted to know why the reference was to "a law" and not the generic "by law". FR, IT, PT and UK preferred *by law*, here as well as in the rest of the Directive.

ANNEX I

CHAPTER V

TRANSFER[185] OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS[186]

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

[186] AT, BE, CH, CZ, CY, DE, DK, EE, FI, FR, IT, NL, NO, PL, PT, RO, SI, UK scrutiny reservation on Chapter V. ES reservation on Chapter V. DE questioned whether the core concept in Chapter V was appropriate and adequacy danger. 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 (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 sequancing of the transfer in Chapter V should 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 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.

Article 33

General principles for transfers of personal data [187]

1. Member States shall provide that any transfer of personal data by competent **(…)** authorities (…) to a third country, or to an international organisation[188], including further onward transfer to another third country or international organisation, may take place only if:[189][190]

[187] PT wanted to see more safeguards in Article 34. The Chair indicated that the equivalent Article had been deleted in the GDPR. AT, FI and PT were against a deletion of Article 33 because the content of Article 13 in DPFD would not be covered. SI was sceptical about the deletion. In contrast BE, CZ, SE supported the deletion. CH, FR entered scrutiny reservations on the possible deletion of Article 33. DE said that the Article did not set out criteria for striking the right balance between data protection and investigation and prosecution of crime. DE criticized that the Directive was drafted in a way that it was not possible to know what was the main rule and which were the exceptions. EE, PL, SE, SI and UK welcomed DE comments about the right balance between data protection and combating crime. DE scrutiny reservation because the scope remained controversial. SE asked how the different Articles in Chapter V were linked and AT how Chapter V fitted into the overall scheme. 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); The relation to Article 36 and 36a was not clear (a reference to Article 36 should be added in point(e) or (e) could be rephrased, in addition a reference to Article 36a should be added in point (d), a possibility to impose a deadline for the Member State from which personal data originated to give its prior authorization should be considered); CZ could also consider copying Article 13 in DPFD. ES meant that the approach of this article was misleading because it looked like international transfers were only possible on the basis of an adequacy decision or appropriate safeguards. ES said that this approach was clearly compromised by Article 36 and ES preferred a more realistic approach. 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.

[188] FR asked for clarifications as to which organisations were intended. BE meant that the role and status of international organisations should be clarified. Cion accepted to clarify the meaning of *international organisation.* FR asked about the relationship between this Directive and those organisations' specific rules on data protection.

[189] 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

[190] 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 [191] criminal offences [and for these purposes], safeguarding of public security, or the execution of [192] criminal penalties; [193] and[194]

(b) (…)

(c) the controller in the third country or international organisation[195] is an authority[196] competent for the purposes referred to in Article 1(1); and

(d) in case personal data are transmitted or made available from another Member State,[197] that Member State has given its prior authorisation[198] to the transfer[199] in compliance with its national law[200]; [201] and

---

191 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.

192 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.

193 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. CZ wished to insert a reference to Article 1(1) in paragraph (a) as had been done in paragraph (c).

194 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.

195 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 and that Interpol should be covered. FI suggested to use *intergovernmental organisation* in accordance with the Vienna Convention on the Law of Treaties. FI thought that the organisations should be set out here, *i.d.* Interpol or that it be made clear in the recitals that Interpol was covered.

196 DE suggested to delete paragraph (c) and 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.

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

198 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 FDDP.

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

200 EE thought that paragraph (d) should be linked to Article 36a.

201 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[202] that the third country or international organisation[203] 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 [204] 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.

[205]

---

[202] AT meant that it was necessary to make a reference to all types of transfer provided for in Chapter V, including Article 36 in order to make it clear that the general basic principles set out in Article 33 (particularly points (c) and (d)) are also fully applicable to transfers referred to in Article 36. Support from FR to mention Article 36.

[203] FR asked for clarifications as to which organisations were intended. BE meant that the role and status of international organisations should be clarified. Cion accepted to clarify the meaning of *international organisation.* FI thought that paragraphs (c) and (e) needed to be fine tuned and that Interpol should be covered. FI suggested to use *intergovernmental organisation* in accordance with the Vienna Convention on the Law of Treaties. FI thought that the organisations should be set out here, *i.d.* Interpol or that it be made clear in the recitals that Interpol was covered.

[204] 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 meant that, in line with Article 34, a territory or specified sector within a specific third country should be mentioned in paragraph (e). DE wanted to add "or where the personal data are transferred in accordance with Article 36" in the end of paragraph (e) to clarify that Article 36, as well as Articles 34 and 35 can serve as grounds for data transfer.

[205] 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. 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*** [206] *for the prevention of an immediate*[207] *and serious threat to public security of a Member State or a third country or to essential interests*[208] *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.*[209]

---

206 UK preferred "necessary" to "essential".

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

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

209 Moved from Article 36a

Article 34

Transfers with an adequacy decision [210]

1. Member States shall provide that a transfer[211] of personal data to a (...) third country or a territory or one or more specified sectors within a third country or an international organisation may take place where the Commission has decided in accordance with Article 41 of Regulation (EU) …./2012 or in accordance with paragraph 3 of this Article that the third country or a territory or specified sector[212] within that third country, or the international organisation[213] in question ensures an adequate level of protection[214]. Such transfer shall not require any specific authorisation. [215]

---

[210] DE scrutiny reservation. 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. ES considered that consistency between the text of GDPR and Article 34 must be ensured so that the adequacy functioned in an equivalent manner. 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.

[211] BE and FR suggested to talk about "any transfer or set of transfer".

[212] 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.

[213] FR thought that the *international organisations* could be deleted in this paragraph.

[214] 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.

[215] BE asked whether the individual MS could have 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. Where no decision adopted in accordance with Article 41 of Regulation (EU) …./2012 exists, the Commission [216] shall[217] assess the adequacy of the level of protection, giving consideration 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 (…)[218] including concerning public security, defence, national security and[219] criminal law as well as (…) security measures, including rules for onward transfer of personal data to another third country or international organisation,[220] which are complied with in that country or by that international organisation; as well as the existence of effective and enforceable data subject rights and effective administrative and judicial redress for data subjects (…) whose personal data are being transferred; [221]

(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[222]; and

---

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

217 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.

218 DE preferred the Cion text, deleting "data protection rules" and adding "in force, both general and sectoral" after *relevant legislation.*

219 DE wanted to delete *and.*

220 DE preferred the text in the Cion proposal, that is deleting the underlined text from *including* to *organisation.*

221 Cion meant that the equivalent text to Article 34.1(a) was clearer in the GDPR (Article 41.2(a).

222 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 [223] in relation to the protection of personal data. [224]

[225]

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 sector**s** 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). [226]

4. (…)

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

---

[223] DE also here wanted a broader assessment, like in paragraph (a) and therefore suggested adding *especially* before *in relation.* FR asked whether it might not be worth including the agreements and international conventions to which the Union is party, because they must as least be presumed having an adequate level of protection, *e.g.* CoE Convention 108.

[224] DE asked what protection level must be kept. Cion reservation.

[225] DE wanted to add the following text: "The Commission shall, as early as possible, give the Member States the opportunity to comment on each adequacy assessment." because it wanted the MS to be able to comment early in the process.

[226] NL wanted to know how this paragraph would be applied. CZ meant that paragraph 3 should include a duty for the Commission to seek opinion of the EDPB and thought that the role of the EDPB should be the same as in the GDPR. CZ wanted that Paragraph 3 should include possibility of Member States to adopt adequacy decision as well (Article 13 in DPFD.

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[227] 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.[228] 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)[229]. 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.[230]

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[231] and 36 (…).[232]

---

227 AT suggestion.

228 AT suggestion. FR thought that it could be made clearer that the repeal of adequacy decisions were based on monitoring by the Cion, as is provided in paragraph 4a and that it is only if the third country changes its legislation or its practice.

229 DE saw no need for an immediately applicable implementing acts and therefore suggested to delete the text after *57(2)*until *57(3).*

230 BE, CH, CZ, DE, FR, NL, SE welcomed the Chair's suggestion to remove paragraphs 5 and 6 on the blacklist. HU preferred the text of the GDPR and the obligation for the Cion to request the opinion of the EDPB and take its opinion into account. CZ meant that paragraph 3 should include a duty of the Commission to seek opinion of the EDPB. CZ wanted that Paragraph 5 included possibility of Member States to adopt adequacy decision as well. ES found it advisable to better assess what impact this may have on the basis of arts. 35 and 36. ES asked if a decision based on this paragraph would prevent, in general terms, a transfer based on Articles 35 and 36. ES would not be in favor of granting the Commission an indirect way to constraint transfers based on Articles 35 and 36.

231 AT said that if a negative adequacy decision had been taken, a transfer under Article 35 could not be envisaged so therefore should the reference to Article 34 be deleted.

232 PL asked how paragraph 6 was linked to a situation where no adequacy decision existed. PL also asked if the controller could set up additional requirements. NL did not see any added value of this paragraph and suggested to delete it or making a link to the EDPB.

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 **1,** 3 and 5.[233]

8. (…)

Article 35

Transfers by way of appropriate safeguards[234]

1. (…)Member States shall provide that, in the absence of a decision pursuant to paragraph**s 1 and** 3 of Article 34, a transfer[235] of personal data to a third country or an international organisation may take place where:[236]

[233] 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.

[234] 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 queried whether INTERPOL fell within the scope of Article 35 and 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. Cion said that *Interpol* would be falling under both paragraphs 1(a)and (b).
BE meant that in order to preserve the coherence between this proposal and the proposal of Regulation on the establishment of the European Public Prosecutor's Office, BE would like to give the possibilities to MS to exchange the information via INTERPOL on the same conditions as those provided in art 54 of that Regulation ("Personal data shall only be transferred by the European Public Prosecutor's Office to third countries, international organizations, and Interpol if this is necessary for preventing and combating offences that fall under the competence of the European Public Prosecutor's Office and in accordance with this Regulation.")

[235] To align with the GDPR. BE asked to replace *transfer* with *any transfer*. FR preferred to use the plural, *transfers* to make it possible to set up channels for regular and routine data exchange. . IE said that Article 35 and 36 should apply to a category of transfers as well as to a single transfer (Article 44 of GDPR).

[236] AT wanted to reinsert the Cion initial text for the *chapeau.*

(a) appropriate safeguards[237] with respect to the protection of personal data[238] have been adduced in a legally binding and enforceable instrument [239]; or

(b) the controller (…) has assessed all the circumstances[240] surrounding [241] the transfer of personal data [242] and concludes that appropriate safeguards exist with respect to the protection of personal data. **Such an assessment may take into account the agreements in place between EUropol and Eurojust and third countries, as well as it may refer to the adequacy assessment carried out pursuant to Article 13.1 (d) of Framework Decision 2008/ 977/ JHA.**data. [243]

2. **(…)** [244]

[237] HU asked what appropriate safeguards was and meant that it could not be a uniform compliance here.

[238] 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),"

[239] 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.

[240] 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.

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

[242] 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),"

[243] NL had doubts about the need to keep Article 36.1(b). NL, AT, HU and RO 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.

[244] Deleted. Article 23 will be redrafted to cover this requirement.

Article 36

Derogations for transfer in specific situations[245]

1. (…) Member States shall provide that, in the absence of an adequacy decision pursuant to Article 34 or appropriate safeguards pursuant to Article 35[246], a transfer or a category of transfers[247] of personal data to a third country or an international organisation may take place only on condition that[248]:

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

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

---

245 UK and CZ asked why the derogations could not be set out as permissions and be further specified. Likewise, DE welcomed this but considered that they should not be set out as derogations. DE also saw the need for complementing the list. NL saw the need for a better balance. ES and UK did not approve of the title of the Article. NL considered that the EDPB should ensure consistency. CZ thought that it could be good to transfer data to a natural person in a third country and suggested to add text to this effect.. DE wanted to change the title to "Transfers after weighing of interests" to take account of the interests existing in practice that is data protection interests and *e.g.* the public interest of preventing and solving crimes. AT found tht the wording of Article 36, in particular points (c) to (e) was too broad and preferred to revert to the wording of Article 13(3) of DPFD that takes account of the derogations of Article 2 of the Additional Protocol to CoE Convention 108. AT thought that Article 36 should stipulate clearly that legislation is to provide for such transfers on the basis of *prevailing* public interests.

246 AT suggestion.

247 To align with the GDPR.

248 DE suggested to draft the *chapeau* in the following way, in line with Articles 34 and 35, to indicate that Article 36 was on equal footing with Articles 34 and 35 and should not only set out derogations: "1.(…) Member States shall provide that, a transfer of personal data to a **recipient or recipients in a** third country or an international organisation may take place ". DE used *recipient* to indicate that transfers also could go to private bodies.

(c) the transfer of the data is necessary [249] for the prevention[250] of an immediate[251] and serious threat to public security of a Member State or a third country; or

(d) the transfer is necessary[252] in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences [and for these purposes], safeguarding of public security or the execution of criminal penalties; or[253]

(e) the transfer is necessary[254] in individual cases[255] for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection [and for these purposes], safeguarding of public security or prosecution of a specific criminal offence or the execution of a specific criminal penalty. [256]

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."[257]

---

249 UK suggestion.

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

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

252 CZ wanted to exchange *necessary* to *essential* as in paragraph (c) or *required* because the meaning of necessary was unclear.

253 CZ asked what documents would be needed for *e.g.* an EAW being transferred to Interpol.

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

255 UK feared that *individual cases* could be interpreted narrowly and therefore suggested to delete these words and explain in the recitals.

256 PL suggested that the *chapeau of the Article* and paragraphs (a) to (e) would form Article 36(1)

257 DE suggestion.

258

259

Article 36a

(…)

Article 37

Specific conditions for the transfer of personal data

(…)

258 DE 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 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).

259 Previous paragraph 2 has been deleted for the same reasons as for Article 35(2), that Article 23 will be redrafted to cover this requirement.

Article 38

International co-operation for the protection of personal data[260]

(…)[261]

CHAPTER X

FINAL PROVISIONS

Article 60

Relationship with previously concluded international agreements in the field of judicial co-operation in criminal matters and police co-operation[262]

---

260 Cion scrutiny reservation against deletion. DE wanted to reinstate Article 38 with a new paragraph (b) with the following wording: " provide the exchange of insights in the level of protection in third countries; this in particular includes the Member States being notified by the Commission of the progress on and the outcome of assessments in accordance with Article 41 of Regulation (EU) ..../2012 and Article 34(2) and (3) of this Directive;" DE added "in the development and" after *mutual assistance* in paragraph (c) first line. In paragraph 2, DE added "supervisory authorities" and the Commission in the first line and deleted the end of the sentence after *supervisory authorities,* in the third line.

261 ES meant that if this article 38 was to be removed it could only be on the basis that within the GDPR the international cooperation is covered with an extensive view and with the scope of this directive included.

262 CH and DE scrutiny reservations. For the UK and CZ Article 60 as it was drafted here was unacceptable. SI said that DPFD was more acceptable and that the text contained no element of flexibility. FR requested the insertion of a grandfather clause, in order to preserve the MS operational exchange channels. FR recalled the link between Article 60 and Chapter V. FR pointed in particular to the fact that the simultaneous promotion of strict rules in Chapter V and the obligation to denounce agreements pursuant to Article 60 would lead to the prohibition of data exchanges which are essential for legitimate public interest aims.
CZ and FR noted that there were no time limits/transition periods foreseen, which entails a more immediate obligation for the MS to denounce and renegotiate their "non-compliant" agreements. FI found the text very ambiguous. For AT the core problem was the dependence on the relevant third countries and that it remained unresolved despite that the-year period for the renegotiation of agreements no longer applied. AT meant that the aim should still be to adapt as soon as possible agreements that do not conform to the provisions of the Directive. AT suggested that intermediate solutions be set out in a recital.

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to the entry into force of this Directive and which are in compliance with Union law applicable prior to the entry into force of this Directive shall remain [263]in force until amended, replaced or revoked.[264]

_____

[263] BE, supported by CZ, suggested to add "unaffected." and delete the rest of the text of the paragraph so that Article 60 is in line with Article 59 in fine. FR could alternatively agree the Article in line with the BE/CZ suggestion to delete the last sentence. ES could accept the current wording but preferred the deletion of the second sentence. PL supported the deletion of the second sentence of the Article. BE asked it to be clarified what would happen if the Cion withdraw an adequacy decision, would the MS need to renegotiate the agreement. CZ said that first sentence provided for *lex specialis* as regards these agreements, the second sentence was therefore not necessary, it was even contradictory. CZ said that such agreements may well be amended and then the amended wording will remain in force; it could even be said that this is the usual result of amending something, at least in the area of international law.

[264] AT considered the Article inflexible. CY scrutiny reservation. BE, CH, IT and CZ objected Article 60. CH asked what would happen when there it was need to revoke the agreement but that another Party to the agreement would refuse to renegotiate it. Cion reservation. DE suggested to reword Article 60 as follows: "International agreements involving the transfer of personal data **processed by competent authorities for the purposes referred to in Article 1(1)** to third countries or international organisations which were concluded by Member States prior to the entry into force of this Directive shall remain **unaffected. To** the extent that such agreements concluded by Member States are not compatible with **this Directive**, the Member State or States concerned shall **make** appropriate **efforts** to eliminate the incompatibilities established." DE aligned the first sentence to Article 59 and clarified that existing agreements did not need to be renegotiated.