COUNCIL OF THE EUROPEAN UNION

Brussels, 30 October 2013

14901/2/13 REV 2

LIMITE

DATAPROTECT 146
JAI 903
DAPIX 129
FREMP 153
COMIX 564
CODEC 2287

Interinstitutional File: 2012/0010 (COD)

NOTE

from:	Presidency
to:	Working Party on Information Exchange and Data Protection
No. prev. doc.:	11624/1/13 DATAPROTECT 83 JAI 570 DAPIX 90 FREMP 96 COMIX 403 CODEC 1618
No. Cion prop.:	5833/12 DATAPROTECT 6 JAI 41 DAPIX 9 FREMP 8 COMIX 59 CODEC 217
Subject:	Proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data - Chapters I-IV

Delegations find below comments on Chapters I-IV received at **30 October 2013**.

TABLE OF CONTENTS

GERMANY

Comments by the Federal Republic of Germany

on Articles 1 through 32 of the Proposal

presented by the Commission on 25 January 2012 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

in the version revised by the Presidency (Doc. 11624/13)

Germany is grateful for the opportunity given it in the letter of 1 August 2013 to provide written comments.

I. Preliminary remarks

During its Presidency, Ireland devoted significant efforts, a high level of expertise and efficient management of negotiations to reforming European data protection. Thanks to these remarkable efforts, Ireland was able to present a revised draft of the European Data Protection Directive within the extremely short period of only two months after the first reading. In many places, the revisions undertaken by the Irish Presidency represent improvements over the Commission's original draft presented on 25 January 2012 (COM (2012) 10 final). However, it was not possible to solve many other problems noted in earlier discussions.

II. General remarks on the draft

Germany appreciates that, with its proposed Directive, the Commission has initiated a discussion on improving data protection and information-sharing in the area of police and judicial cooperation in criminal matters. Nevertheless, our experts still have substantial concerns about the proposal, also in the version revised by the Irish Presidency, in general and about individual provisions in particular. Germany does not believe that the proposed Directive will help improve data protection or the exchange of information.

It is questionable whether the proposed Directive provides added value over the current Framework Decision 2008/977/JHA particularly with regard to data transmission between Member States. After extensive consultations, the Framework Decision only went into effect on 20 January 2009 and has not yet been implemented in all Member States. Until the Framework Decision has been sufficiently tested and shown to be inadequate, Germany does not find it appropriate to develop new data protection legislation. Where the scope of the Directive extends to data processing at the national level, Germany's Bundesrat is of the view that the proposal for a Directive cannot use Article 16 (2) of the Treaty on the Functioning of the European Union (TFEU) as its legal basis (Bundesrat decision of 30 March 2012, printed document 51/12).

Lastly, the proposed Directive's aim of harmonizing national law on data protection by the police and judiciary is likely to be very difficult to achieve given that the subject matter is so close to police law and criminal procedural law: Member States have very different laws on the police and criminal procedures. Harmonizing these laws is not a policy objective, nor would it be allowed by European law. For this reason, the intended standardization of national data protection law must not lead to a gradual harmonization of police and criminal procedural law through the back door.

III. Major need for amendment and especially significant issues

Nonetheless, Germany is willing to assist with what it views as an urgently needed, comprehensive revision of the proposal presented by the Commission to overcome, if possible, the problems with it. Germany has therefore suggested specific changes to Articles 1 to 32 of the draft version revised by the Irish Presidency (Doc. 11624/13; revisions marked) with brief explanatory footnotes (**Annex 1**). In addition, to explain its position Germany has prepared more detailed remarks on selected problem areas of the draft Directive which in our view are especially significant (**Annex 2**).

Germany has striven to resolve the tension between the draft Directive's goal of achieving a high level of data protection on the one hand and the interests of effective threat prevention and law enforcement on the other. Where the draft Directive provides for administrative obligations, the resulting administrative burden must be manageable in practice and in reasonable proportion to usefulness for data subjects. When revising the Directive, close attention should be paid to ensure that law on police and criminal procedures, which is the sole competence of the Member States, is not unlawfully curtailed. Under no circumstances, should the Directive prevent or unreasonably complicate the use of modern investigative techniques such as comparing DNA profiles.

In Germany's view, the following revisions and issues are especially significant:

- The **delimitation between the Directive and the General Data Protection Regulation must be readjusted**, also taking into account the results of the current consultations on the Regulation's treatment of the public sector. It is necessary to make sure that all **threat prevention** by the police continues to be subject to uniform principles of data protection also in future.

- Because national law on the police and criminal procedures cannot be harmonized for reasons of competence alone, the Member States must retain the ability to enforce special restrictions, such as on the use of data exchanged within the European Union. The Member States should also have the option to adopt data protection rules which go beyond what the Directive requires. Article 1 (2) (b) and Article 1 (3) therefore **clarify that the Directive only sets minimum standards and that conditions may continue to be set for data transmission to other states**.

- Police and judicial authorities are regularly authorized or obligated by national law to transmit personal data under certain conditions for purposes other than threat prevention or law enforcement. Article 2 (1) **clarifies that such transmission for other purposes is governed by the Directive, not the Regulation**; Article 7 determines the conditions under which such transmission is permitted.

- Files are increasingly kept in electronic form. In Germany's view, the important **question in this context as to whether the scope of the Directive includes files as well as (electronic) notes and drafts** has not been sufficiently answered, neither in Article 2 (2) nor in recital 15. This question urgently requires an answer given the anticipated increase in administrative burdens which would result from applying the Directive without restrictions to files and notes.

- The duties of controllers with regard to **rectifying, erasing and blocking personal data** which are of central importance to the data subject should be summarized in a new Article 4a which fits systematically into Chapter II. In the case of obligations and/or claims based on Articles 4a, 15 and 16, it is necessary to ensure that **no barriers** are raised to **ascertaining the truth**, which is the unique purpose of investigations and criminal proceedings themselves. Further, conflicts must be avoided with the principle enshrined in Germany's Constitution that files must be complete and accurate. The new **obligation of proactive notification of all recipients** in Article 15 (3) must not lead to overwhelming and unmanageable **bureaucratic burdens** in practice and therefore still requires review.

  As to the **rights to erasure** provided for in the Directive (Articles 4a and 16), important, practically relevant **exceptions** in which blocking the data is sufficient should be added.

- The newly proposed Articles 7 (1a) and 8 (2) (d) provide – within the framework of legally mandated tasks and powers of the authorities – for the **voluntary consent of data subjects** defined in Article 3 (8a) as additional justification, as every individual should in principle be able to freely control their data. This corresponds to the intent of Article 8 (2) of the EU Charter of Fundamental Rights. The consent of the data subject is essential in certain crucial areas, such as in prevention projects or when taking blood samples or conducting DNA testing.

- The rules on the **treatment of special categories of personal data** in Articles 3 (10), 8 and 9 are unsuitable when the rules and exceptions apply for the work of the police and justice authorities. They might even mean that the automated comparison of DNA profiles would no longer be allowed. **The Directive must not rule out the use of such important and legitimate investigative methods**.

- Articles 11, 11a and 12 provide for **extensive information and access obligations** for authorities which do not provide any noticeable added value for the data subject, but would have a massive impact on ordinary police work, making it highly bureaucratic. To be effective, data protection must remain practicable for the authorities. The Member States should therefore openly discuss **appropriate limits on the above-mentioned rules, in particular whether in Articles 11 and 11a providing information should be obligatory or only discretionary**.

- **The scope of Article 17 requires clarification**. To prepare for the necessary discussion, Germany asks the Council's Legal Service for an opinion (see Annex 2).
- It is necessary to clarify who within the competent authority is considered the **controller** and who is the **processor** (Article 21). Germany asks the Legal Service for its opinion on this matter.
- Apart from specific questions, it is important to make sure that the administrative efforts required to meet the **documentation obligations in Articles 23 and 24** are manageable in practice and in reasonable proportion to their usefulness for data protection.
- The obligation of **prior consultation of the supervisory authority (Article 26)** must be carefully reviewed for its compatibility with police and judicial concerns.
- The **requirements on notifying the supervisory authority and the data subject (Articles 28 and 29)** require intensive review and must not lead to unnecessary bureaucracy nor threaten police or judicial interests or performance.

IV. Remarks on the significance of the Directive and on the process

In general, Germany is following the discussion of the Directive with great concern. It is often said that the General Data Protection Regulation and the Data Protection Directive make up a single reform package. In fact, however, the questions and problems related to the Directive have had a lower priority. Taking into account the differing urgency of reform, the different priority of Regulation and Directive may seem understandable and possibly even advisable. In view of the fundamental changes the new Directive will bring in comparison to the current law, especially as it will expand the scope to national data processing for the first time, the draft Directive too needs careful review. Even the rather cursory discussion of the draft during the first reading, held after only six sessions, demonstrated that the Member States have significant concerns, both of a fundamental nature and with regard to individual provisions, which must be resolved.

Other important issues, such as the cross-cutting issues mentioned by the Irish Presidency during the DAPIX meeting on 21 February 2013 (need for amendment in view of Framework Decision 2008/977/JHA, which entered into force on 20 January 2009; extending the scope to national data processing; setting minimum standards or full harmonization) have been identified but have not yet been discussed due to time constraints. So the discussion of the Directive is still in the early stages. Further shortening the subject-related and political discussion would be detrimental to the project and would do justice neither to the data protection concerns of the public nor to the enormous significance of the Directive for the area of police and justice.

V. Scrutiny reservation

Germany finds it essential to review the draft Directive and give its consent with the necessary care and attention to detail. Germany therefore maintains its **scrutiny reservation** with regard to all provisions of the Commission's proposal presented on 25 January 2012 in the Presidency's revised version (Doc. 11624/13). Further, Germany reserves the right to make additional comments on the recitals, of which only selected points have so far been mentioned. In our view, discussing the recitals makes sense only after the legislative text has taken a more final form.

GERMANY

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and objectives

1. This Directive lays down the rules relating to the protection of individuals with regard to the processing of personal data by competent public[1] authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences [~~and for these purposes, the maintainance of public order,~~]or the execution of criminal penalties [and for the purposes of maintaining and assuring the public security and order by the police and customs][2].

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

---

[1] Germany will examine the possible impacts of limiting the scope to public authorities and whether mentioning natural persons only in the term "processor" in Article 3 (7) is sufficient.

[2] Scrutiny reservation. Germany agrees with Romania's analysis in that the area of threat prevention by the police ("administrative police") should not be included in the scope of the General Data Protection Regulation. Instead, Germany finds it necessary for subject-related and legal reasons for the Directive to cover general threat prevention by the police, i.e. regardless of whether legal interests protected by criminal law are at issue. To this end, it is necessary to find wording that takes into account the justified concerns expressed by the Romanian Delegation on 8 April 2013 (Doc. 8208/13) without excessively expanding the scope of the Directive. The passage inserted in Article 1 by the Presidency and subsequently deleted by Germany is not suitable for this purpose, as it leaves the scope of the Directive unchanged. In their necessary consideration of the problem the Member States should start with the wording given here in square brackets, which is based on the Romanian proposal. For a more extensive discussion of this issue, see Annex 2 of our comments.

(b) ensure that the exchange of personal data by competent public authorities within the Union is neither restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data by restrictions or prohibitions stricter than those applicable at national level[1].

3. With regard to national data processing, this Directive does not preclude Member States from providing safeguards for the protection of personal data which are stricter than those established in this Directive.[2]

Article *2*

Scope

1. This Directive applies to the processing of personal data by competent public authorities for the purposes referred to in Article 1(1) and their transmission by competent public authorities for other purposes[3].

---

[1] In line with the philosophy anchored in Articles 1 (5) and 12 of Framework Decision 2008/977/JHA, Member States should not be prevented from enacting stricter national data protection legislation (see Article 1 (3)) which other Member States would then have to abide by when data are transmitted to them. This philosophy prevents data protection from being undermined without interfering with the Member States' cultural and legal traditions concerning the police and judiciary. For a more extensive discussion of this issue, see Annex 2 of our comments.

[2] Germany opposes full harmonization in the area of police and the judiciary and instead is in favour of defining only minimum standards at a high level of protection (for more detail, see Annex 2 of our comments). The proposed provision corresponds to Article 1 (5) of Framework Decision 2008/977/JHA.

[3] The addition makes clear that data transmission by threat prevention and law enforcement authorities for purposes other than threat prevention or law enforcement is governed by the Directive (and not the General Data Protection Regulation). This addition should be viewed in connection with Article 7 (1) (b).

2. This Directive applies to the processing of personal data wholly or partly by automated means, 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[1].

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, in particular concerning national security[2]; ~~(…)~~

(b) by the Union institutions, bodies, offices and agencies[3].

---

[1] Scrutiny reservation with regard to the question whether the scope of the Directive includes files and (electronic) notes and drafts. This point must be fully clarified. The text of Article 2 (2) and of recital 15 are not sufficiently clear. If files, notes or drafts are to be included in the scope, exceptions would have to be made to a number of provisions in the Directive in order to avoid almost impossible bureaucratic burdens which would otherwise result.

[2] This is an important example for the Member States and should be explicitly mentioned in the legislative text.

[3] Germany believes that exempting the Union institutions, bodies, offices and agencies from the context of the Directive is not appropriate. Data processing by the Union in the area of police and criminal justice must be subject to the same conditions as processing by the Member States. The Directive should therefore at least specify how to ensure that the provisions are as comparable as necessary.

Article 3

Definitions

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 by the controller or the recipient[1], directly or indirectly[2], in particular by reference to an identifier such as a name, an identification number, location data, online identifier[3] or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

(…)

---

[1] It may be worth considering whether Article 3 (1) of the Directive should explicitly mention the controller and the recipient of the data (and not "any other natural or legal person", as stated in the Commission's draft version) as persons whose ability to identify the data subject directly or indirectly is what matters. Whether and to what extent there needs to be a link here to the Regulation and what the specific results would be is currently being examined. In principle, the definitions in Article 3 should be in parallel in both the Directive and the General Data Protection Regulation unless there are objective reasons to differentiate between the two; this should also be noted with regard to the following proposals at first concerning only Article 3 of the Directive.

[2] In the Commission's original draft, data were considered personal only if the data subject could be identified by the controller or any other natural or legal person "by means reasonably likely to be used". This passage has been deleted with nothing to replace it. It is still found in Recital 16, where it is also specified further. However, it seems questionable whether the revised wording of Article 3 (1) still makes enough of a connection to the thoughts expressed in Recital 16. Germany therefore is in favour of restoring this passage to the legislative text.

[3] Germany is examining whether to delete or modify "online identifier". IP addresses may not always constitute personal data. For example, when combating botnets, it is usually not possible to identify individuals using IP addresses. Further, in investigations IP addresses are sometimes processed which were assigned so long ago that it is impossible to identify individuals via the Internet service provider.

(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, blocking, ~~(…) or (…)~~ erasure or destruction[1];

(4) ~~'restriction of processing~~ blocking'[2] means the marking of stored personal data with the aim of limiting their processing in the future;

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

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

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

(8) 'recipient' means a natural or legal person, public authority, agency or any other body other than the data subject, the controller or the processor[3] to which the personal data are disclosed;

---

1 Germany finds it preferable to retain the terminology of the original draft of the Directive.

2 Germany finds it preferable to keep the terminology used in Articles 2 (c) and 18 of Framework Decision 2008/977/JHA and refer to "blocking" rather than "restriction of processing".

3 Germany approves of this clarifying addition.

(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[1]

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

(10) 'genetic data' means all personal data, (…) relating to the genetic characteristics of an individual that have been inherited or acquired, resulting from an analysis of a biological sample from the individual in question; non-coding DNA sequences are not regarded as genetic data[2]

---

[1] This definition of consent uses the same wording as Article 4 no. 8 of the General Data Protection Regulation. It may be necessary to examine whether the wording should be adjusted in line with Article 2 (g) of Framework Decision 2008/977/JHA. Regardless of the exact definition used, it should in principle be possible to process data also on the basis of the data subject's voluntary consent.

[2] Apart from our concerns about an absolute ban on the processing of genetic data (see comments on Articles 8 and 9 below), the legal definition of genetic data in Article 3 (10) still seems in need of clarification despite the welcome specification by the Irish Presidency. Not all genetic data allow conclusions to be drawn about the data subject's personality. Although non-coding DNA can be individualized, it does not contain highly sensitive hereditary information. So it is impossible to draw conclusions about the genetic code and personal characteristics of the person in question. In terms of data protection law, the data subject therefore faces a much lower risk than if DNA components containing hereditary information are examined and analysed. The more precise definition of genetic data proposed here is intended to take these distinctions into account. Further examination is needed to determine whether similar differentiation would be helpful or advisable in the scope of the General Data Protection Regulation and thus whether the legal definition there should be revised.

~~[1](11) 'biometric data' means any personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual, such as facial images, or dactyloscopic data;~~

~~(~~

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

(12a) 'profiling' means any form of automated processing of personal data intended to create or use a personal profile by evaluating personal aspects relating to an individual[2];

(…)

(13) '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;[3]

---

1 In principle, we welcome the specification added to Article 3 (11) by the Presidency. However, none of the provisions in the Directive refers to the term "biometric data". For this reason, Article 3 (11) can and should be deleted.

2 Germany enters a scrutiny reservation regarding the term "profiling". This term ultimately remains unclear, nor has it so far been possible to define it conclusively with regard to the General Data Protection Regulation. Germany is examining whether, in view of Article 9 of the Directive, we should return to the term "automated individual decision" used in Article 7 of Framework Decision 2008/977/JHA.

3 The definition is based on Article 1 (a) (iii) and (iv) of Framework Decision 2005/214/JHA of 24 February 2005 on the application of the principle of mutual recognition to financial penalties and on Article 5 (b) and (c) of Framework Decision 2008/978/JHA on the European evidence warrant. It is necessary in order for the Directive – like other comparable European legislative acts – to cover administrative offences in Germany (*Ordnungswidrigkeiten*) which are less serious offences subject to a fine. In terms of procedural law, *Ordnungswidrigkeiten* in Germany are dealt with based on the Code of Criminal Procedure, so that if they were to come under the General Data Protection Regulation, Germany would have to create a completely new and inappropriate system to punish *Ordnungswidrigkeiten.*

(14) 'competent public[1] authority' means [the police, customs and][2] any authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

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

CHAPTER II

PRINCIPLES

Article 4

Principles relating to personal data processing

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

(a) processed (…)[3] lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes[4];

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

---

[1] Germany enters a scrutiny reservation in order to be able to examine the impacts of these restrictions, for example on action by natural persons charged with fulfilling state functions.

[2] Depending on the exact wording of Article 1 (1), Article 3 (14) needs to be revised in response to the expansion of the scope of application in Article 1 (1). This cannot be done until the final wording of Article 1 (1) has been determined.

[3] Germany approves of this deletion. The term "fairly" comes from civil law and is not appropriate in this context.

[4] It is still necessary to explain how Article 7 is to be read together with the principles of data processing under Article 4, in particular the principle of purpose limitation.

(d) accurate and, where necessary, kept up to date; (…)

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

(ee) processed in a manner that ensures appropriate security of the personal data[1].

(…)

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

Article 4a

Rectification, erasure and blocking[3]

1. Personal data shall be rectified if inaccurate.[4]

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[5].

---

1 It is necessary to clarify whether the reference to the need for appropriate security of personal data in Article 4 (1) (ee) is simply a declaratory reference to Chapter IV Section 2, Data Security. If so, this should be made clear in a suitable way (e.g. with an appropriate addition in brackets in Article 4 (1) (ee)).

2 Germany would like to know why Article 4 (f) of the Commission's draft has been deleted and replaced with the differently worded Article 4 (2), and whether this is intended to alter the content. In our view, both the deleted and the newly added provision have only a declaratory nature, as the obligations of the controller are listed in detail in the Directive.

3 Article 4a is an explanatory summary and addition to the central provisions on rectification, erasure and blocking. It is necessary to create a parallel between the obligations to be met by the controller in processing data on the one hand and the rights of data subjects covered in Chapter III on the other.

4 Germany understands the obligation of rectification to mean that, at least in files, inaccurate data will not have to be erased, but only the fact of their inaccuracy will have to be noted. Otherwise this provision would risk violating the principle enshrined in Germany's Constitution that files must be complete and accurate.

5 The statement in the previous footnote applies accordingly to the obligation to erase.

3. Personal data shall not be erased but merely blocked if[1]

(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[2], or

(c) the erasure would be technically feasible only with a disproportionate effort, for instance on account of the special nature of the storage[3].

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.[4]

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.[5]

---

1 The exceptions to erasure allowed in paragraph 3 must be addressed in general form, not only when data subjects apply for erasure pursuant to Article 16. The same exceptions are needed in the case of data to be erased ex officio.

2 Such cases are especially important in practice. As a rule, data stored in back-up filing systems cannot be erased selectively without a great deal of technical effort, if at all. Blocking would therefore make sense here until the entire back-up file can be overwritten or destroyed.

3 These constellations are similar to those in (b). If the specific mode of storage results in the deletion being impossible or requiring disproportionate effort, blocking the data must suffice.

4 A clear rule is needed on how to deal with blocked data and which processing is allowed under what conditions.

5 This is the same language as in Article 5 of Framework Decision 2008/977/JHA, the content of which should be retained.

Article 5
Distinction between different categories of data subjects

(…)[1]

Article 6
Different degrees of accuracy and reliability of personal data[2]

(…)

The competent authorities shall take all reasonable steps to provide that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, the competent authorities shall, as far as practicable, verify the 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 Member State to assess the degree of accuracy, completeness, up-to-dateness and reliability.

---

1 We approve of the deletion of Article 5 ("distinction between different categories of data subjects") in the Commission's draft.

2 The question addressed in Article 6 of the accuracy of data was discussed at length during the negotiations on Framework Decision 2008/977/JHA. The result was the obligation in Article 8 of the Framework Decision to verify the quality of personal data as required before they are transmitted, the exact wording of which has been adopted here. In Germany's view, there is no reason to seek a different solution.

Article 7

Lawfulness of processing[1]

1. Member States shall provide that the processing of personal data is lawful only if and to the extent that processing is necessary[2]:

(a) for the performance of a task carried out by a competent public authority, based on Union law or Member State law[3], for the purposes set out in Article 1(1); or

---

1 It will not be possible to make a final judgement of the provision until the exact scope of the Directive has been established.

2 It is still necessary to explain how Article 7 is to be read together with the principles of data processing under Article 4, in particular the principle of purpose limitation.

3 It will be very difficult to achieve the goal of EU-wide harmonization of data protection law using Article 7 given its reference to the Member States' (highly heterogeneous) national laws. It is correct to refer to these laws, because national law on the police, criminal code and criminal procedures must be authoritative for the work of the police and judicial authorities. But law on the police, criminal law and criminal procedural law differ widely among the EU Member States and do not fall under the EU's power to legislate. Overall, this demonstrates the enormous difficulty of the Directive's pursuit of harmonization of data protection law. Also for this reason, the passages added to Article 1 (2) (b) and Article 1 (3) are needed.

(b) for compliance with a legal obligation[1] or for the lawful exercise of a legal power[2] the controller is subject to[3].

~~(…)~~

(c) in order to protect the vital interests of the data subject or of another person[4]; or

(d) for the prevention of an immediate and serious threat to public security.[5]

---

1 Germany finds it essential to restore this ground for lawfulness for practical and legal reasons. 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.

2 In Germany's view, particularly with regard to use for different purposes already addressed in Article 2 (1), the previous Article 7 needs additional text. In many cases, the police and judicial authorities must transmit information acquired during the course of their investigations to other authorities so that they are informed of relevant circumstances and can take the necessary measures, for example to protect children or young persons or to exercise trade supervision. In Germany, the applicable provisions take the form of powers (subject to certain conditions) of the transmitting authorities; for this reason, simple reference to "legal obligations" as in the current draft is not sufficient.

3 Germany is checking whether, in addition to the changes made to the text, 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."

4 Scrutiny reservation. It is necessary to clarify whether this provision overlaps with paragraph 1 (a) and (b). If so, (b) can probably be dispensed with. If not, it will be necessary to determine whether the Directive in general and Article 7 in particular allow data to be transmitted to private parties to a sufficient extent. If such data transmissions can be based only on Article 7 (1) (c), which allows for data processing in order to protect vital interests, this seems far too limited, because private parties may have a legitimate interest in data transmission which does not meet this condition, for example to claim legal rights.

5 Scrutiny reservation to the same extent and for the same reasons as in the previous footnote. Article 7 (1) (d) allows the processing of personal data only "for the prevention of an immediate and serious threat to public security". But the competent authorities must be able to take action to prevent crimes even in the absence of imminent danger, for example to foil a planned bombing long before it is supposed to be carried out. With this in mind, the addition "immediate and serious" should be deleted.

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.[1]

2. Member States ~~shall~~ may[2] provide that the controller may ~~further~~ process personal data for historical, statistical or scientific purposes as well as for the purposes of basic and advanced training, subject to appropriate safeguards for the rights and freedoms of data subjects.

[3]~~*Article 7a*~~

~~***Specific processing conditions***~~

[3]~~1. Member States shall provide that where Union law or the national law applicable to the transmitting competent public authority provides for specific conditions applicable in specific circumstances to the processing of personal data, the transmitting public authority shall inform the recipient to whom the data are transmitted about such conditions and the requirement to respect them.~~

---

[1] In line with Article 8 (2) of the EU Charter of Fundamental Rights, data processing for the purpose of fulfilling assigned tasks must be allowed also when the data subject has given voluntary consent. The possibility of consent-based data processing is essential in certain crucial areas, such as in prevention projects or when taking blood or conducting DNA testing. Consent-based data processing is often a less bureaucratic alternative, for example to a court order required by law. In Germany's view, at the very least it is essential for the Member States not to be prevented from enacting laws declaring that data processing by the police and judiciary is lawful on the basis of voluntary consent of the data subject alone. Further review is required to determine whether consent solutions should be allowed which are not governed by special legislation on the discharge of police and judicial functions but only (as in Germany) by general data protection legislation.

[2] Paragraph 2 must not create an obligation but only an option for the Member States.

[3] The deletion of Article 7a should be seen in connection with the addition to Article 1 (2) (b) (see also Annex 2 of our comments).

~~2. Member States shall provide that the transmitting public authority does not apply conditions 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 the transmitting public authority.~~

Article 8

Processing of special categories of personal data[1]

1. Member States shall ~~prohibit~~ restrict the processing of personal data revealing racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or of data concerning health or sex life to the extent which is strictly necessary.[2]

2. No restriction pursuant to ~~Paragraph~~ paragraph 1 is required, if:[3] ~~shall not apply where:~~

   (a) the processing is authorised by Union law or Member State law which provides appropriate safeguards[4] for the rights and freedoms of the data subjects; or

   (b) the processing is necessary to protect the vital interests of the data subject or of another person[5]; or

---

1 Even though the data listed in Article 8 are certainly especially sensitive, Germany finds the absolute prohibition on processing these data in paragraph 1 to be too far-reaching and impractical. Especially in the area of law enforcement and threat prevention, it is necessary to process sensitive data in various ways. The provision should therefore allow the processing of sensitive data if necessary to carry out the tasks of the relevant agencies, taking into account the special sensitivity of the data (see also the Annex to our comments).

2 Germany is still checking whether the following sentence should be added for clarification: "In particular, these data shall be excluded from transmission or being made available in so far as the purpose of the transmission or making available is not thereby impaired and excluding them is feasible with an appropriate effort."

3 The introductory sentence to Article 8 (2) has been revised simply for linguistic reasons.

4 It is still unclear what is meant by "appropriate safeguards".

5 Article 8 (2) (b) is too narrowly focused, especially if the German proposal for a revised Article 8 (1) is rejected. Exceptions should be possible not only to protect vital interests, but also when other high-priority legal interests (such as permanent loss of eyesight or other serious bodily injury) are affected.

(c) the processing (…) is necessary for the prevention of an immediate and serious threat to public security[1]; or

(d) the data subject has consented to the processing[2].

Article 9

(…) Profiling (…)[3]

~~1.~~ Member States shall provide that a decision[4] based solely on profiling which produces an adverse legal effect for the data subject or severely affects him or her (…) shall be prohibited unless authorised by a law which provides appropriate safeguards for the rights and freedoms of the data subject (…).

---

1 Germany welcomes the inclusion of another ground for exception for prevention of an immediate and serious threat to public security. The provision seems too narrow, however, especially if the German proposal for a revised Article 8 (1) is rejected. Please see the comments on Article 7 (1) (d) in this regard.

2 Clarification that consent is possible also in this context.

3 Scrutiny reservation. Apart from the general competence-related concerns about the draft Directive, it is still necessary to determine whether Article 9 (1) in this form is covered by the legislative competence of the Union. This provision does not address whether or how data may be processed but instead prohibits a decision. Although this decision is based on data processing, the decision itself does not belong to data protection law but is instead made on the basis and in the exercise of police, criminal and/or criminal procedural law, which is solely the competence of the Member States.

4 Germany believes it makes sense for Article 9 (1) not to refer to "measures" but (in line with Article 7 of Framework Decision 2008/977/JHA) to "decisions".

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

CHAPTER III

RIGHTS OF THE DATA SUBJECT

Article 10

Communication and modalities for exercising the rights of the data subject[2]

1. (…)[3]

---

[1] Germany agrees with the deletion of the original paragraph 2, as this paragraph would have ruled out important and legitimate investigative measures, in particular the automated matching of DNA or data matching for threat prevention. In our view, the new version of paragraph 2 proposed by the Irish Presidency does not add anything to the content of Article 8 and should therefore be deleted. See also the comments on Article 3 (12a).

[2] Germany largely agrees with the Irish Presidency's revisions to Article 10. We especially welcome the fact that the explicit reference to articles 11, 11a, 12, 15 and 29 makes clear that Article 10 does not create grounds for any separate, new obligations, but only governs how data subjects' rights granted by other provisions of the Directive are to be exercised. Nonetheless, Germany maintains a scrutiny reservation.

[3] We agree with the deletion of Article 10 (1).

2. Member States shall provide that the controller shall take appropriate measures to provide any information referred to in Articles 11 and 11a and any communication under Articles 12 ~~and~~ to 16~~5~~ and 29 relating to the processing of personal data to the data subject in an intelligible and easily accessible form, using clear and plain language as far as possible[1]. ~~The information shall be provided in writing or, where appropriate, electronically or by other means.~~[2]

~~3. Member States shall provide that the controller takes all reasonable steps to provide the information referred to in Articles 11 and 11a and to facilitate the exercise of data subject rights under Articles 12 and 15 (…).~~

[3]

~~4. Member States shall provide that the controller informs the data subject about the follow-up given to his or her request without undue delay.~~[4]

---

[1] This addition is intended to clarify that the "intelligible form" required in Article 10 (2) does not require translations. The recitals should note that it is sufficient for information to be provided in the relevant official language. Directive 2010/64/EU contains comprehensive rules on translation obligations in criminal proceedings. Given the numerous information obligations resulting from the draft Data Protection Directive, the requirement to translate everything would result in an overwhelming expense and amount of work.

[2] The second sentence should be deleted, as it is more practical, less bureaucratic and also sufficient from the data subject's perspective to require that only refusals must be in writing and otherwise leave open the form in which information is to be provided.

[3] Compared to the only definitive articles 11 through 16, paragraph 3 has no regulatory content of its own; it can therefore be dispensed with and should be deleted.

[4] It is necessary to delete paragraph 4 in order to make clear that it is not necessary to inform the data subject of every single step taken in response to his or her request. From the perspective of the data subject and with an eye to the bureaucratic burden for authorities, it is sufficient to inform the data subject of the results of the review.

3. In cases referred to in Articles 12, 15 and 16, Member States shall provide that the controller informs the data subject in writing of any refusal or restriction of access, rectification, erasure or blocking, of the reasons for the refusal and of the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy. This shall not apply where the provision of such information would undermine a purpose under Article 13 (1).[1]

5. Member States shall provide that the information provided under Articles 11 and 11a and any communication under Articles 12, 15, 16 and 29 shall be provided (…) free of charge[2]. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character (…)[3], the controller may refuse to act on the request. In that case, the controller shall state the reasons for the refusal. ~~bear the burden of demonstrating the manifestly unfounded or excessive character of the request~~ (…).

5a. Where the controller has reasonable doubts concerning the identity of the individual making the request referred to in Articles 12, ~~and~~ 15 and 16, the controller may request the provision of additional information necessary to confirm the identity of the data subject[4].

---

1 This new paragraph contains a generalized summary of the previous Article 13 (3) and Article 15 (2). Further review is needed to determine whether a documentation obligation can be made to apply generally on the model of Article 13 (4).

2 Scrutiny reservation. Germany too believes that the access rights of data subjects must not be undermined in fact by unreasonably high fees. However, it is not clear why Article 10 (5) requires information to be provided free of charge, thus differing from Article 17 (1) of Framework Decision 2008/977/JHA, which only prohibits "excessive" expense. Germany is therefore checking whether it is advisable to use the wording of the Framework Decision.

3 Germany is pleased that, in the revised version, unfounded requests are not only subject to a fee but may also be refused. Germany is still examining whether, in line with the Commission's original wording, the "size or volume of the request" should be restored as an indication of unfounded or excessive requests.

4 We expressly welcome the new Article 10 (5a) because it prevents unauthorized investigations.

Article 11

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

1. Subject to Article 11b, Member States [shall / may][1] provide that where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with *at least* the following information:

(a) the identity and the contact details of the controller and, if any, of the data protection officer;

(aa) whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data; and

(b) the purposes of the processing for which the personal data are intended;

(c) (…)

(d) (…)

(e) the right to lodge a complaint to a supervisory authority (…).

[1] Although the excessive information obligations in the Commission's original proposal have been reduced through welcome deletions made to Article 11 (1), key provisions of the Commission's draft, in particular the one on limitations to the rights of information (Article 11b) have remained unchanged, leaving the large number of notifications to be made. Germany encourages the Member States to discuss whether providing information should be obligatory or only discretionary.

(f) (…)

(g) (…).

2. (…)

3. (…)

4. (…)

5. (…)

Article 11a

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

1. *Subject to Article 11b, Member States [shall / may] provide that where personal data have not been obtained from the data subject, the controller shall provide the data subject with at least the following information:*

   (a) the identity and the contact details of the controller and, if any, of the data protection officer;

   (b) the categories of personal data concerned;

   (c) the purposes of the processing for which the personal data are intended;

   (d) the right to lodge a complaint to a supervisory authority.

[1] ~~*2. The controller shall provide the information referred to in paragraph 1:*~~

~~*(a) within a reasonable period after obtaining the data, having regard to the specific circumstances in which the data are processed, or*~~

~~*(b) if a disclosure to another recipient is envisaged, at the latest when the data are first disclosed.*~~

Article 11b[2]

Limitations to the rights of information

1. Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to Article 11 and 11a to the extent that, and as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the individual concerned:

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

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

(c) to protect public security;

(d) to protect national security;

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

---

[1] Germany rejects the obligation newly included in the draft Directive that data subjects are to be informed at the latest when the data are disclosed to another recipient. This provision would unreasonably interfere with the work of the responsible authorities. For example, if a group of suspects and/or witnesses is to be questioned, it is often necessary to alternately use information taken from statements of others which typically includes personal data. In such cases, it is impossible to inform the data subject when these data are disclosed.

[2] If Articles 11 and 11a are formulated with "may", this provision could be dispensed with. If not, the proposed revisions are urgently needed.

1a. Member States may provide that the provision of information may be dispensed with temporarily, wholly or partly[1]

(a) if the data subject is already in possession of the information or voluntarily waives the right to the information;

(b) if the personal data are not collected from the data subject, the processing is explicitly subject to statutory regulations and the controller makes a general representation of the information referred to in paragraph 1 generally available in writing and electronically; this exception shall not apply to the collection of data in secret from the data subject;

(c) if further personal data would first have to be collected in order to provide the information;[2]

(d) if the effort involved in weighing the interests of the data subject in receiving the information and that required in providing the information would be disproportionate;[3]

(e) if this is obviously not appropriate due to special circumstances or would significantly endanger or interfere with the performance of law enforcement tasks[4].

---

1 Article 11b (1) refers only to reasons specific to law enforcement and security for limitations to information rights. However, general grounds are also conceivable. The proposed rules take this into account. They address those cases when the data subject's need for information has already been met ((a) and (b)) or when information need not be provided for other reasons or the provision of information would not be proportionate ((c) through (e)).

2 Collection of additional data should be avoided.

3 This proposal is based on Article 14 (5) (b) of the General Data Protection Regulation and is needed for practical reasons also in the area of police and justice. There is no reason for the Directive to put police and the judiciary in a worse position than the addressees of the Regulation.

4 In a number of situations (e.g. a car accident or other emergency situation) more important and urgent measures may be needed first.

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

Article 12

Right of access for the data subject[2]

1. Subject to Article 13, Member States shall provide for the right of the data subject to obtain from the controller at reasonable intervals and free of charge confirmation as to whether or not personal data relating to him or her are being processed. W, ~~and w~~here such personal data are being processed, the controller shall provide ~~to obtain access to such data and~~ the following information:

   (a) the purposes of the processing;

   (b) (…)

   (c) the recipients or categories of recipients to whom the personal data have been ~~or will be~~[3] disclosed, in particular the recipients in third countries;

---

1 It is still unclear what is meant by "categories of data processing". This criterion does not seem very appropriate for the decision to be made by national legislators whether and to what extent to provide information ex officio to the data subject.

2 Despite the proposed revisions, Germany maintains its scrutiny reservation with regard to Article 12. It is necessary to determine whether even the revised version of Article 12 (1) differs from Article 17 of Framework Decision 2008/977/JHA, whether this is justified and how it would affect the work of the police and judicial authorities.

3 We welcome the deletion of "or will be". It is likely to be difficult, if not impossible, to predict what transmission will take place in the future. For this reason, a right of access in this regard would lead to major problems.

(d) ~~where possible,~~ the envisaged period for which the personal data will be stored or the rules applicable to calculating this period[1];

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

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

(g) communication of the personal data undergoing processing ~~(…)~~[2].

~~1a. Member States shall provide that where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 35 relating to the transfer.~~

2. (…)[3]

---

1 It is likely to be difficult to forecast the actual or envisaged length of time personal data will be stored. Referring to the provisions on which the period of storage is based (e.g. the implementing legislation for Article 4a (5)) would be less bureaucratic and would also satisfy data subjects' need for information.

2 Removing Article 12 (1) (g) providing for an exact description of the processed data and the deletion of "any available information as to their source" makes it much easier to manage the content of data subjects' right of access. Article 12 (1) (g) would have established a far too extensive obligation to provide access and resulted in significant bureaucratic effort. It would have also threatened the protection of sources. We therefore expressly welcome its deletion. However, it would go too far not even to inform data subjects which of their data have been processed.

3 We welcome the deletion of Article 12 (2) on the "right of the data subject to obtain from the controller a copy of the personal data undergoing processing". Written information is sufficient to uphold the rights of data subjects. Article 12 (2) would have resulted in significant bureaucratic effort. And it would have been very difficult not to reveal information about law enforcement intelligence-gathering.

Article 13

Limitations to the right of access[1]

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

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

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

   (c) to protect public security;

   (d) to protect national security;

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

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

---

[1] Germany is still examining the need to include additional exceptions, for example if paper files may also be subject to requests for access (see the remarks concerning Article 2 (2)): If the personal data which are the subject of the request are neither automated nor stored in automated databases, then it should be obligatory to provide access only if the data subject provides information enabling the data to be found, and if the effort required to provide access is not disproportionate to the data subject's interest in the information. In addition, it is necessary to check whether an exception for electronic files is needed (e.g. in case their search functions are limited).

[2] As already noted with regard to Article 11b (2), it is still unclear, even with reference to Article 13 (2), what is meant by "categories of data processing".

~~3. In cases referred to in paragraphs 1 and 2, Member States shall provide that the controller informs the data subject (…) of any refusal or restriction of access, of the reasons for the refusal and of the possibilities of lodging a complaint to the supervisory authority [and seeking a judicial remedy]. This shall not apply (…) where the provision of such information would undermine a purpose under paragraph 1.~~[1]

4. Member States shall ensure that in cases of Article 10 (3) 2 the controller documents the grounds for omitting the communication of the factual or legal reasons on which the decision is based.

~~[2] *Article 14*~~

~~Additional~~ ~~m~~odalities for exercising the right of access

~~1. Member States shall provide for the right of the data subject to request, in cases referred to in Article 13, that the supervisory authority checks the lawfulness of the processing.~~

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

~~3. (…)~~

[1] Paragraph 3 deleted as a result of changes to Article 10 (3).

[2] The content of the deleted Article 14 (1) and (3) is already covered in Article 45 (1) (b). Article 14 (2), also deleted, is the subject of Article 10 (3).

Article 15

Right to rectification[1], ~~erasure and restriction of processing~~

1. Having regard to the nature and purpose of the processing concerned, Member States shall provide for the right of the data subject to obtain from the controller the rectification of personal data relating to him or her which are inaccurate and (…) the right to obtain completion of incomplete personal data, if the addition is relevant for the purposes referred to in Article 1(1)[2]~~. including by means of providing a supplementary statement.~~

[3]~~*1a. Member States shall provide for the obligation of the controller to erase personal data without undue delay and of the right of the data subject to obtain from the controller the erasure of personal data (…) without undue delay where the processing does not comply with the provisions adopted pursuant to Articles 4 (a) to (e), 7 and 8 of this Directive, or where the data have to be erased for compliance with a legal obligation to which the controller is subject.*~~

---

1 Germany enters a scrutiny reservation regarding Article 15, even if the proposed revisions are accepted, with regard to the matter addressed in the footnote to Article 4a (1). Further, the accuracy or inaccuracy of statements by other participants or (possibly provisional) assessments by the responsible officials cannot be determined at the level of data protection law, but is the main purpose of investigations and criminal proceedings themselves; further examination is necessary to determine whether recital 21 sufficiently solves this problem. And Article 15 differs from Article 18 of Framework Decision 2008/977/JHA at least in its wording for no apparent reason. Germany would like an explanation of why the wording has been changed, how the changed wording does or is intended to affect the content and what grounds led to the new formulation. Last but not least, the overall relationship between Article 4 (d), Article 15 (1) and Article 15 (1a) is unclear. In our view, for reasons of logic alone the rights of data subjects cannot exceed the corresponding obligations of the responsible authority.

2 The wording added by Germany is intended to prevent misuse. An unconditional right would contradict the principle of the necessity of collecting data anchored in Article 4 (c). It would also create unnecessary bureaucracy for the authority, as it would not be able to simply accept this information but would have to check it for accuracy. This provision would open the door to nuisance requests.

3 We have deleted paragraph 1a because the obligation to erase should be dealt with separately in Article 16, as proposed by the Commission, to improve clarity.

[1]~~1b. Member States shall provide for the right of the data subject to obtain from the controller the restriction of the processing of personal data where their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data, or where they are required by the data subject for the establishment, exercise or defence of legal claims.~~

~~2. Member States shall provide that the controller informs the data subject (…) of any refusal of rectification, erasure or restriction of the processing, the reasons for the refusal and the possibilities of lodging a complaint to the supervisory authority [and seeking a judicial remedy].~~[2]

3. Member States shall provide that in the cases referred to in paragraphs 1~~, 1a and 1b~~ the controller shall notify the recipients and that the recipients shall rectify~~, erase or restrict~~ the processing of the personal data under their responsibility, if these measures are important for the recipient or necessary to protect the data subject's rights.[3]

---

[1] Paragraph 1b has been deleted because data whose accuracy is contested by the data subject cannot be blocked in criminal proceedings or proceedings for the purpose of threat prevention: The point of such proceedings is to determine the truth; to this end, much evidence, the accuracy or inaccuracy of which is often unclear, must be collected and evaluated. The data subject will naturally contest the accuracy of much data; the authorities' task is to evaluate all the data and arrive at an objective overall picture. To do so, it must have access to all the data, which thus cannot already be blocked by the data subject's application for rectification. The deletion of paragraph 1b does not affect the authority's ability to block the data rather than erasing it as requested when certain conditions are met (Article 16 (2)).

[2] Paragraph 2 deleted because this content is already covered in Article 10 (3).

[3] Scrutiny reservation: Despite Germany's addition, it is necessary to determine with regard to bureaucracy whether the provision should be further limited (or if necessary deleted entirely). In any case, there is not the same (Internet-specific) situation as in the case of the "right to be forgotten" intensively discussed in relation to the General Data Protection Directive. Further, due to the broad legal definition of recipients in Article 3 (8), witnesses and suspects might also have to be informed when information supplied by other participants was later corrected. Article 15 (3) would then lead to complex problems which were already intensively discussed under the heading "accuracy of data" during the negotiations on Framework Decision 2008/977/JHA and which were one of the reasons Article 6 of the Commission's original proposal for the Directive was deleted.

Article 16

Right to erasure[1]

1. Member States shall provide for the right of the data subject to obtain from the controller the erasure of personal data relating to them without undue delay where the processing does not comply with the provisions adopted pursuant to Articles 4 (a) to (c)[2] as well as 7 and 8 of this Directive. The same applies if the processing does not comply with the provisions adopted pursuant to Articles 4 (e); in these cases the controller may anonymise the personal data instead of erasing them[3].

2. Instead of erasure, the controller shall block the personal data where the conditions under Article 4a (3) are met.[4]

(…)

---

1 To follow up on the footnote to Article 4a (2), here as well Germany understands the obligation to erase to mean that data at least in files do not have to be erased as long as doing so would violate the principle enshrined in Germany's Constitution that files must be complete and accurate. Otherwise, Germany would have to object to the obligation to erase in this form.

2 No reference to Article 4 (d), as there is no right to erasure but rather a right to rectification pursuant to Article 15.

3 The option created here of anonymizing data rather than erasing it creates the necessary link to Article 4 (e).

4 The obligations of the controller should correspond to the rights of the data subject. The proposed provision leads to harmony with Article 4a (3).

Article 17

Rights of the data subject in criminal investigations and proceedings[1]

Member States may provide that the exercise of the rights (…) referred to in Articles 11, 11a, 12, 15 and 156 is carried out in accordance with national rules on judicial proceedings where the personal data are contained in a judicial decision or record processed in the course of criminal investigations and proceedings.

[1] The regulatory content of Article 17 urgently requires clarification. In Germany's view, Article 17 gives the Member States the option of applying their own national law on criminal procedure when exercising the rights mentioned in Articles 11 through 16, where the personal data are contained in a judicial decision or record processed in the course of criminal investigations and proceedings. According to the Commission's interpretation expressed at the DAPIX meeting on 19–20 December 2012, Article 17 is not intended, despite its wording, to give the Member States any general authority to apply their own criminal procedural law to the rights of data subjects and in particular does not allow for any derogation from the articles in Chapter III; thus Article 17 must not be interpreted as an optionality clause for criminal proceedings, but as a purely declaratory provision which only leaves it up to the Member States to decide where exactly in their national law they will regulate the rights of access, information, rectification and erasure made binding by the Directive. Germany asks the Council's Legal Service for its opinion on this question. The Legal Service is also asked to address the following two questions in its opinion: Does Article 17 also cover data processing undertaken on the basis of a court order? Is it possible and reasonable to expand the optionality clause of Article 17 also to such data processing undertaken on the basis of a decision of the public prosecutor's office which is subject to judicial review?

CHAPTER IV

CONTROLLER AND PROCESSOR

SECTION 1

GENERAL OBLIGATIONS

Article 18

Obligations of the controller

1. Member States shall provide that the controller implements appropriate measures and be able to demonstrate that the processing of personal data is performed in compliance[1] with the provisions adopted pursuant to this Directive.

1a. Where proportionate in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller[2].

2. The measures referred to in paragraph 1 shall in particular include:

(a) keeping the documentation referred to in Article 23;

(b) complying with the requirements for prior consultation pursuant to Article 26;

(c) implementing the data security requirements laid down in Article 27;

(d) designating a data protection officer pursuant to Article 30.[3]

[1] ~~(...)~~

---

1 In our view, it remains unclear which specific conditions the new obligation to demonstrate compliance can, may and must meet. In particular, it is not clear how this obligation relates to the documentation and logging obligations in articles 23 and 24.

2 Germany is pleased that the obligation to develop appropriate data protection policies in the revised Article 18 (1a) is now more clearly based on the principle of proportionality. However, in our view it is still unclear what is meant by "policies" and what significance this term has next to the "measures" referred to in Article 18 (1) and (1a). The added value of this paragraph cannot be determined until this matter has been clarified.

3 Restoration of Article 18 (2) in the Commission's version. This seems helpful to specify the undefined legal term "measures" as far as possible.

Article 19

Data protection by design and by default[2]

1. In automated processing systems Member States shall provide that, having regard to available technology and the cost of implementation and taking account of the risks for rights and freedoms of individuals posed by the nature, scope and purpose of the processing, the controller shall implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of provisions adopted pursuant to this Directive and protect the rights of the data subject.

2. In automated processing systems t~~T~~he controller shall implement, as far as is feasible and appropriate, mechanisms for ensuring that, by default, only those personal data which are necessary for the purposes of the processing are processed.[3]

Article 20

Joint controllers[4]

Member States shall provide that where a controller determines the purposes (…) and means of the processing of personal data jointly with others, the joint controllers must determine the respective responsibilities for compliance with the provisions adopted pursuant to this Directive, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them, unless the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject[5].

---

1 We agree with the deletion of the vague Article 18 (3).

2 In Germany's view, it is still unclear what is meant by "mechanisms" in Article 19 (2). In any case, the organizational measures mentioned in Article 19 (1) are required only "in automated processing systems" and only "as far as is feasible and appropriate".

3 Germany maintains a scrutiny reservation, among other things because with reference to Article 19 it has not yet been decided whether appropriate examples could be added to the principle of data protection by design (e.g. examples which could address the separate processing of data stored for different purposes or the extent of search functions).

4 Germany enters a scrutiny reservation.

5 We agree that the division of responsibility resulting from the addition to Article 20 can be determined by law and not only by private arrangement.

Article 21

Processor

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

2. Member States shall provide that the carrying out of processing by a processor must ~~shall~~ be governed by a legal ~~act~~ provision or contract binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller (…)[2].

3. (…)[3]

Article 22

Processing under the authority of the controller and processor

(…)

---

1 Germany maintains a scrutiny reservation, among other things because it has not yet been decided whether the principle of Article 21 (1) should be extended to cases in which IT systems are maintained by external firms.

2 Germany agrees with the deletion of the second clause ("in particular, where the transfer of the personal data used is prohibited").

3 Germany agrees with the deletion of Article 21 (3), which seems unclear and illogical.

Article 23

Records of categories of personal data processing activities[1]

1. Member States shall provide that each controller and processor shall maintain a record of all processing systems (…)[2] under their responsibility.

2. (…)

3. The controller and the processor shall make such records available, on request, to the supervisory authority.

Article 24

Logging[3]

1. In automated processing systems all transmissions of personal data shall be logged or documented for the purposes of verifying the lawfulness of the data processing, self-monitoring and proper data integrity and security.

~~1. Member States shall ensure that logs are kept of at least the following processing operations: collection, alteration, consultation, disclosure, combination or erasure in automated processing systems. The logs of consultation and disclosure shall show (…) the purpose, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data.~~

---

1 Article 23 and especially Article 24 derogate from the documentation obligation in Article 10 of Framework Decision 2008/977/JHA and that of Article 28 of the Regulation. Germany believes it is not necessary to make the documentation obligations stricter in this way, and therefore opposes doing so. And the terminology in both articles is still vague and therefore problematic.

2 Germany agrees with deleting "procedures".

3 Also in the Presidency's revised version, Article 24 (1) stipulated extensive obligations for documenting individual processing operations; these obligations are not found in the General Data Protection Regulation. Although it welcomes the Presidency's restriction to "automatic processing systems", the German delegation takes a critical view of such an isolated introduction of documentation obligations exclusively for the area of police and criminal prosecution and does not believe it is justified. The new provisions Germany has added instead correspond to Article 10 of Framework Decision 2008/977/JHA. Germany has not yet concluded its deliberations as to whether the obligation to document is to be introduced for all transmissions or only in automated processing systems.

2. Logs or documentation prepared under paragraph 1 shall be communicated on request to the competent supervisory authority to monitor data protection. The competent supervisory authority shall use ~~The logs shall be used~~ this information only to monitor data protection and ensure proper ~~(…) for the purposes of verification of the lawfulness of the~~ data processing as well as, ~~self monitoring and for ensuring~~ data integrity and data security.

Article 25
Cooperation with the supervisory authority

(…)

Article 26

Prior consultation of the supervisory authority[1]

2. Member States shall ensure that the controller or the processor consults the supervisory authority prior to the processing of personal data which will form part of a new automated[2] filing system to be created where:

(a) significant quantities of[3] special categories of personal data referred to in Article 8 are to be processed;

(b) the type of processing, in particular where using new technologies, mechanisms or procedures, involves specific risks for the (…) rights and freedoms (…) of data subjects.

---

1 Regardless of the revisions suggested here, Germany is still examining whether the effort required by the provision is proportionate to the benefit it provides.

2 Non-automated files and filing systems do not pose any threat justifying prior consultation of the supervisory authority.

3 A single incidence of processing individual sensitive data must not be subject to the obligation of prior consultation. A practical limitation is needed here. Further, it is necessary to consider whether a limitation is appropriate for those files which are kept only a short time before being erased.

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

3. Member States shall provide that where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 does not comply with the provisions adopted pursuant to this Directive, in particular where risks are insufficiently identified or mitigated, it shall within a maximum period of 6 weeks following the request for consultation give advice to the data controller. This period may be extended for a further month, taking into account the complexity of the intended processing.[2]

4. Member States may provide that the controller or processor may consult the supervisory authority without undue delay after the the processing referred to in paragraph 1, if otherwise serious disadvantages for the purposes mentioned in Article 1 (1) are expected.[3]

---

[1] Paragraph 2 has been deleted, because it is purely declaratory and therefore unnecessary. Member States of course have the option to enact legislation to this effect without the Directive having to mention it.

[2] We approve the addition of Article 26 (3). If prior consultation of the supervisory authority is required, it must not lead to unnecessary delays.

[3] A provision on urgent cases is needed.

SECTION 2

DATA SECURITY

Article 27

Security of processing[1]

1. Having regard to available technology and the costs of implementation and taking into account the nature, context, scope and purposes of the processing and the risks for the rights and freedoms of data subjects, Member States shall provide that the controller and the processor implement appropriate technical and organisational measures to ensure a level of security appropriate to these risks (…).

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

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

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

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

---

1 Because of its similarity to Article 22 of Framework Decision 2008/977/JHA we have no objections to Article 27. We welcome the fact that the provision takes into account the available technology and weighs the costs of protective measures against the risks of processing. The provision is technology-neutral, which makes sense given the rapid development of technology.

2 The criteria and conditions for the risk evaluation are still unclear. No unnecessary burdens should be created. The main thing is that the measures described in detail in (a) through (j) are carried out.

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

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

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

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

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

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

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

3. (…)[1]

[1] We agree with the deletion of Article 27 (3). With regard to technical data protection, specifying detailed requirements in implementing acts makes little sense and would ultimately violate the principle of technology neutrality.

Article 28

Notification of a personal data breach to the supervisory authority[1]

1. Member States shall provide that in the case of a personal data breach which is likely to severely affect the rights and freedoms of data subjects[2], the controller notifies, without undue delay (…) the personal data breach to the supervisory authority (…).

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

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

3. The notification referred to in paragraph 1 shall at least describe the nature of the personal data breach, the likely consequences of the personal data breach identified by the controller, and the measures taken or proposed to be taken by the controller to address the personal data breach[4]. (…)

---

1 The revisions by the Irish Presidency have made improvements (in particular, we welcome the deletion of the 24-hour deadline given in the Commission's draft, as such a short deadline would be impossible to meet in practice). However, the revisions do not resolve the reservations concerning this provision. The breadth of Article 28 remains unclear. From its position within the Directive, one might think that the obligation to notify only applied when rules of technical data protection were violated. But the text clearly goes further in referring to a "personal data breach". It is necessary to ensure that the notifications and their handling by the supervisory authorities endanger neither the legitimate interests of third parties nor police and judicial interests.

2 We agree with the addition to Article 28 (1). The obligation in the Commission draft to report all breaches to the supervisory authority would go too far. It is preferable to take into account the risk associated with the specific breach.

3 In Germany's view, it would seem preferable to insert Article 29 (3) (a) and (b) here in order to avoid a reference to subsequent text.

4 If, in the version revised by the Irish Presidency, the notification under Article 28 (3) is supposed to describe the likely consequences and the measures taken or proposed to address it, further review is required. The review must focus on whether the provision threatens to create bureaucratic requirements that could get in the way of the actions urgently needed in such situations: actually containing the damage that has already happened or is happening, ultimately to the detriment of the data subjects.

4. Member States shall provide that the controller documents any personal data breaches referred to in paragraph 1, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose[1].

4a.[2] In the event that proceedings must be brought against a controller or processor on account of a violation of duty which necessitates the measures under Articles 28 or 29, Member States may provide that the measures taken by the controller and processor under Article 28 and 29 may not be used in these proceedings.

5. (…)

6. (…)[3]

[1] Germany is still examining whether the documentation obligation in Article 28 (4) makes sense in view of the obligation to notify the supervisory authority and the data subjects.

[2] This addition is necessary because the obligation to incriminate oneself may be problematic in terms of fundamental rights.

[3] We agree with the deletion of Article 28 (5) and (6).

Article 29

Communication of a personal data breach to the data subject[1]

1. Subject to paragraphs 3 and 4 of this Article, Member States shall provide that when the personal data breach is likely to severely affect the rights and freedoms (…) of the data subject, the controller shall, after the notification referred to in Article 28, communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and communicate the identity and contact details of the data protection officer referred to in Article 30 or other contact point where more information can be obtained[2] (…).

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

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

---

1 The remarks made concerning Article 28 also apply to Article 29. The provision would introduce an instrument which, at least in Germany, is only intended for private bodies. Applying this concept also to the police and judicial authorities, as intended by Article 29, requires intensive examination. In particular, it is necessary to examine whether doing so would ignore significant differences between the public and private sectors. Greater scrutiny is also needed to determine whether "negative publicity" can have impacts on security authorities similar to those in the private sector, and whether it even seems reasonable and advisable, given that public administration is bound by the law and in view of the existing mechanisms for legal and technical supervision and the possibility of judicial review. Lastly, it is also necessary to determine the extent to which notifying data subjects would interfere with the work of the police and judicial authorities.

2 Germany is still examining whether the obligation to recommend to the data subject measures to limit the possible damage could be added to paragraph 2.

3 In terms of content, we agree with the deletion in Article 29 (3) (a) and with the new Article 29 (3) (b) and (c). If the content of Article 29 (3) (a) and (b) is moved to Article 28 (1a) as suggested by Germany, a reference to Article 28 (1a) would then be needed here.

(b) the controller has taken subsequent measures which ensure that the data subjects' rights and freedoms are no longer likely to be severely affected; or

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

4. The communication to the data subject referred to in paragraph 1 may be delayed, restricted or omitted on the grounds referred to in Article 11b.

SECTION 3

DATA PROTECTION OFFICER

Article 30

Designation of the data protection officer[1]

1. ~~Union law or~~ Member State law ~~may~~ shall provide that the controller or the processor designates a data protection officer.

3. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 32.

4. A single data protection officer may be designated for several competent public authorities, taking account of their organisational structure (…) and size.

[1] The designation of a data protection officer should be mandatory, because this officer can exert valuable influence to ensure proper data processing. However, it is still necessary to examine whether additional instruments (already standard practice in Germany) to protect government data protection officers should be adopted, such as special protection against dismissal and discrimination (see the German proposal for Article 31), or whether the rules for data protection officers in paragraphs 7 through 10 in Article 35 of the General Data Protection Regulation could be included in a suitable place in the Directive.

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

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

Article 31

Position of the data protection officer

The data protection officer shall suffer no disadvantage through the performance of his duties.

(…)

Article 32

Tasks of the data protection officer

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

(b) to inform and advise the controller or the processor of their obligations in accordance with the provisions adopted pursuant to this Directive (…);

(b) to monitor compliance with provisions adopted pursuant to this Directive[1] and with (…) the policies in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in the processing operations and the related audits;

[1] We agree with the addition to Article 32 (b) describing the tasks of the data protection officer in terms both general and sufficiently specific. In our view, the other revisions to Article 32 (b) and the deletion of (c) through (f) follow from this addition and do not affect the content.

(c) (…)

(d) (…)

(e) (…)

(f) (…)

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

(h) to act as the contact point for the supervisory authority on issues related to the processing of personal data and consult, (…) as appropriate, on any other matter[1] (…)

[1] We have no objections to the revisions to Article 32 (h). However, we feel that clarification is needed as to whether "consult" here means only the prior consultation referred to in Article 26 or whether data protection officers are supposed to have the general option of proactively consulting the supervisory authority.

GERMANY

Annex to comments of the Federal Republic of Germany

– More detailed remarks on selected problem areas of the draft Directive –

Overview:

1. Minimum standards instead of full harmonization
2. Inclusion of threat prevention (at the same time: Delimitation of Directive and General Data Protection Regulation)
3. Data exchange within the EU
4. Consent of data subjects
5. Processing of special categories of personal data
6. Right of information
7. Scope of Article 17
8. Remarks concerning the anticipated administrative costs as identified by the Commission

1. Minimum standards instead of full harmonization, Article 1 (3)

Germany opposes full harmonization in the area of police and the judiciary and instead is in favour of defining only minimum standards at a high level of protection. In line with the philosophy anchored in Articles 1 (5) and 12 of Framework Decision 2008/977/JHA, the Member States should not be be prevented from enacting stricter national data protection legislation which other Member States would then have to abide by when data are transmitted to them. This philosophy prevents data protection from being undermined without interfering with the Member States' cultural and legal traditions concerning the police and judiciary. By contrast, in the event of full harmonization, all Member States with higher data protection standards would be forced in the course of implementing the Directive to undertake legislative reforms which would reduce the level of national protection.

To this end, the proposed paragraph 3 should be added to Article 1. Further, all passages in the Directive implying full harmonization will have to be revised, including recital 12, referring to the "*same level of protection*".

2. Inclusion of threat prevention (at the same time: Delimitation of Directive and General Data Protection Regulation, Article 1 (1)

With regard to threat prevention by the police, it is very difficult to distinguish between the scope of the Directive and that of the Regulation. Because the Directive in its current version applies only to the prevention and prosecution of "criminal offences", key areas of police work would come under the Regulation: Police are responsible not only for preventing and prosecuting criminal offences but also for averting other threats to public security and order regardless of whether the threat in question is punishable. The same applies to the customs authorities. Germany finds it unacceptable to apply the Regulation to threat prevention by police and customs because the Regulation has no provisions which would adequately address the special nature of threat prevention.

Specifically, the following examples may serve to illustrate: If the threat to be averted is not a punishable offence, as may happen in the case of aviation security or border protection, and thus the police are not preventing criminal offences as defined in Article 1 (1) of the proposed Directive, then the Directive would not apply. Countless other examples from everyday police work could be cited. If, in accordance with current proposals, the General Data Protection Regulation applies in such cases, it seems entirely unsuitable for the area of threat prevention and its specific characteristics. We therefore oppose applying the General Data Protection Regulation to the police sector.

Further, it is often impossible to distinguish clearly between the prevention and prosecution of criminal offences (Directive) and other, non-punishable threats (Regulation). For example, when a dead body is found, it must first be determined whether (punishable) foul play or only (non-punishable, at least in Germany) suicide was involved. When a person is reported missing, it is of course impossible to say whether he or she has been kidnapped or even murdered, or whether no crime is involved. Similar problems would arise in cross-border cases, when the same act may be punishable in one Member State and not punishable in another (e.g. suicide, hit-and-run driving). Nor is it clear what should be done if an act is punishable in the abstract but cannot be prosecuted in the concrete case. Such constellations may occur if there is legal justification for the act, when the perpetrator acts without culpability or is below the age of criminal responsibility, or in the event of an absolute procedural impediment. Special problems may arise in international cases, if Member State criminal law or criminal procedural law differ, for example when it comes to the justification of punishable acts.

Lastly, a serious problem is the fact that, in the context of threat prevention by the police, it is very difficult in fact to determine with the desirable clarity when the line is crossed between criminal offences (Directive) and non-punishable preparatory actions which are nonetheless relevant for police prevention of threats to public security and order (Regulation). It does not make much sense for the same police officer on the same case to be governed first by the Regulation and then – at some point difficult to determine – by the Directive.

In the current law, two different European legal instruments (Directive 95/46/EC and Framework Decision 2008/977/JHA) both had to be implemented in national law, enabling national legislators to resolve issues of when which law applies. By contrast, with the new Directive and Regulation, such issues would be open and impossible to resolve: The General Data Protection Regulation will be directly applicable, while the Data Protection Directive will have to be implemented in national law. As a result, law at two different hierarchy levels would be affected. The national legislators of the Member States would not be able to set boundaries between the two.

Following the explanations given here, what is needed is a real, i.e. constitutive, expansion of the scope of the Directive, accompanied by a corresponding reduction in the scope of the Regulation. Like the proposal made by the Romanian Delegation on 8 April 2013 (Doc. 8208/13), Germany finds it necessary for subject-related and legal reasons for the Directive to cover general threat prevention by the police, i.e. regardless of whether legal assets protected by criminal law are at issue. To do so, appropriate wording must be found to expand the scope of the Directive to include data processing for purposes of maintaining and assuring the public security and order by the police. This wording must also include the customs authorities, where the same problem arises. At the same time, it is necessary to keep the scope of the Directive from expanding excessively. In their necessary consideration of the problem the Member States could start with the wording given here in square brackets, which is based on the Romanian proposal ("*and for the purposes of maintaining and assuring the public security and order by the police and customs*"). The question whether the added phrase "by the police and customs" is sufficient to address the concerns noted here will require further discussion, particularly among the Member States.

The addition in square brackets to Article 1 (1) of the draft Directive as revised by the Irish Presidency is not suitable for resolving the issue of delimitation ("*and for these purposes, the maintenance of public order*"), because this addition does not change the scope of the Directive. On the contrary, the unambiguous wording ("*and for these purposes*") makes it clear without a doubt that only a (purely declaratory) clarification *within* the scope proposed in the Commission's original draft is intended.

3. Data exchange within the EU, Article 1 (2) (b) and Article 7a

According to Article 1 (2) (b), the exchange of personal data should be "*neither restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data*". This could be interpreted to mean that in future, a lower level of data protection will no longer be sufficient reason to prohibit the transmission of personal data to another Member State or limit it by attaching conditions to the further processing of transmitted data. This would be incompatible with the demand that the Directive should only set minimum standards and would also assume a uniform, EU-wide level of data protection which the Directive does not bring about.

According to the Commission's draft, (further) processing of data transmitted within the EU is subject only to the general conditions of lawfulness given in Article 7. In derogation from the current Articles 11 and 12 of Framework Decision 2008/977/JHA, after being transmitted within the EU personal data could then be used without regard for any processing restrictions applicable in the transmitting Member State. Data transmission within the EU could cancel out even central principles of national law on threat prevention and criminal procedure if these principles do not exist in the receiving Member State. This could affect rules on confidentiality (official secrecy, professional secrecy, tax secrecy, confidentiality of social welfare data, etc.) or rules prohibiting the disclosure of data which could endanger the purpose of the investigation or an individual (such as a witness). Regardless of their significance in police or criminal procedural law, such rules could always be seen as restrictions on processing under data protection law, which are to be disregarded under Articles 1 (2). This would give data protection law aspects an impermissible dominance over police and criminal procedural law.

For this reason, Member States must be able to require other Member States to comply with their national restrictions on processing, for example on using data gathered from telecommunications interception for purposes other than those for which they were collected. The addition to Article 1 (2) (b) makes this clear.

While the addition of a new Article 7a in the Presidency's revised version (Doc. 11624/13) points in the right direction, it does not entirely resolve the problem: The scope of Article 7a is too broad, as it also covers purely national data transfers. It is also unclear which cases the "specific conditions" in Article 7a are supposed to cover, in comparison to Article 1 (2) (b) which prohibits all restrictions or prohibitions on the exchange of data. Lastly, contrary to Article 1 (2) (b), it must be possible in certain cases to refuse the cross-border exchange of data. Article 7a does not provide for such refusal of data transmissions.

4. Consent of data subjects, Articles 3 (8a), 7 (1a) and 8 (2)

Articles 3 (8a), 7 (1a) and 8 (2) provide for the voluntary consent of data subjects as additional justification, as all individuals should in principle be able to freely control their data. This also corresponds to the intent of Article 8 (2) of the EU Charter of Fundamental Rights.

The consent of the data subject is essential in certain crucial areas, such as in prevention projects or when taking blood samples or conducting DNA tests. In German law, consent-based data processing is often a less bureaucratic alternative to a court order.

Because these solutions are crucial to police work, the consent of data subjects should be unambiguous and anchored in the draft Directive in a way that ensures legal certainty. In Germany's view, at the very least it is essential for the Member States not to be prevented from enacting laws declaring that data processing by the police and judiciary is lawful on the basis of voluntary consent of the data subject alone. Further review is required to determine whether consent solutions should be allowed which are not governed by special legislation on the discharge of police and judicial functions but only (as in Germany) by general data protection legislation.

5. Processing of special categories of personal data, Articles 8 and 3 (10)

Even though the data listed in Article 8 are certainly especially sensitive, Germany finds the absolute prohibition on processing these data in paragraph 1 to be too far-reaching and impractical. Especially in the area of law enforcement and threat prevention, it is necessary to process sensitive data in various ways.

The following examples may serve to illustrate: Genetic data are crucial for proving without a doubt that a particular person has committed a crime and that others have not (as to the latter they are thus essential for ending investigations of innocent persons). The DNA analysis database plays a key role in solving crimes; automated trace matching within the EU Member States in particular frequently helps identify perpetrators or links between cases. Prosecuting criminal offences of a sexual or extremist nature also depends on collecting sensitive data. Information about data subjects' religious affiliation is essential in the case of Islamist terrorism. The situation is similar with regard to right-wing extremism: It is often necessary to have access to information on the political views of a data subject in order to recognize racist, anti-Semitic or xenophobic individuals or groups. Information as to whether a suspect has an infectious disease, is a drug user or a sexual offender is also crucial to the safety of law enforcement officers and for preparing and conducting overt measures under the Code of Criminal Procedure. In criminal proceedings, the (health) status of those involved is often relevant, for example when judging a victim's injuries or whether a perpetrator can be found criminally responsible.

Processing special categories of personal data must therefore not be prohibited as a basic principle, but should only be limited to the extent which is strictly necessary. Taking into account the special sensitivity of the data, the provision should allow the processing if necessary to carry out the tasks of the relevant agencies.

It is still unclear what the term "appropriate safeguards" in Article 8 (2) (a) means. Among other things, it is unclear whether these safeguards must go beyond those that already apply to processing other data. It would also be helpful to clarify whether and to what extent these safeguards leave room to take opposing (i.e. police and judicial) interests adequately into account.

The exception in (b) seems too narrow, especially if the above-mentioned German proposal of Article 8 (1) is rejected. Exceptions should be possible not only to protect vital interests, but also when other high-priority legal interests (such as permanent loss of eyesight or other serious bodily injury) are affected.

We oppose deleting (c) of the Commission's draft allowing the processing of data published by data subjects themselves. Deleting this provision would result in the paradoxical situation in which the police and judiciary could not legally respond to data subjects' own announcements on the Internet of planned racially or religiously motivated terrorist attacks. The exception added in (c) for an immediate and serious threat to public security is welcome, although it still seems too narrow, at least if Germany's proposed revision of Article 8 (1) is rejected.

In connection with the concerns just expressed, the legal definition of "*genetic data*" in Article 3 (10) is also significant. Despite the Irish Presidency's welcome attempt at greater precision, the definition is still too undifferentiated or at least in need of clarification. Not all genetic data allow conclusions to be drawn about the data subject's personality. In Germany, for example, the police analyse only the non-coding components of human DNA. Although they may be individualized, they do not contain highly sensitive hereditary information. So it is impossible to draw conclusions about the genetic code and personal characteristics of the person in question. In terms of data protection law, the data subject therefore faces a much lower risk than if DNA components containing hereditary information are examined and analysed. Germany's proposed definition of "*genetic data*" is intended to take these distinctions into account.

6. Right of information, Articles 11, 11a and 11b

Germany continues to reject the notification obligations, in particular their current scale, in Articles 11, 11a and 11b. Although the clearly excessive scale of information obligations in the Commission's original proposal has been reduced through welcome deletions in Article 11 (1) and 11a (1), the provisions of the Commission's draft on limitations to the rights of information (Article 11b) have remained unchanged, leaving inter alia the large number of notifications to be made.

Overall, the major efforts required of public authorities are still disproportionate to the (at least partially) rather limited usefulness to data subjects of the information obligations. Even the revised version establishes very extensive and, for a directive, unusually detailed requirements concerning the information public authorities are to provide ex officio to data subjects. These provisions differ considerably from Article 16 of Framework Decision 2008/977/JHA. As a result, the draft Directive overshoots its target. The police and judiciary must not be hindered by excessive bureaucracy from carrying out their primary tasks. If notification requirements should be provided for at all, the Member States must be given much more discretion in formulating them.

Articles 11, 11a and 11b would result in practice in an unmanageable amount of information to be provided ex officio, which in some cases would be redundant. For example, a defendant in ordinary criminal proceedings in Germany would be notified up to six times that his or her information had been recorded (by the local police, in the central police register INPOL, by the public prosecutor's office, in the Central Public Prosecution Proceedings Register (ZStV), and by the local court and regional court). More information obligations would result if the case were transferred to another police station, customs authorities, public prosecutor or court, or if other institutions, such as the state criminal police office, juvenile court aid or probation assistance, were involved. The data subject would be flooded with notifications providing no additional value. But the administrative burden for the public authorities would be considerable. Case management often includes the complainant and/or victim, which would increase the information obligations exponentially.

For the police, too, the information obligations would create a massive bureaucratic burden, although it is naturally difficult to provide specific statistical data at the present time. A one-day test conducted by the Munich police headquarters demonstrated that, if the draft Directive were implemented, 2,100 police notifications would have to be sent every day, amounting to 766,500 notifications per year (for a population of 1,388,308 residents). Estimates from other German states confirm this tendency; in some cases, the number of notifications to be sent annually even exceeds the number of residents.

Further, in cross-border investigations the need would arise for a comprehensive obligation to inform persons in other Member States or third countries. The notifications in question would have to be sent to the relevant persons in other (European) countries; given the anticipated number of notifications, this would also lead to a disproportionate and overwhelming bureaucratic burden in this area.

We also fear that ex officio information obligations would make threat prevention and law enforcement in certain areas of crime much more difficult. Crime solving and threat prevention depend on information from tips, witnesses and persons filing complaints. Especially in cases of child abuse, violence against women, drug trafficking, corruption, tax fraud and the like, it is often possible to gain useful evidence only by guaranteeing complainants and informants that their information will be treated confidentially. This trust would be undermined by having to notify everyone involved in an investigation (even if the investigation never yielded any result). Such notification could also lead to reprisals or threats against witnesses and others furnishing information, made outside the protection of the investigating authority. This would seriously reduce the number of crimes solved in these already difficult areas.

It should also be considered that notifications would often have to be delayed on the grounds now given in Article 11b. However, this would not reduce burdens on the public authorities but on the contrary increase them, as repeated examination would be necessary to determine whether the delay was still required. In such cases, by the time the data subjects were notified, the information would have little value, since the proceedings would typically be completed by then.

For these reasons, the Member States should be given much more discretion in implementing Articles 11 and 11a. The Member States should therefore discuss appropriate limits and whether providing information should be obligatory or only discretionary.

If the Directive makes the provision of information to data subjects mandatory, the extent of these obligations and the timing of notification will have to be carefully re-examined. For example, Germany rejects the obligation newly included in the draft Directive that data subjects are to be informed at the latest when the data are disclosed to another recipient. This provision would unreasonably interfere with the work of the responsible authorities. For example, if a group of suspects and/or witnesses is to be questioned, it is often necessary to use information taken from statements of other involved persons which typically includes personal data. In such cases, it is impossible to inform the data subject when these data are disclosed.

Above all, however, additional exceptions from the right of information should be included in the draft Directive. Germany's proposal to add a paragraph 1a to Article 11b takes into account the fact that limitations on the right of information can be based not only on law enforcement- and security-specific grounds; general grounds are also conceivable. Data subjects need not be informed when the data subject's need for information has already been met ((a) and (b)) or when information need not be provided for other reasons (not specific to security) or the provision of information would not be proportionate ((c) through (e)).

7. Scope of Article 17

In Germany's view, Article 17, which is relevant for all of Chapter III, gives the Member States the option of applying their own national law on criminal procedure when exercising the rights mentioned in Articles 11 through 16, where the personal data are contained in a judicial decision or record processed in the course of criminal investigations and proceedings. According to the Commission's interpretation expressed at the DAPIX meeting on 19–20 December 2012, Article 17 is not intended, despite its wording, to give the Member States any general authority to apply their own criminal procedural law to the rights of data subjects and in particular does not allow for any derogation from the articles in Chapter III; thus Article 17 must not be interpreted as an optionality clause for criminal proceedings, but as a purely declaratory provision which only leaves it up to the Member States to decide where exactly in their national law they will regulate the rights of access, information, rectification and erasure made binding by the Directive.

Germany asks the Council's Legal Service for its opinion on this question. The Legal Service is also asked to address the following two questions in its opinion:

- Does Article 17 also cover data processing undertaken on the basis of a court order?
- Is it possible and reasonable to expand the optionality clause of Article 17 also to such data processing undertaken on the basis of a decision of the public prosecutor's office which is subject to judicial review?

8. Remarks concerning the anticipated administrative costs as identified by the Commission

Germany asks the Presidency to call on the Commission to present its impact assessment to the DAPIX Council Working Party.

According to the report on impact assessment within the Council (Council Doc 8406/13 of 15 April 2013), impact assessments are a key instrument for smart regulation. They are supposed to help in drafting regulation that is as effective as possible while minimizing administrative burdens. Accordingly, the Commission's impact assessments is to be discussed regularly and systematically in the Council. The Commission must have an opportunity to explain how the impact assessment supports its proposal. The delegations must be given the opportunity to ask the Commission for more information about its impact assessment, including the scope, thoroughness, methodology and data used.

In Germany's view, the Commission's conclusions on the anticipated administrative costs of the Directive are not sufficiently concrete or comprehensive, thus making it impossible to review the anticipated financial burdens to the necessary extent. Such a review is necessary not least due to the information, access and documentation obligations given in the draft Directive; complying with these obligations would require a great deal of time, money and bureaucratic effort.

The draft Directive itself does not contain any information on the financial implications of the proposal. It refers only to the financial statement for the proposal for a General Data Protection Regulation. However, this financial statement refers only to the General Data Protection Regulation and only addresses costs incurred by the Commission and the European Data Protection Supervisor. It lacks the necessary information specific to the Directive and addressing the Member States' administrative burdens.

Nor do the accompanying documents presented by the Commission contain any figures relevant to the Directive. The summary of the impact assessment states that the fragmentation of the legal framework has led to legal uncertainty and inconsistencies in data protection associated with costs of roughly €3 billion per year (p. 11) and that uniform, EU-wide regulation could reduce the administrative burden and result in cost savings of roughly €2.3 billion per year (p. 3). However, these statements clearly apply to the private sector, which is covered by the draft General Data Protection Regulation. The same is true of Annex 9 (Calculation of Administrative Costs in the Baseline Scenario and Preferred Option) and the corresponding costs sheet.

The impact assessment merely notes that the entire public sector was left out of the calculations "as no reliable statistics are available". For the area of police and judicial cooperation in criminal matters, the costs of information obligations resulting from Framework Decision 2008/977/JHA that involve administrative burdens on public authorities "were judged to be negligible, given the wide exemptions in this area" and thus no reliable conclusions could be drawn. Here, the Commission should take additional measures in order to provide information about the anticipated costs. Given its significantly expanded scope, the Directive can be expected to result in much higher costs than Framework Decision 2008/977/JHA. It also contains much more extensive information and access obligations. The Member States have repeatedly criticized the draft Directive as excessively bureaucratic.

Further, we are concerned that the Commission is creating the impression that the main issue is the financial implications of European data protection reform as a whole, and that the General Data Protection Regulation and Directive can be regarded from an overall perspective. The Commission is operating on a false assumption. The General Data Protection Regulation and the Directive are two very different legislative acts. They regulate different matters for different addressees of legal norms and pursue different goals. They must therefore be treated separately when it comes to estimating their administrative costs. In particular, it would not be permitted to apply any cost savings (ostensibly) resulting from the General Data Protection Regulation to the costs of the Directive.

SPAIN

1. Introduction

The Spanish delegation's comments are in two parts.

The first part, which can be found in this document, includes the "general comments". The general comments concern the entire instrument.

The second part, which can be found in an Excel file, contains the specific amendments and suggestions proposed, and concern particular sections of the instrument, whether recitals or articles.

2. General comments

Spain maintains its scrutiny reservation on the whole of the instrument.

We still have significant doubts about the relevance of this Commission initiative given the existence of Framework Decision 2008/977/JHA, which in our experience adequately addresses the issues of privacy that arise from data processing in the context of judicial and criminal cooperation.

In our opinion, there is currently no pressing need to regulate these aspects any further at EU level. In any case we consider that, in accordance with the principle of subsidiarity, the approach should be the same as for the above Framework Decision, i.e. to regulate cross-border processing only.

The internal data processing that the Directive now attempts to regulate has a strategic scope which is particularly relevant to each Member State, and also has specific national features that must be taken into account. This means that in this case the proposed objectives are unlikely to be better achieved at Union level, within the meaning of Article 5(3) TEU.

We also consider that the issue relating to "public order" needs to be resolved. In order to determine whether or not the processing relating to "public order" is covered by the Directive, we require either a definition of what is meant by "public order" or clear confirmation that this definition will be left up to the Member States when they come to transpose the Directive.

Finally, from a procedural point of view we do not see much sense in trying to make substantial progress on the negotiation of this Directive until we have firm and definitive solutions for the Regulation in areas that they have in common. That is why our delegation would prefer to focus on the Regulation for the time being, since we also consider that this instrument is the clear priority.

CROATIA

Article 2

Scope

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

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

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

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

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

- Paragraph 1 - unlike the Framework Decision 2008/977/JHA the Draft Directive is not limited to the exchange of personal data between Member States, but also includes the processing of personal data by competent national authorities, therefore, relates to the processing of personal data within member States, substantially expanding the scope of the Draft Directive; this scope of application and its justification should be further considered;

Article 3

Definitions

For the purposes of this Directive:

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

(…)

(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 (…) or (…) erasure;

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

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

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

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

(8) 'recipient' means a natural 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;

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

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

(11) 'biometric data' means any personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual, such as facial images, or dactyloscopic data;

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

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

(…)

(14) 'competent public authority' means any authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

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

- Item 5. definition of "filing system" needs to be further specified, the question is whether it also includes case files assembled by the police, prosecution and / or courts in paper form (if the definition also includes such documents, the provisions of the Directive, pursuant to Article 2, paragraph 2, would be applied to all records of these bodies because they necessarily contain certain personal information);

Article 7

Lawfulness of processing

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

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

(…)

€ in order to protect the vital interests of the data subject or of another person; or

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

2. Member States shall provide that the controller may further process personal data for historical, statistical or scientific purposes, subject to appropriate safeguads for the rights and freedoms of data subjects.

- It is proposed to consider the consent of the person the data relates to as the basis for the processing of personal data;

Article 8

Processing of special categories of personal data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

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

(b) 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 and serious threat to public security.

Ban of the processing of personal data relating to racial or ethnic origin, political beliefs, religious or philosophical beliefs or trade union membership, with exceptions provided for, seems reasonable. However, we emphasize that processing of personal data concerning health or sex life (as an exception, under the conditions explicitly prescribed by the law), should be allowed; for example, in cases related to crimes against sexual freedom personal data concerning health and sexual life will be collected on a regular basis. An absolute ban on the processing of this data would be unacceptable, especially if the information is necessary to prove the offense. Also it is necessary to draw attention that the data concerning the health status is regularly processed during the execution of criminal sanctions, therefore processing of such data should not be restricted more than necessary;

The issue of collecting, processing, use and storage of data obtained by molecular - genetic analysis ("genetic data") needs to be further clarified, as data in question is often necessary for establishing the identity of the persons, in particular the identity of the suspect, and thus has great significance for the successful conduct of criminal proceedings. Such information in regard to the degree of intrusion into the private sphere of the individual must have a stronger degree of protection; however, the use of such data for lawful purposes should be enabled.

The term "appropriate safeguards" in paragraph 2 (a) (which is used in Article 9, paragraph 1) in our opinion should be defined more clearly.

The question remains whether the processing of personal data under Article 8 should be allowed if there is consent of the person to whom the data relates, for example, the consent of the victim of the crime.

Article 11

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

1. Subject to Article 11b, Member States shall provide that where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with *at least* the following information:

(a) the identity and the contact details of the controller and, if any, of the data protection officer;

(aa) whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data; and

(b) the purposes of the processing for which the personal data are intended;

€ (…)

(d) (…)

€ the right to lodge a complaint to a supervisory authority (…).

(h) (…)

(i) (…).

6. (…)

7. (…)

8. (…)

9. (…)

Article 11a

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

1. Subject to Article 11b, Member States shall provide that where personal data have not been obtained from the data subject, the controller shall provide the data subject with at least the following information:

(a)the identity and the contact details of the controller and, if any, of the data protection officer;

(b)the categories of personal data concerned;

€the purposes of the processing for which the personal data are intended;

(d)the right to lodge a complaint to a supervisory authority.

2. The controller shall provide the information referred to in paragraph 1:

(a)within a reasonable period after obtaining the data, having regard to the specific circumstances in which the data are processed, or

(b) if a disclosure to another recipient is envisaged, at the latest when the data are first disclosed.

Article 11b

Limitations to the rights of information

1. Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to Article 11 and 11a to the extent that, and as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the individual concerned:

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

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

   € to protect public security;

   (d) to protect national security;

   € to protect the rights and freedoms of others.

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

We propose to add item "h" to Article 11, paragraph 1:

" (h) The legal basis for the processing of personal data in cases where the collection of such data is mandatory."

Providing detailed information listed in these articles should be associated with the request of the person to whom the collected personal data relate. Giving this information, ex officio, would be burdensome to the authorities;

It is questionable whether the police authorities (which fall under the definition of "controller" in accordance with Article 3 (6) of the motion) should be required to inform the person to whom the data relates of the fact that such data is collected, since it may jeopardize the interests of the criminal proceedings.

It should be noted that Article 11b leaves broad discretion to prescribe delay, limit or deny this right when it is necessary and appropriate for the reasons given in the cited article;

Article 12

Right of access for the data subject

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

(a) the purposes of the processing;

(b)(…)

€ the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular the recipients in third countries;

(d) where possible, the envisaged period for which the personal data will be stored;

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

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

(g)(…)

1a. Member States shall provide that where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 35 relating to the transfer.

2. (…)

Article 13

Limitations to the right of access

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

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

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

   € to protect public security;

   (d) to protect national security;

   € to protect the rights and freedoms of others.

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

3. In cases referred to in paragraphs 1 and 2, Member States shall provide that the controller informs the data subject (…) of any refusal or restriction of access, of the reasons for the refusal and of the possibilities of lodging a complaint to the supervisory authority [and seeking a judicial remedy]. This shall not apply (…) where the provision of such information would undermine a purpose under paragraph 1.

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

The right of access to information in art. 12 should be limited to the right of notification of whether personal data of a specific person is processed by the authority and for what purpose. Of course, all at the request of the person to whom personal data to be processed relates, and not ex officio;

Article 13 contains restrictions that seem justified

Article 15

Right to rectification, erasure and restriction of processing

1. Having regard to the nature and purpose of the processing concerned, Member States shall provide for the right of the data subject to obtain from the controller the rectification of personal data relating to him or her which are inaccurate and (…) the right to obtain completion of incomplete personal data, including by means of providing a supplementary statement.

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

1b. Member States shall provide for the right of the data subject to obtain from the controller the restriction of the processing of personal data where their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data, or where they are required by the data subject for the establishment, exercise or defence of legal claims.

2. Member States shall provide that the controller informs the data subject (…) of any refusal of rectification, erasure or restriction of the processing, the reasons for the refusal and the possibilities of lodging a complaint to the supervisory authority [and seeking a judicial remedy].

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

*We propose the rectification, erasure and restriction of the processing of personal data to be conducted only **ex officio,** because the solution presented in proposed Directive could compromise the effectiveness of the criminal proceedings.*

In paragraph 1, after the words "relating to him or her which is" the phrase "in any way" should be added, "inaccurate" left and "false, incomplete, inaccurate, outdated, etc.)" added in parenthesis.

Article 28

Notification of a personal data breach to the supervisory authority

1. Member States shall provide that in the case of a personal data breach which is likely to severely affect the rights and freedoms of data subjects, the controller notifies, without undue delay (…) the personal data breach to the supervisory authority (…).

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

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

3. The notification referred to in paragraph 1 shall at least describe the nature of the personal data breach, the likely consequences of the personal data breach identified by the controller, and the measures taken or proposed to be taken by the controller to address the personal data breach. (…)

4. Member States shall provide that the controller documents any personal data breaches referred to in paragraph 1, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.

5. (…)

6. (…)

After paragraph 4 we propose to add a paragraph 5, which would read:

Competent authority monitors the protection of personal data at the request of the respondents, on a proposal from a third party or ex officio.

ITALY

First of all, we maintain a scrutiny reservation on the entire text and believe that the DAPIX Working Party should continue to examine the proposal for a Directive alongside its analysis of the proposal for a Regulation, in order to maintain as much coherence and synergy between the two texts as possible, and given that their scopes are complementary. It should in fact be taken into account that even though, according to the EU Treaties, certain matters (such as border control, immigration and asylum policy, procedures for issuing passports, residence permits, visas etc.) are not considered law enforcement activities per se, but rather administrative activities, specific decisions have nevertheless been adopted to establish the methods, procedures and guarantees for access to data collected for the purpose of these activities, as well as for subsequent use of these data by the police and other law enforcement agencies. (see, for example, decisions on law enforcement agencies' access to the VIS and Eurodac).

Article 1 (linked to recital 7)

We confirm our earlier comments in which we asked for clarification of the concept of "competent authority for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties", in order to precisely define the scope of the Directive's principles, and the interaction between the Directive and Regulation in cases in which the same authority carries out activities in several different fields, partly governed by the Directive and partly by the Regulation. We also welcome the addition of the word "public" to "competent authorities", highlighting that the "prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties" are the duties of a State authority. It does in fact seem necessary to emphasise that the above duties are entrusted to the State and to the bodies empowered by national law to fulfil them, without this undermining their essentially "public" nature.

Indeed, when some or all of these public duties are entrusted to private entities, clear principles and the necessary guarantees must be established for any personal data processing carried out by these entities. Specific provisions should therefore be added to the text to indicate that private entities (subcontractors, outsourcers, cloud providers, contractors) should, according to their level of decision-making in relation to data collection and use, be considered joint controllers or controllers (and therefore subject to the provisions of Articles 20 and/or 21) or, if the private nature of these entities is predominant for the activities for which the processing is taking place, provisions should ensure that they are governed by the future Regulation (potentially with the safeguards considered necessary under Article 21 of the current proposal).

Since it is difficult to distinguish between purely administrative tasks and tasks relating to the prevention, investigation, detection or prosecution of criminal offences, the two texts - Directive and Regulation - must be as consistent as possible, and as clear as possible on the tasks entrusted to the competence/responsibility of public authorities to which the Directive should apply.

In this respect we welcome the proposal to make reference to the maintenance of public order, although only with the due safeguards, to avoid this bringing under the scope of the Directive all those activities carried out by law enforcement agencies which are not strictly connected to the existence of a criminal investigation.

We do not believe the wording used in paragraph 2(b) is suitable for the activities included in the scope of the Directive, since it should also provide for the possibility that Member States may introduce or maintain more protective provisions (de minimis approach).

Article 2

Our previous comments also apply to this article, as we believe the meaning of "competent authority" needs to be specified in order to precisely define the scope of the Directive's principles. Clarification is still needed of which activities carried out by which bodies are considered "outside the scope of Union law" as set out in paragraph 3(a), possibly by including an indicative list. Finally, we would like the relationship between Article 2(3)(b) and Article 59 to be made clear.

Article 3

We advocate ensuring that the definitions which appear in the Directive and in the Regulation are identical, in the interests of consistency and uniformity of application, and therefore advise that Article 3 of the Directive should be and remain aligned with the corresponding article of the Regulation. We agree with the insertion of a definition of competent authority, but the definition given in paragraph 14 should be improved (for instance "authority on which national legislation confers the competence to …" or "institutionally competent to ...").
We do not agree with the suggestion made by some delegations to insert a provision relating to consent-based data processing, given that, in the cases which should be governed by the Directive, the legal basis for data processing is not consent but the law.

Article 4

We request the reinsertion of the adjective "fairly" as suggested in the Commission's initial proposal and provided for in the Regulation.
We also ask for an amendment to Article 4(e), linking the period for which data can be kept with the objectives of the Directive as set out in Article 1 ("prevention, investigation, detection or prosecution of criminal offences, and for these purposes the maintenance of public order or the execution of criminal penalties"), and with the purposes for which the personal data were collected.

Article 7

The tasks referred to in paragraphs (c) and (d) should be covered by paragraph (a) and should be attributed to the competence of the authority carrying out the processing (for example processing the data of cooperative subjects, including changes to personal details, etc.).
This is a key article for the enacting terms and must therefore be worded very carefully. We could consider a wording along the lines of "for the performance of tasks specifically attributed by Union law or national law to the competent public authority".

HUNGARY

Hungary retains its comments on Articles 1-8 of the proposal. Further to these comments submitted in November 2012, we would like to express the following non-exhaustive remarks to the Document 11624/1/13.

Chapter I

- Hungary does not agree with the deletion of the term ‘restriction’ and ‘destruction’ in the definition of processing in Article 3 (3) of the draft directive, as it might result in the contraction of the notion of data processing. Therefore Hungary suggests to restore the deleted terms as it is applied in the Framework Decision 2008/977/JHA (hereafter: FD) as well.

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

- Hungary is of the opinion that so as to ensure the due compliancy in terminology, it is worth monitoring the pieces of legislation being done in other working groups concerning criminal investigation (i.e. the Europol regulation). Also with this end in view, Hungary does not see any substantial legal reason behind using the term ‘restriction of processing’ instead of ‘blocking’, whereas the latter is used in both the FD and the Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA. Furthermore, there is no difference between the definitions of the two concepts.

Therefore Hungary suggests the following wording in Article 3 (4) of the draft directive:

~~'restriction of processing'~~ 'blocking' means the marking of stored personal data with the aim of limiting their processing in the future

Chapter II

- Albeit there is an implicit reference to the lawful duration of processing in Article 4 of the draft directive, Hungary suggests to complete point a) or add a new point which explicitly states it as follows:

  option Nr. 1

Member States shall provide that personal data must be: a) processed lawfully and to the extent and for the duration necessary to achieve its purpose;

  option Nr. 2

Member States shall provide that personal data must be: bb) processed only to the extent and for the duration necessary to achieve its purpose;

Chapter III

- In relation to Article 12 of the draft, Hungary requires further clarification on the notion of 'reasonable intervals', hence it suggests the following wording:

option Nr. 1

Subject to Article 13, Member States shall provide for the right of the data subject to obtain from the controller at reasonable intervals <u>defined by Member State's law</u> free of charge confirmation as to whether or not personal data relating to him or her are being processed, and where such personal data are being processed to obtain access to such data and the following information:

option Nr. 2 adds a new Paragraph to Article 12

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

In case of option Nr. 2, the numbering of the current Article 12 (1a) should be changed to Article 12 (1b) and a new Paragraph (1a) should be inserted as follows:

<u>(1a) The information described in Paragraph (1) shall be provided free of charge for any category of data once a year.</u>

- Hungary deems Article 17 of the draft to be supplemented with a reference to documents, registry and decisions of police and public prosecutors. Hungary finds no rationale behind the applicability of regime of access to data during criminal proceedings having been confined only to the judicial phase.

Therefore Hungary suggests the following wording in Article 17 of the draft directive:

Member States may provide that the exercise of the rights referred to in Articles 11, 11a, 12 and 15 is carried out in accordance with national rules on ~~judicial~~ criminal proceedings where the personal data are contained in a judicial, police and public prosecutorial decision or record processed in the course of criminal investigations and proceedings.

Chapter IV

- Hungary supports the inclusion of obligation imposed on the controller and the processor to consult the supervisory authority prior to the processing of personal data defined in Article 26 (1) of the draft directive. It still remains questionable whether this type of consultation has justification in case of data processing referred to in Article 7 (1) (a) where it is more viable that instead of the controller the legislator consults the supervisory authority.

  Therefore Hungary suggests supplementing Article 26 with Paragraph (1a) as follows:

(1a) In the case of processing referred to in Article 7 (1) a) Member States shall ensure that the legislator consults the supervisory authority prior to the adoption of a law concerning the processing of personal data referred to in paragraph (1).

AUSTRIA

General remarks

Austria welcomes a high standard of data protection, established in a comprehensive and coherent set of rules.

The areas affected by the above mentioned proposal are already subject
- to existing national data protection rules in each Member State,
- to the Rules established in the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,
- specifically with regard to police and criminal prosecution to the guidelines established in the Recommendation no. R (87) 15 of the (Council of Europe) Committee of Ministers to Member States regulating the use of personal data in the police sector,[1]
. and to the rules established by the Framework Decision 2008/977/JHA[2]

The Framework Decision 2008/977/JHA was the result of long and intensive negotiations and can be regarded as a solid compromise in a delicate field.

As shown by certain elements of the Commission's Proposal and by certain statements in the ongoing discussions, the proposal for enacting a new Directive involves the danger of triggering a development below the standards that have been secured in this important legal instrument.

Austria strongly advocates maintaining at least the level of data protection attained with the Framework Decision.

[1] http://www.coe.int/T/DG1/LegalCooperation/Economiccrime/organisedcrime/Rec_1987_15.pdf
[2] Council Framework Decision 2008/977/JHA of 27 November 2008, Official Journal 350 (30 December 2008), 60.

On general note, Austria would like to question why the words “and seeking of a judicial remedy” has been put between bracket throughout the text in the Presidency’s version. In Austria’s view, the brackets can be removed in order to express the fact that wherever data are used by the judiciary in their judicial function, the applicable remedy is not with the supervisory authority but with the applicable judicial remedy (as an example, see the Austrian proposal on Article 13).

Art. 1

[COM proposal, modified by PRES]

“Article 1 Subject matter and objectives
1. This Directive lays down the rules relating to the protection of individuals with regard to the processing of personal data by competent public authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences [and for these purposes, the maintainance of public order,] or the execution of criminal penalties.

Notes:
Austria is in favor of extending the scope of the directive to the maintenance of the public order (of course, as far as they fall within the ambit of EU law, cf. Article 3 para 2).

Austrian proposal

“1. This Directive lays down the rules relating to the protection of individuals with regard to the processing of personal data by competent public authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. 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.”

Art. 1a

[not yet contained in the existing texts]

Austria requests the preservation of a provision in the vein of Art. 1 para. 5 of the Framework Decision 2008/977/JHA

Reasons:

The sensitive area of police and criminal law enforcement requires an adequate balance between the state's powers of data collection and use and the individual's need for protection of privacy.

This sensitive balance must be struck on the national level and must be adequate to the powers granted to the authorities. Not only do these powers and the constitutional limits to these powers vary to a great extent from Member State to Member State. The respective national legal culture and the sensibility of the public vis à vis data protection as a limit to police and law enforcement also greatly vary from Member State to Member State.

The logic underlying the Data Protection Rules of the Directive 95/46/EC is the logic of an internal market which aims at leveling down the differences of national Data protection rules with the goal of creating standard rules to enable private actors to do business moving from one Member State to another without having to abide by different data protection standards.

This logic cannot be transposed to the Sector of Police and Judicial Cooperation.

The inadequacy of the internal market logic for purposes of judicial and police work has already been recognized by the authors of the Framework Decision 2008/977/JHA. The new legal basis (Art 16 TFEU) does not change this fact.

Austrian proposal: Maintain Art. 1 para. 5 of the FD 2008/977/JHA:

"Art 1a

This Directive shall not preclude Member States from providing, for the protection of personal data collected or processed at national level, higher standards than those established in this Directive."

Art. 2 (3)

[COM proposal, modified by PRES]

"Art. 2

Scope

1. …

2. …

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, ~~in particular concerning national security~~;

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

Notes:

Under the Presidency-proposal the exception for activities which fall outside the scope of EU law has become even less precise than under the COM-proposal. The exception must be made more precise because the extent of EU law applicable to police cooperation and judicial cooperation in criminal matters as well as substantive criminal law and procedural law, is not clear in practice (it is even less clear with regard to activities in the domain of the public order!). To state an example: Using a wide approach, even purely internal police work or a purely internal criminal procedure where a person faces prison charges could potentially fall under the scope of EU law. The same would be true for measures of police authorities in the field of public order. In the absence of a clarification, the Court of Justice could be lead towards finding that any measures taken by the police authorities, even in the field of public order are encompassed by the Directive, even without any factors connecting the case to any area of Union Law. This would certainly not be the intent of the Member States.

The unclear and vague wording of the COM-proposal would allow an interpretation that extends the scope even to such cases. However, it is completely unclear whether such a wide scope was intended and may legitimately be regulated under Art. 16 TFEU. In everyday practice, the authorities (and the transposing legislators) shall not depend on such vague terms. The applicability of the Directive shall be triggered only in situations regulated by specific instruments adopted in the field of police and judicial cooperation purposes. Furthermore, the term “institutions, bodies, offices and agencies” shall be specified in order to clarify that Europol and Eurojust are already governed by specific data protection rules.

Austrian proposal

“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, 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**,

(b) processed by the Union institutions, bodies, offices and agencies, such as Europol or Eurojust.”

Art. 3 (1)

Austria welcomes the text proposed by the Presidency.

Art. 3 (5)

[COM proposal, modified by PRES]

“Art. 3
…
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;

Austrian proposal:

It should be made clear in a Recital under which circumstances files in paper form fall within the ambit of the Directive. (see for example recital 15 of Directive 95/46/EC).

Art. 3 (10)

[COM proposal, modified by PRES]

"Art. 3

…

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, resulting from an analysis of a biological sample from the individual in question ~~which are inherited or acquired during early prenatal development~~;"

Notes:

The Presidency modified the original definition proposed by the COM: According to the Presidency's version, the previous step of analysis of genetic data would be made a condition for data to be further considered as "genetic" data. This definition could be understood in such a way as to exclude the step of gathering and collecting of genetic data from the protection afforded by the Directive. Both the European Court of Human Rights and the Austrian Constitutional Court (as well as other Constitutional Courts) have stressed that genetic data is liable to specific rules of protection not only after the analysis has occurred, but from the beginning of its existence.

It is absolutely clear that the instruments of DNA-gathering and DNA-analysis are of crucial importance for police and law enforcement. The proposed definition does not mean that these tools shall be forbidden. Their purpose is simply to make sure that the treatment of genetic data shall always be based on the law and shall be subject to adequate guarantees.

Austrian proposal:

Delete the words: [~~resulting from an analysis of a biological sample from the individual in question~~]

"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, ~~resulting from an analysis of a biological sample from the individual in question which are inherited or acquired during early prenatal development~~"

(preferred) Alternative:

"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**"

Art. 3 (11) – biometric data

[COM proposal, modified by PRES]

"Art. 3

(11) 'biometric data' means any personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual, such as facial images, or dactyloscopic data;"

Notes:

The Same remarks as those made for Art 3 (10) apply: Data Protection does not start after data has been analyzed but begins from the moment on that personal data exists. The data carried by the human body is as such worthy of protection.

Austrian proposal

Delete the words “resulting from” and replace them by “liable to” or “in the context of”

“(11) 'biometric data' means any personal data ~~resulting from~~ **liable to / in the context of** specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual, such as facial images, or dactyloscopic data; ”

Art. 4 (1) a

[COM proposal, modified by PRES]

“Article 4
Principles relating to personal data processing

1. Member States shall provide that personal data must be:
(a) processed (…) lawfully;”

….

Notes:

Austria notes that the Presidency proposed to delete the principle of “fair” processing from the general principles of the Directive.

This principle is a well-established principle of European Data Protection Law (cf Art 5 a of the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data). Also, deletion would be inconsistent with the Regulation and with Art 8 of the Charter of Fundamental Rights.

Furthermore, the current proposal (Presidency version) lacks a provision in the sense of Art. 4 para 2 of the FD 2008/977/JHA. It is not sufficient that erasure/rectification/blocking takes place individually in case of a specific request of the individual (cf. Article 15 para. 1a of the Presidency’s version) but the erasure/rectification/blocking must be a self standing obligation of the controller to be fulfilled also in the absence of a request.

Austrian proposal

Austria pleads for a return to the text proposed by the Commission (especially with regard to the principle of fairness, see Art. 8 of the Charter of Fundamental Rights and many international data protection standards)

"Art. 4
Principles relating to personal data processing
1. Member States shall provide that personal data must be
a. processed fairly and lawfully;
….

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

In addition, Austria pleads for the re-introduction of provisions along the lines of Article 4 paras. 3 and 4 of FD 2008/977/JHA,

Art. 5 and 6

[COM proposal, modified by PRES]

"[The Presidency proposal deleted Articles 5 and 6]"

Notes:
In view of the deletion of Article 5 and 6 Austria stresses the importance of maintaining recital 23 and 24. Both the distinction between different categories (suspect / victim / witness / innocent bystanders / etc) as well as the distinction between different levels of quality of data (mere allegation / mere suspicion / doubtful allegation / partially confirmed allegation / legally proven allegation / etc) are important aspects that may play a crucial role in the interpretation of other rules of the Directive, such as for example the question whether the collection, in databases, of certain categories of data is "relevant" in the , sense of Art. 4 (1) c or "accurate" in the sense of Art. 4 (1) d or whether certain categories of data shall be made available only to certain specially authorised officers within an organization (see Article 27 – data security).

Austrian proposal

Maintain Recitals 23 and 24.

Perhaps these Recitals could, additionally, be completed by a statement of the reflections presented above (relevance of different categories for application of rules on accuracy, relevance and data security measures).

Art. 4 and 7

[COM proposal, modified by PRES]

"Article 7

Lawfulness of processing

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

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

(…)

I in order to protect the vital interests of the data subject or of another person; or

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

2. Member States shall provide that the controller may further process personal data for historical, statistical or scientific purposes, subject to appropriate safeguards for the rights and freedoms of data subjects."

Notes:

Neither the COM-proposal nor the PRES proposal contain any rules that regulate the question of admissibility (proportionality and legality) and the conditions for

a. access, by law enforcement authorities, to personal data processed by other controllers, originally for purposes others than those mentioned in Article 1.

b) further use or further transfer, by law enforcement authorities, of personal data to

i. further processing for another purpose set out in Article 1 which is not compatible with the initial purpose: for example: transmission of data initially collected for a criminal procedure for a further secondary use in databases for (police) purposes of prevention of crime or prevention of danger.

*ii. other sectors pursuing activities other than those mentioned in Art 1 (for example to private persons, or for use by other public institutions such as **family welfare**, financial supervisory authorities, **or use for statistical or historical purposes**).*

The lack of rules addressing these topics leads to the following question:

Since the wording of Article 7 indicates that this Article shall set up an exhaustive list of permissions ("is lawful only if and to the extent that processing is necessary: a) for .., b) in order…, c) …").

Is the Directive to be interpreted as restricting the cases of processing mentioned above? Or is it to be interpreted as allowing them without regulating any adequate conditions (regarding legality and proportionality)?

Does the omission of rules concerning the topics mentioned above mean that Member States will remain competent to regulate these limits? This would result in a lack of common european standards regarding these question.

Austrian proposal

Austria proposes to adopt rules along the lines of the amendments proposed by the EP-rapporteur in the LIBE committee, Dimitrios Droutsas, who proposed an new Article 4a and an Article 7a of the Droutsas-report[1].

[1] http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/923/923072/923072en.pdf

Art. 7a

[COM proposal, modified by PRES]

"Article 7a
Specific processing conditions
1. Member States shall provide that where Union law or the national law applicable to the transmitting competent public authority provides for specific conditions applicable in specific circumstances to the processing of personal data, the transmitting public authority shall inform the recipient to whom the data are transmitted about such conditions and the requirement to respect them.

2. Member States shall provide that the transmitting public authority does not apply conditions 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 the transmitting public authority."

Notes:
The introduction of this Article, proposed by the Presidency, takes account of the opinion (expressed by many Member States) that the rules elaborated in the Framework decision 2008/977/JHA are already well suited for the area that the Directive aims to regulate anew.

Austria welcomes Article 7a as proposed by the Presidency.

Art. 8

Austria welcomes this version of the Article.

Art. 17 and 44 (2)

Austria welcomes the clarification brought about by the Presidency's proposal.

Art. 10, 11, 11a and 11b

Austria welcomes the fact that the general structure of these Articles remains unchanged.

Many Delegations expressed the view that "the right to access and information should be the exception and not the rule". However, Austria supports the view that, although there will be many restrictions, general principles of a right to information and access have to be set out. The right to information and to access has to be the rule, whereas any restriction of these rights may be adopted in national (or Union) law, as an exception to the rule, where such an exception is deemed necessary and proportional by the competent legislator.

Any other construction of the relationship between "rule" and "exception" would be contrary to the principles emanating from Articles 8 and 52 (1) of the Charter of Fundamental Rights.

It goes without saying that, in practice, especially in the field of criminal law and the prevention of danger, these general principles will be subject to wide and various restrictions in many instances: Article 11b allows for the adoption of those exceptions.

Accordingly, Austria **welcomes** the preservation of the general rules of Articels 10-11a as well as the framework for derogations established by Article 11b.

Art. 13
[COM proposal, modified by PRES]

"Article 13 Limitations to the right of access
….
3. In cases referred to in paragraphs 1 and 2, Member States shall provide that the controller informs the data subject (…) of any refusal or restriction of access, of the reasons for the refusal and of the possibilities of lodging a complaint to the supervisory authority [and seeking a judicial remedy]. This shall not apply (…) where the provision of such information would undermine a purpose under paragraph 1.

Notes:

Exposing the reasons for the refusal may prove to be unfeasible. In Austrian Law, in case the police or law enforcement authorities wish to deny access for reasons of secrecy in the public interest, the response to a request for access consists in a neutral, "standard" answer. The text of this standard answer is the as in cases, where, in fact, no data exists. This way, the data subject receives a response in order to be able to initiate a complaint. The supervisory authority will then have to check the lawfulness of the neutral answer by conducting an examination as to whether the controller had legitimate reasons for having recourse to this form of reply. The relevant provision of Austrian Law states:

> "In all cases where no information is given even when in fact no data on the person requesting information is used instead of giving a reason in substance, an indication shall be given that no data are being used which are subject to the right to information. The legality of such course of action is subject to review by the Data Protection Commission [Datenschutzkommission] pursuant to § 30 para. 3 and the special complaint proceeding before the Data Protection Commission pursuant to § 31 para. 4. "

The introduction of such a modality will eliminate the need for the last sentence of the proposed Article 13 para 3 ("This shall not apply (…) where the provision of such information would undermine a purpose under paragraph 1.)

The Article does not address the case where data is being processed by a judicial authority. In this case, the Member States shall be able to provide for a judicial remedy instead of a complaint to the supervisory authority (see Article 44 para. 2) This aspect needs to be reflected in the text of Article 13.

Austrian proposal

"3. In cases referred to in paragraphs 1 and 2,or when, in fact, no data on the person requesting the information is processed, Member States shall provide a neutral reply, instead of giving a reason in substance, stating that "no data are being used which are subject to the right to information". In addition, an information on the possibilities of lodging a complaint to the supervisory authority **or, where applicable the seeking of a** judicial remedy shall be given."

Art. 15

[COM proposal, modified by PRES]

"Article 15
Right to rectification, erasure and restriction of processing
1. Having regard to the nature and purpose of the processing concerned, Member States shall provide for the right of the data subject to obtain from the controller the rectification of personal data relating to him or her which are inaccurate and (…) the right to obtain completion of incomplete personal data, including by means of providing a supplementary statement.
2. …"

Austria proposes to delete the last part of the sentence: "~~including means of providing a supplementary statement~~"

ROMANIA

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 public authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences [and for these purposes, the maintainance of public order,] or the execution of criminal penalties.*

Comments:

RO would like to draw attention that the unclear delimitation between the Directive and Regulation will have major negative impact on the law enforcement authorities. Practical activities of the Police include the maintaining and ensuring the public order, during which the processing of personal data is a very important part. Leaving these activities under the regulation would practically block the possibility to legally process personal data of persons when fulfiling duties by the police officers. It is compulsory that the maintaining and ensuring the public order be regulated by the directive.

RO presented the issue in document no. ST8208/13. We maintain our text proposal:

"*1. This Directive lays down the rules relating to the protection of individuals with regard to the processing of personal data by competent public authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties* **and for the purposes of maintaining and ensuring the public order.**"

Also as a general remark we consider that the widespread wording *"vital interest"* in the text of the directive should be properly be defined for legal clarity of the text.

Article 3

Comments

At paragraph (13) of the draft text, we propose to introduce a definition of the special categories of personal data to which art. 8 paragraph (1) makes reference; we propose to also include biometric data within the list mentioned in art. 8 paragraph (1);

Article 8

Processing of special categories of personal data

2. Paragraph 1 shall not apply where:

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

Comments

RO seeks for clarification regarding the wording "appropriate safeguards" stipulated in this paragraph, in order not to leave room for interpretation but to ensure legal clarity of the text.

At paragraph 1 we propose to add biometric data within the category of data with a special character, in view of the risks posed to individuals' rights by their processing;

Article 10

Communication and modalities for exercising the rights of the data subject

4. Member States shall provide that the controller informs the data subject about the follow-up given to his or her request without undue delay.

Comments

RO seeks for clarification regarding the wording "without undue delay". We would like to know the meaning of the condition "without undue delay" in order to appreciate the time frame in which the obligation must be fulfilled by the controller.

Article 11

Comments

We propose including art. 11a into 11 with the title "The right to be informed", taking into consideration the title of Chapter III "Rights of Data Subjects" and the fact that art. 11 b is titled "Restrictions of the right to be informed".

Article 12

1a. Member States shall provide that where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 35 relating to the transfer.

Comments

We believe that these provisions should be included within art. 11 on the right to be informed.

Article 18

Obligations of the controller

1. Member States shall provide that the controller implements appropriate measures and be able to demonstrate that the processing of personal data is performed in compliance with the provisions adopted pursuant to this Directive.

1a. Where proportionate in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

Comments

We would like to know which are the criteria which ensure the proportionality of the processing activities when the controller decides to draft own procedures. We are of the opinion that the wording*: "proportionate in relation to the processing activities "* is too vague and does not leave room to ensure the conformity with the stipulations of the directive.

We request further clarification of the term "policies", in view of the fact art. 19 also establishes an obligation of the data controller to implement adequate technical and organisational measures, procedures and mechanisms, which may lead to certain confusion as regards the data controller's administrative burdens

Article 23

Records of categories of personal data processing activities

1. Member States shall provide that each controller and processor shall maintain a record of all processing systems (…) under their responsibility.

2. (…)

3. The controller and the processor shall make such records available, on request, to the supervisory authority.

Comments

RO seeks for clarification regarding what data the record defined in this article may contain and who will chck whether this record is properly documented.

Article 24

Logging

1. *Member States shall ensure that logs are kept of at least the following processing operations: collection, alteration, consultation, disclosure, combination or erasure in automated processing systems. The logs of consultation and disclosure shall show (…) the purpose, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data.*

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

Explanations

RO appreciates that by establishing the processing operations and the recording features, the tool proposes standards that can be assessed as minimal, in the "cloud" processing age .

RO proposes that the expression *"at least"* be introduced in paragraph 1 as follows:

"(…)*The logs of consultation and disclosure shall show* ***<u>at least</u>*** *the purpose, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data.*"

Member states should be given the possibility to provide for extra options which will be shown in the logs in order to thoroughly document the processing operation.

We request further clarifications as regards the processing operations listed, especially the "consultation" and "disclosure", more exactly if these operations include the possibility that the date are also consulted by other police authorities (of antother state/"transfer" of data).

Article 32

Tasks of the data protection officer

…….

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

Proposal

We suggest to complete art. 32 letter b) as following:

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

FINLAND

Article 1.1

Article 1

Subject matter and objectives

OPTION 1:

This Directive lays down the rules relating to the protection of individuals with regard to the processing of personal data by competent **public** authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences **and for these purposes, the maintainance of public order and security** or the execution of criminal penalties

OPTION 2:

This Directive lays down the rules relating to the protection of individuals with regard to the processing of personal data by **competent authorities that exercise public powers** for the purposes of the prevention, investigation, detection or prosecution of criminal offences **and for these purposes the maintainance of public order and security,** or the execution of criminal penalties.

Finland supports the views expressed by RO and supported by various other delegations, to add "**public order and security**" to the subject matter of the Directive. Adding that element to the scope would facilitate the implementation of the Regulation and Directive, particularly in those member states where both personal data relating to crime prevention and criminal investigations and personal data relating to the maintenance of public order and security are entered in the same police information system. We feel that the expression "maintenance of public order and security" would cover the range of police duties better than "public order" alone.

Finland could support the expression proposed by EE, ""…**by competent authorities that exercise public powers for the purposes of** …", but would need to enter a scrutiny reservation to the proposed expression "prevention of threats and risks" until a further analysis has been done. In any case, a common understanding of the meaning of maintenance of public order and security would be welcome, preferably by adding a more detailed reference to police duties in the recitals. However, it must be remembered that no common definition seems to exist at this point and some caution is needed as to the creation of any new concepts in a data protection instrument.

As for addition of private security companies to the scope, we would need to enter a scrutiny reservation until a further analysis of that proposal has been done.

The exact coverage of the directive in respect of “prosecution” and courts should be clarified. Courts give sentences and determine punishments. The execution/enforcement of criminal penalties is the task of executive authorities, not that of courts. Therefore, the wording of Article 1 paragraph 1 does not seem to cover courts.

Article 2

If option 2 in article 1 paragraph 1 is chosen, article 2 paragraph 1 should be amended accordingly and the word public deleted:

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

We suggest a new paragraph 4 :

> **This Directive does not apply to personal data contained in a judicial decision or to records processed in courts during criminal proceedings.**
>
> Justification: The Directive should not affect national rules on judicial proceedings.

Article 3

As regards point (4), Finland would welcome an analysis by the Commission of the difference between blocking and restriction, but we don't see a problem with the use of "restriction". The expression chosen has to be in line with Article 15.

As regards point (14), in our opinion the definition of “competent public authority” does not cover courts (see Article 1.1. above).

Article 12

A new paragraph (1a) has been added. That paragraph should perhaps be linked to Article 13 to ensure correct interpretation, in the same way as has been done in paragraph 1. The expression used could be "**subject to/ without prejudice to Article 13".**

1a. **Subject to/Without prejudice to Article 13** Member States shall provide that where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 35 relating to the transfer.

Article 13

In paragraph 3, the words "**or restriction**" should be added on the third line after the word "refusal".

3. In cases referred to in paragraphs 1 and 2, Member States shall provide that the controller informs the data subject (…) of any refusal or restriction of access, of the reasons for the refusal **or restriction** and of the possibilities of lodging a complaint to the supervisory authority [and seeking a judicial remedy]. This shall not apply (…) where the provision of such information would undermine a purpose under paragraph 1.

Article 17

Article 17 is very ambiguous and should either be redrafted of deleted. We have understood the COM explanations so that the exercise of the rights in Articles 11, 11a, 12 and 15 must be provided for either in accordance with national rules on judicial proceedings or in other domestic legislation, e.g. in data protection legislation. However, we are not sure if we have interpreted the COM explanations correctly. It is impossible to comment on the article since we don´t know what its exact meaning is. At least the last two **words "and proceedings" should be deleted,** also from the title of the article (see our comments on article 2).

SWITZERLAND

(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 public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences [and for these purposes, the maintenance of public order,] or the execution of criminal penalties. At the same time the legitimate activities of the competent public authorities should not be jeopardised in any way.

Footnote 6: Addition:

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."

(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 public authority based on Union law or Member State law or in order to protect the vital interests of the data subject or of another person, or for the prevention of an immediate and serious threat to public security. Furthermore, a processing of personal data should be lawful if the data subject has given his or her consent to the processing of his or her personal data for one or more specific purposes. The data subject's consent means any freely-given specific, informed and explicit indication of his or her wishes by which the data subject signifies his agreement to personal data relating to him being processed.

(25a) Member States should provide that where Union law or the national law applicable to the transmitting competent public authority provides for specific conditions applicable in specific circumstances to the processing of personal data, the transmitting public authority should inform the recipient to whom data are transmitted about such conditions and the requirement to respect them. These obligations apply also to transfers to recipients in third countries or international organisations. Member States should provide that the transmitting public authority does not apply conditions pursuant the first sentence 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.

(44) (…) A person with expert knowledge of data protection law and practices may assist the controller or processor to monitor internal compliance with the provisions adopted pursuant to this Directive. A data protection officer may be appointed jointly by several public authorities or bodies, taking into account of their organisational structure and size (…). Such data protection officers must be in a position to perform their duties and tasks in an independent (…) manner.

(49) Transfers not based on such an adequacy decision should only be allowed where appropriate safeguards have been adduced in a legally binding instrument, which ensure the protection of the personal data or where the controller (…) has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and, based on this assessment, considers that appropriate safeguards with respect to the protection of personal data exist. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress.

By way of derogation, in specific situations where no adequacy decision or appropriate safeguards exist, a transfer could take place if necessary in order to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides, or where it is essential for the prevention of an immediate and serious threat to the public security of a Member State or a third country, or in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, or in individual cases for the establishment, exercise or defence of legal claims. Furthermore, a transfer of personal data should be lawful if the data subject has given his or her consent to the transfer of his or her personal data for one or more specific purposes.

(55) While this Directive applies also to the activities of national courts and other judicial authorities, the competence of the supervisory authorities should not cover the processing of personal data when they are acting in their judicial capacity, so that it doesn't interfere with national rules on judicial proceedings. However, this exemption should be limited to (…) judicial activities in court cases and not apply to other activities where judges might be involved in accordance with national law.

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

Article 1

Subject matter and objectives

1. This Directive lays down the rules relating to the protection of individuals with regard to the processing of personal data by competent public authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences [and for these purposes, the maintainance of public order,] or the execution of criminal penalties.

Footnote 15 can be deleted

Article 3

Definitions

For the purposes of this Directive:

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

(8bis) "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.

(11)

Footnote 49:

CH suggested to add a definition of consent: " '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 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)

Article 4

Principles relating to personal data processing

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

(d) accurate and, where possible and necessary, completed or kept up to date; (…)

€ erased or made anonymous when they are no longer required for the purposes for which they were lawfully collected or are lawfully further processed.;

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

(…)

2. Further processing for another purpose shall be permitted in so far as:

(a) it is not incompatible with the purposes for which the data were collected;

(b) the competent authorities are authorised to process such data for such other purpose in accordance with the applicable legal provisions; and

€ processing is necessary and proportionate to that other purpose.

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

Article 7a

Specific processing conditions

2. Member States shall provide that the transmitting public authority does not apply conditions 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 .

Article 10

Communication and modalities for exercising the rights of the data subject

3.

5. Member States shall provide that the information provided under Articles 11 and 11a and any communication under Articles 12, 15 and 29 shall be provided (…) free of charge. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character (…), the controller may refuse to act on the request or may charge a fee. In that case, the controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request (…).

5a. Where the data subject intends to exercise his or her rights according to Articles 12 and 15, he or she has to prove his or her identity to the controller. *Article 11*

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

1. Subject to Article 11b, Member States shall provide that where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with *at least* the following information:

(a) the identity and the contact details of the controller; the controller may also include the contact details of the data protection officer if any;

10. (…)

11. (…)

12. (…)

13. (…)

14. Paragraph 1 shall not apply where and insofar as the data subject already has the information.

Article 11a

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

1. *Subject to Article 11b, Member States shall provide that where personal data have not been obtained from the data subject, the controller shall provide the data subject with at least the following information:*

(a) the identity and the contact details of the controller and, the controller may also include the contact details of the data protection officer if any;

3. Members States may provide that paragraphs 1 and 2 shall not apply where and insofar as:

(a) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject, which provides appropriate measures to protect the data subjects legitimate interests,

(b) the provision of such information proves impossible or would involve a disproportionate effort.

Article 11b

Limitations to the rights of information

3. When personal data have been transmitted or made available between Member States, each Member State may, in accordance with the provisions of its national law referred to in paragraph 1, ask that the other Member State does not inform the data subject. In such case the latter Member State shall not inform the data subject without the prior consent of the other Member State.

Article 13

Limitations to the right of access

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

Article 15

Right to rectification, erasure and blocking of processing

1a. *Member States shall provide for the obligation of the controller to erase personal data of the data subject of its own motion or upon request and without undue delay where the processing does not comply with the provisions adopted pursuant to Articles 4 (a) to €, 7 and 8 of this Directive, or where the data have to be erased for compliance with a legal obligation to which the controller is subject.*

1b. Member States shall provide for the right of the data subject to obtain from the controller the blocking of the processing of personal data where their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data.

1bb. Member States may/shall provide that in case where the accuracy of an item of personal data is contested by the data subject and its accuracy or inaccuracy cannot be ascertained, referencing of that item of data may take place. Personal data shall be blocked instead of erased if they are required by the data subject for the establishment, exercise or defense or legal claims.

2. Member States shall provide that the controller informs the data subject (…) of any refusal of rectification, erasure or restriction of the processing, the reasons for the refusal and the possibilities of lodging a complaint to the supervisory authority [and seeking a judicial remedy].

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

Article 17

Rights of the data subject in criminal investigations and proceedings

Member States may provide that the exercise of the rights (…) referred to in Articles 11, 11a, 12 and 15 is carried out in accordance with national rules on judicial proceedings where the personal data are contained in a judicial decision or record processed in the course of criminal investigations and proceedings.

Footnote 107: Deletion of CH

Article 21

Processor

2. Member States shall provide that the carrying out of processing by a processor shall be governed by a legal or contractual act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller (…).

Article 23

Records of processing systems

Article 24

Logging

1. Member States shall ensure that logs are kept of at least the following processing operations: collection, alteration, consultation, disclosure, combination or erasure in automated processing systems. The logs of consultation and disclosure shall show (…) date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data.

Footnote 119:

ES and CH wanted the reference to purpose to be deleted. In contrast AT thought that it was important to keep the reference to purpose.

Footnote 120:

EE considered that the paragraph was too restrictive.

Article 30

Designation of the data protection officer

5. Union law or Member State law may provide that the controller or the processor designates a data protection officer and, in such a case, determine the requirements to be fulfilled by the data protection officer.

6.

7. A single data protection officer may be designated for several competent public authorities, taking account of their organisational structure (…) and size.

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

5.

Article 32

Tasks of the data protection officer

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

(c) to inform and advise the controller or the processor of their obligations in accordance with the provisions adopted pursuant to this Directive (…);

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

Footnote 141:

CH refers to the letter of the Mission of Switzerland dated 28.08.2013 to the Legal Service of the General Secretariat of the Council of the European Union. Even if the General Data Protection Regulation will not be a Schengen development, Switzerland is of the opinion that it will continue to be considered as an integral Schengen/Dublin country regarding the exchange of data between EU Member States and Switzerland in the area of Schengen and Dublin cooperation, and not as a third country. DE had doubts if Article 34 corresponded with reality. DE further did not support the Cion's role regarding adequacy decisions. UK supported DE that it was better that the adequacy decision were taken by the MS rather than Cion. DE said that Article 60 and Article 34 were contradictory.

Footnote 169:

DE scrutiny reservation. EE and CH opposed this Article because their respective national law did not allow for penalties on public bodies. EE and CH reservations. Cion stated that Article 55 existed in the Regulation as well and was a standard provision.