Council of the European Union

Brussels, 14 April 2015
(OR. en)

7740/15

Interinstitutional File: 2012/0010 (COD)

LIMITE

DATAPROTECT 44
JAI 218
DAPIX 53
FREMP 70
COMIX 158
CODEC 457

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	15391/14 DATAPROTECT 164 JAI 859 DAPIX 166 FREMP 201 COMIX 603 CODEC 2221
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 and II

The Presidency is suggesting to discuss the scope of the Directive as well as Chapter II at the DAPIX meeting on 20 April 2015.

The Data Protection Directive is part of a data protection package consisting of the Directive and the General Data Protection Regulation.

The scope of the Data Protection Directive was discussed at DAPIX the last time in November 2014. The Italian Presidency had put forward three options for a possible scope. It concluded that most delegations were in favour of an extended scope of the Data Protection Directive and of the suggested wording in its Article 1(1). The scope of the two instruments in the package is mutually exclusive: extending the scope of the Data Protection Directive to subject matters that are currently covered by the scope of the General Data Protection Regulation reduces the scope of the Regulation to the same extent.

At the informal Ministerial Meeting in Riga in January 2015 the delimitation of the scope of the Directive and the Regulation was discussed on the basis of the text that most delegations had approved in the end of 2014. Ministers informally confirmed to extend the scope of the Directive to also cover 'maintaining law and order and the safeguarding of public security'. Also Ministers suggested that examples of the activities that would be covered by the Directive be set out in recital. The Presidency has therefore added a number of examples that are set out in recital 11a.

Delegations are asked to confirm the wording of Article 1(1) and the corresponding recitals 11 and 11a as amended.

At its meeting on 13 March 2105 the Council reached a partial general approach on Chapter II of the General Data Protection Regulation. In light of that partial general approach, the Presidency has inserted the changes that it sees appropriate in the Data Protection Directive.

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

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 as well as for the purposes of maintaining law and order and the safeguarding of public security, as well as the free movement of such data[1]

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

After consulting the European Data Protection Supervisor[2],

Acting in accordance with the ordinary legislative procedure,

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

[2] OJ C… , p.

Whereas:

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

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

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

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

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

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

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

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

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

(9) On that basis, Regulation EU …../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.

---

4 OJ L 350, 30.12.2008, p. 60.

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

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

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

---

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

7 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 **authorities** are mainly focused on the prevention, investigation, detection or prosecution of criminal offences **for example police activities without prior knowledge if an accident is a criminal offence or not. However,** the activities **performed by the above-mentioned authorities** also include **maintaining law and order when performing functions characteristic exclusively to the police and the safeguarding of public security which in each Member State should be considered as tasks** aimed at preventing human behaviour which may lead to threats to fundamental interests of the society **protected by the law, is contrary to social values and customary norms of society** and which may lead to a criminal offence. **A competent authority is allowed to take coercive measures in the context of such activities, for example police activities at demonstrations and major sporting events**[8].

Agencies or units dealing especially with national security issues should not be considered as law enforcement authorities.

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] [10] [11]

---

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

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

10 AT, FI, IE scrutiny reservation on recital 11a. Cion reservation.

11 BE found that the clarifications of *public security* was too narrow and said that salubrity and peacefulness belong to the areas of activity of the police in Belgium and should therefore be covered.

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

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

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

12 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.

(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[13] concerning national security, taking into account Articles 3 and 6 of the Treaty on the Functioning of the European Union, nor[14] to data processed by the Union institutions, bodies, offices and agencies, such as Europol or Eurojust. [15]

(15a) Regulation (EC) No 45/2001[16] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal instruments applicable to such processing of personal data should be adapted to the principles and rules of Regulation EU …../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. [17]

---

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

14 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.

15 AT did not find recital 15 clear.

16 OJ L 8, 12.1.2001, p. 1.

17 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. [18]
[19]

(16a) Genetic data should be defined as personal data relating to the genetic characteristics of an individual which have been inherited or acquired as they result from an analysis of a biological sample from the individual in question, in particular by chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained.[20]

(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.

---

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

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

[20] SE expressed concerns with recital 16a because of DNA profiles 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.[21]

(19) For the prevention, investigation and prosecution of criminal offences it is necessary for competent (…) authorities to (…) process personal data, collected in the context of the prevention, investigation, detection or prosecution of specific[22] criminal offences beyond that context to develop an understanding of criminal phenomena and trends, to gather intelligence about organised criminal networks, and to make links between different offences detected.

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 **archiving purposes in the public interest or**[23] scientific, statistical or historical purposes should not be considered as incompatible with the original purpose of processing. Personal data should be adequate, relevant and not excessive for the purposes for which the personal data are processed. (…). Personal data which are inaccurate should be rectified or erased.[24]

---

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

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

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

24 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. SE supported ES and pointed out that the purpose of court proceedings in criminal matters was to establish what is true and false and that judgements cannot be corrected.

(21) The principle of accuracy of data should be applied taking account of the nature and purpose of the processing concerned. Since personal data relating to different categories of data subjects are processed, *the competent public authorities (…) should, as far as possible*[25], *make a distinction between personal data of different categories of data subjects such as persons convicted of a criminal offence, suspects, (…)victims and third parties.*[26] In particular in judicial proceedings, statements containing personal data are based on the subjective perception of individuals and are in some cases not always verifiable. Consequently, the requirement of accuracy should not appertain to the accuracy of a statement but merely to the fact that a specific statement has been made.

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

(23) (…).[27]

(24) (…) The competent (…) authorities should (...) ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. In particular, personal data should be distinguished, as far as possible, according to the degree of their accuracy and reliability; (…) facts should be distinguished from personal assessments in order to ensure both the protection of individuals and the quality and reliability of the information processed by the competent (…) authorities. [28]

---

[25] CZ suggested to replace *possible* with *relevant.*

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

[27] Deleted since Article 5 was deleted. ES, DK and SE suggested deleting recital 23 since Article 5 was deleted. Cion reservation on deletion. Cion said that both the Europol Convention and the Eurojust Regulation have an Article on the requirement of making a distinction of the different categories of data.

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

(25) In order to be lawful, the processing of personal data should be necessary for (…) the performance of a task carried out in the public interest by a competent (…) authority based on Union law or Member State law for the purposes of prevention, investigation, detection or prosecution of criminal offences *or the execution of criminal penalties* **as well as for the purposes of maintaining law and order and the** safeguarding of public security. Processing by a competent (…) authority should also be lawful, where the processing is necessary or in order to protect the vital interests of the data subject or of another person, or for the prevention of an immediate[29] and serious threat to public security[30]. The performance of the task of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent authorities allows them to require/order individuals to abide to the requests made. In this case**,** the data subject's consent (as defined in Regulation **XXX)**[31] should not provide a legal ground for processing personal data by competent (…) authorities. Where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the data subject's reaction could not be considered as a freely-given indication of his or her wishes. This should not preclude Member States to provide by law, for example, that an individual could be required for example to agree to the monitoring of his/her location as a condition for probation or expressly authorize processing of data which can be particularly invasive for his/her person, such as processing of special categories of data**.**[32]

---

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

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

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

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

(25a) Member States should provide that where[33] Union law or the national law applicable to the transmitting competent (…) authority provides for[34] specific conditions applicable in specific circumstances to the processing of personal data,[35] such as for example the use of handling codes the transmitting (…)authority should inform the recipient to whom data are transmitted about such conditions and the requirement to respect them. Such conditions may for example include that the recipient to whom the data are transmitted does not inform the data subject in case of a limitation to the right of information without the prior approval of the transmitting authority. These obligations apply also to transfers to recipients in third countries or international organisations. Member States should provide that the transmitting competent **(…)** authority does not apply conditions pursuant to paragraph 1[36] to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters IV and V of Title V of the Treaty on the Functioning of the European Union other than those applicable to similar national data transmissions.[37]

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

(26) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights (…) and freedoms, including genetic data, deserve specific protection. 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[38] 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[39] 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[40]**.** However, the agreement of the data subject should not provide in itself a legal ground for processing such sensitive personal data by competent **(…)** authorities. [41]

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

---

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

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

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

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

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 the

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

[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.

[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. NO said that private enterprises could be involved in this area, *e.g.* as processors. Cion said that the Directive was only applicable to competent (public) authorities carrying out activities listed in paragraph and where the same activities were carried out by a private enterprise the Regulation was applicable (see Article 21 and recital 16 in GDPR)this was in line with the Treaty.. The Cion indicated that the DPD was applicable to courts for criminal matters whereas for other courts the Regulation would be applicable.

[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. 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.

prevention[47], investigation[48], detection[49] or prosecution[50] of criminal offences *or the execution of criminal penalties*[51] as well as for **the purposes of** maintaining law and order and the safeguarding of

---

47 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. BE, NL and NO wanted that all activities of the police be covered by the Directive, BE and NL also administrative tasks. AT mentioned that all police activities should not be covered for example administrative tasks, food stuff/first aid or traffic police should not be covered. DE wanted that threat prevention by the police be covered by uniform provisions.

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

49 PL suggested to add "of crime and perpetrators".

50 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.

51 BE, DE, ES, FI, FR, PL and SE, queried whether this Directive would cover court proceedings (also valid for Article 3(14) and if so to what extent. The Chair explained that courts are covered and that recital 55 had been changed to make this explicit. ES did not want the Directive to cover court activities. RO, supported by CZ, wanted to add "and ensuring public order and security". 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". 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). The underlined text should be added to the list of areas in Article 2 (e) of the GDPR upon which t that Regulation will not apply. DE said that the wording came from Articles 72.2 and 87.1 from TFEU.

public[52] security.[53]

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

[53] DE suggestion. DE mentioned that activities of the border police, activities linked to aviation security, police activities at demonstrations should be covered.SE preferred the previous text keeping the links to combating crime and that without this link the scope risked to be too extensive. SE thought that *prevention* could cover a broad scope such as law and order. Cion accepted to work on the notion of *prevention of a criminal offence.* CZ raised concerns about the GDPR being used by omission. DE asked how the idea of *safeguarding public security* could be reformulated and hinted to the RO suggestion in doc 8208/13. For NL and RO *internal security* needed to be clarified in a recital. FR, supported by FI, NL, NO, CZ and CY and with the acceptance of DE, suggested to replace *internal security* with *public security*. For FI using *public security* was acceptable and said that it was if not defined at least use in secondary legislation such as the Prûm Decision. AT, supported by FI, said that the notion of *public security* must be made clear. NL did not see any problems with *law enforcement services.* In contrast AT feared that *other law enforcement services* was too far reaching especially since private bodies would be included in the scope. RO, supported by CY and EE suggested to refer to *law enforcement authorities* instead of *services.* RO wanted to refer to *public* order instead of *public security.* HR and UK wanted it to be set out in the body of the text that intelligence activities be excluded from the scope. MT and SI asked what was meant with *law and order.* HU wanted that the Directive cover all kinds of crimes, also petty crimes but not administrative sanctions. NO suggested to talk about *police tasks* or define the scope negatively so as to exclude administrative tasks. Cion reservation on DE suggestion. Cion said that if public security would be introduced without being linked to criminal offences, areas that were currently covered by the 1995 Directive would be covered by the Directive which would lead to a lower level of protection, a situation that the Cion could not accept. Cion suggested to keep the previous text and explain and clarify the notion of *public security* in a recital. Cion found that the DE suggestion introduced imprecisions, *e.g. internal security* and *maintaining law and order*. EE also meant that the law enforcement services should only be covered by one instrument. Cion indicated that there were 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 either 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 previous text 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. 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

1a. This Directive shall not preclude Member States from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent (…) authorities.[54]

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

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

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. EE asked if for example environmental offences would be covered. EE and CH did not find that the Directive should cover courts and judicial bodies. CZ meant that public order should be maintained for other reasons than prevention etc. of criminal offences. SE meant that public security was a difficult notion and too broad a notion, especially if private bodies would be included in the scope. 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. UK found the notion of public security uncertain. Cion preferred *public security* because it was a well-known notion in the acquis and was an autonomous definition.

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

(b) ensure that the exchange of personal data by competent (…) authorities within the Union, where such exchange is required by Union or national law, is neither restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.[55] [56] [57] [58] [59] [60]

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

[56] SK suggested to reformulate this paragraph as follows: "not restrict nor prohibit the exchange of personal data by competent authorities within the Union if individuals data protection is safeguarded". SE meant that the balance between individuals' integrity and security needed to be ensured and that aspect was not yet sufficiently clear in the current text.

[57] IT and SI queried the interaction with other fundamental rights and referred to the need to protect attorney-client privilege. CH suggested to insert a recital to clarify that MS could foresee more restrictive provisions with regard to the purpose for which data could be used.

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

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

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

Article *2*

Scope [61]

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

2. This Directive applies to the processing of personal data wholly or partly by automated means[63], 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.[64]

---

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

[62] 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.

[63] 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,".

[64] 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[65]; (…)[66] [67];

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

---

65 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.

66 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.

67 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[68].

[69]

[68] 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.

[69] 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[70]

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[71], in particular by reference to an identifier such as a name, an identification number, location data, online identifier[72] or to one or more factors specific to the physical, physiological, genetic[73], mental[74], economic, cultural or social identity of that person.[75];

(…)

---

70 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.

71 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".

72 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.

73 FR reservation.

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

75 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 (…)[76] erasure or (…)[77];

(4) 'restriction of processing' means the marking[78] of stored personal data with the aim of limiting their processing in the future; [79]

(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; [80]

---

[76] HU opposed the deletion of *restriction.*

[77] 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.*

[78] 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.

[79] 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

[80] 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[81] 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[82];

(7) 'processor' means a natural or legal person (…) [83] authority, agency or any other body which processes personal data on behalf of the controller[84];

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

[82] 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.

[83] Cion suggestion.

[84] 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[85] 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[86];
[87]

(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[88];

---

85 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.

86 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".

87 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.

88 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[89], resulting from an analysis of a biological sample from the individual in question[90];

(11) (...)[91];

(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[92];

[89] 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".

[90] 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.

[91] 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.

[92] 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 **consisting of using those data to** (…) evaluat**e** personal aspects relating to an individual;[93]]

(…)

94

93 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.

94 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[95] (…) authority' means [96]any (...) public authority competent in each Member State for the prevention, investigation, detection or prosecution of criminal offences *or the execution of criminal penalties as well as the maintaining of law and order and the safeguarding of public security* [97] or any body/entity[98] entrusted by national law[99] to perform public duties or exercise public powers for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

---

95 DE scrutiny reservation.

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

97 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. 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.

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

99 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.

100

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

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

(16) 'international organisation' means an organisation and its subordinate bodies governed by public international law or any other body which is set up by, or on the basis of, an agreement between two or more countries,[101], as well as Interpol.[102]

[103]

[104]

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

[102] DE preferred *including* instead of *such as.*

[103] 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.

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

CHAPTER II [105]

PRINCIPLES

Article 4

***Principles relating to personal data processing*[106]**

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

(a) processed lawfully *and fairly*;[107]

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

[106] 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. NL suggested to merge Article 4 and 7.

[107] HU suggested to add "and to the extent and for the duration necessary to achieve its purpose" in the end of paragraph (a) or add a new paragraph (bb) "processed only to the extent and for the duration necessary to achieve its purpose.". EE and SE scrutiny reservation on the reinserting of *fairly*. DE and HR opposed to the reinsertion of *fairly*. IE, supported by SI, saw problems in reinserting *fairly* and pointed to covert police investigations that would not be possible then. SI meant that future proceedings would be influenced and meant that *fairly* had nothing to do in Article 4. CY asked whether it was feasible to ensure fairness. HR meant that *fairly* was inherent to the criminal procedure as a whole so it did not give any added value to the text. HR thought that in the case of transfer of inaccurate or illegal data the person should be notified and inaccurate data deleted or its dissemination ceased. FR and NL and Cion on the other hand welcomed *fairly* and FR saw no problems with police activities if the term was reinserted.

(b) collected for specified, explicit and legitimate purposes and only processed in a way (…) compatible with those purposes[108];

(c) adequate, relevant, and not excessive in relation to the purposes for which they are processed[109];

(d) accurate and, **(…)**[110], kept up to date; (…)[111]

(e) kept in a form which permits identification of data subjects[112] for no longer than is necessary for the purposes for which **the personal data** are processed;[113];

---

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

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

110 EL, NL and MT suggested to delete "where necessary".

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

112 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.

113 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. BE suggested to add *or further processed* in the end of the paragraph.

(ee) processed in a manner that ensures appropriate security of the personal data[114].

(…)

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.[115]

[116]

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

[115] Inserted at the AT and CH request.

[116] (…). AT pleaded for the re-introduction of provisions along the lines of Article 4.3 and 4 of DPFD.

2. Further processing **by the same controller**[117] for another purpose[118] shall[119] be permitted in so far as:

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

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

(c) processing is necessary and proportionate to that other purpose.[120]

---

117 (…) preferred further processing to be prohibited instead of permitted.
SE found that the paragraph was too narrow and wanted that *e.g.* the police should be able to inform social authorities of personal data processed by the police in a criminal investigation and which showed that a child was being mistreated (data sent from the police to the social authorities was covered by the Directive whereas the processing by the social authorities should fall under the GDPR).

118 DE and SE appreciated 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; DE noted that this did not only concern the Directive internally but also in relation to the GDPR. FI and SI supported DE and meant that it was important not to hamper police work and SI thought that information to social services and schools could be subsumed under the police's general tasks. FR supported DE and provided other examples such as transport licenses and election registers. Cion said that further processing across the two legal instruments would create problems and that there were no specific Articles to be used for that. Cion further stated that if a legal obligation to transfer data to the police existed, such transfer would be considered as the initial police processing. For the Cion the crucial point was that there were no gaps in the protection. The Cion said that if the purpose was outside the scope of the Directive the GDPR was applicable, see Article 6.4 that required a legal basis.
DE, supported by AT, FI, suggested that Article 11.2 from DPFD be introduced here (prior consent of the transmitting MS). Cion meant that Article 7(a) covered the situation in Article 11.2 DPFD. DE asked about when a different purpose occurred and suggested that once Article 6(4) of GDPR was agreed, this text should be inserted here.

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

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

3. *Member States may* [121] *provide that the* **controller** *may further process personal data for* **archiving purposes in the public interest** or [122]*for scientific, statistical or historical purposes***,** subject to appropriate safeguards for the rights and freedoms of data subjects.".[123]

[124]

3a. Member States **may**[125] set conditions in national legislation[126] 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.[127]

---

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

122 SE, supported by FI, suggestion as well as for recital 20.

123 UK queried why processing for historical or scientific purposes was different regarding law enforcement from other investigations. CZ supported paragraph 3. DE asked about the relationship between this paragraph and paragraphs 1 and 2, if it was *lex specialis* or if they should be applied cumulatively.

124 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.

125 DE suggested to replace *shall* with *may*.

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

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

4. The controller shall be responsible for compliance with paragraph 1, 2 and 3.[128]

[129]

[128] DE asked whether the amended text was meant to change the content.

[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, except paragraphs 3(c) and 4 which needed to be further considered.

130

Article 5

***Distinction between different categories of data subjects*[131]**

(…)

130 AT suggested to add a new Article 4a along the lines of Article 4a in the Droutsas report (7428/14):
"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."

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 **as far as practicable**[134]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.[135]

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[136] or restricted in accordance with Article 15.[137]

---

132 HR found the text confusing and suggested dividing it in two parts. BE, CH, IE, RO, SI and UK questioned the added value of the Article. FR and UK said that Article 4(d) set out the same idea. BE and CZ suggested to delete the Article AT in contrast accepted the reinsertion of an Article with that heading. FI thought that an Article on accuracy was needed but was not certain that current Article 6 fulfilled that requirement.

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

134 IE suggestion.

135 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.

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

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

Article 7[138]

Lawfulness of processing[139]

1. Member States shall provide that the processing of personal data is lawful[140] only if and to the extent that processing is necessary[141]:

[138] 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, UK and CH IE favoured the addition of consent. SI suggested to introduce a recital on consent. DK could consider it. IT and PT questioned the possibility of consent in the field of police work. Cion confirmed that consent was not relevant in the field covered by the draft Directive.CZ suggested to build in consent for processing, *e.g.* victims of stalking could consent to have phone calls tapped. FR meant that consent had to be treated with caution and did not want to have it as an autonomous legal basis for processing. BE meant that consent set out in a law would be acceptable. BE and FR reservation as regards consent. Cion questioned whether consent was necessary beyond what was set out in paragraphs (c) and (d) and stressed that consent should not be an individual ground for processing. Cion agreed that text on consent could be set out for example in a recital clarifying that in some cases consent could be a relevant factor.

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

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

[141] 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 (…)[142] [143] or

(…)[144]

(c) in order to protect the vital interests[145] of the data subject or of another person[146]; or[147]

---

142 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.

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

144 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.

145 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.

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

147 NL meant that paragraphs (a) and (c) needed revisiting.

148

(d) for the prevention of an[149] immediate and serious[150] threat to public security[151].

152

153

148 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.

149 IE asked whether it was possible to prevent an immediate threat and suggested, supported by ES and 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. For UK all threats to public security were important. Cion said that the text was standard wording in the acquis.

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

151 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).

152 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.

153 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."

154

Article 7a

Specific processing conditions *155*

1. Member States shall provide that where[156] Union law[157] or the national law applicable to the transmitting competent (…) authority provides specific conditions[158] (...) to the processing of personal data,[159] the transmitting **competent** 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[160] does not apply conditions[161] 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[162].

163

---

154 BE suggested to create a Chapter IIA.

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

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

157 NL asked what was meant with EU law.

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

159 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.

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

161 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.

162 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).

163 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[164]

Processing of special categories of personal data

1. (…)The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data[165] or of data concerning health[166] or sex life[167] shall only be allowed[168] when strictly[169] necessary and

---

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

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. PT said that what is sensitive data was not an absolute notion. HR thought that processing concerning health and sex life should be allowed because in cases related to crimes against sexual freedom such personal data would be collected regularly. RO wanted to add "biometric data" to the category with a special character. FR, supported by NL, said that the notions did not correspond to those set out in the 95 Directive, nor in the DPFD or the Charter and opposed the terms used.

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. FR said that they preferred the text inspired by Article 27(4) in the Eurojust Regulation "…may be processed only when such data are strictly necessary and if they supplement other personal data already processed. Such processing shall be authorized by Union law or Member State law.

(…) the processing authorised by Union law or Member State law which provides appropriate safeguards[170] for the rights and freedoms of the data subjects.

(…)[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

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

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

[172] DE scrutiny reservation on paragraph 2 and SE scrutiny reservation on the underlined text. SE asked whether *in exceptional cases* represented a stronger protection or an exception. HR found the drafting of this part of the Article imprecise. For DE it was not clear how paragraphs 1 and 2 were linked and that something was missing.

[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.

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

[179]

[Article 9]

*[(…)**Automated individual decision (…)***[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 (…).]

---

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

[180] DE, ES, IT, SI entered scrutiny reservations. Cion reservation. RO suggested to define "profiling" and move the Article to Chapter III, support from CZ, EE, IT, FI, SI, SE to define "profiling". SE serious doubts about the Article. DE meant that it was necessary to determine if Article 9 in its current form was 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.