COUNCIL OF THE EUROPEAN UNION

Brussels, 28 November 2012

16497/12

Interinstitutional File: 2012/0010 (COD)

LIMITE

DATAPROTECT 131
JAI 817
DAPIX 144
FREMP 140
COMIX 651
CODEC 2738

NOTE

from:	General Secretariat
to:	Working Group on Information Exchange and Data Protection (DAPIX)
No. Cion prop.:	5833/12 DATAPROTECT 6 JAI 41 DAPIX 9 FREMP 8 COMIX 59 CODEC 217 + ADD 1 + ADD 2
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

Further to the invitation by the Presidency (CM 4718/12) delegations have sent in written comments on Articles 1-8 of the 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.

The comments received at 27 November 2012 are set out hereafter.

TABLE OF CONTENT

BELGIUM

Proposition de directive "Police and Criminal Justice Data Protection Directive"	Belgian proposition
Subject matter and objectives	
Art.1.1 This Directive lays down the rules relating to the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.	BE souhaite émettre une réserve de fond sur l'art. 1.1 : -elle souhaite que les traitements réalisés à des fins de police administrative soient soumis à un régime juridique identique que les traitements de données de police judiciaire ; -elle comprend néanmoins que les restrictions des droits des personnes concernées soient proportionnées aux nécessités des traitements de police administrative. ~~Afin d~~e ~~de clarté~~ BE ~~elle~~ souhaite rajouter un considérant disant : "Le caractère pénal des infractions ou des peines au sens de l'article 1 n'est pas déterminé par la législation nationale des Etats membres mais par la Cour européenne des droits de l'homme qui précise que le caractère pénal dépend des critères suivants : (1) la classification interne ; (2) la nature de l'infraction ; (3) la sévérité de la peine potentielle que la personne concernée risque d'encourir.

Principes relatifs au traitement des données à caractère personnel	
BE : Art. 4 Ajout d'une 2ième alinéa: 4.2. Further processing for another purpose shall be permitted in so far as:	Inspiré de l'art. 3, 2 de la Décision-cadre 2008/977
(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	
(c) processing is necessary and proportionate to that other purpose.	
The competent authorities may also further process the personal data transmitted by the competent authorities of other Member States for historical, statistical or scientific purposes, provided that Member States provide appropriate safeguards, such as making the data anonymous.	
Scope	
Distinction between different categories of data subjects	
Art.5 Member States shall provide that, as far as possible, the controller makes a clear distinction between personal data of different categories of data subjects, such as:	

(a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;	
(b) persons convicted of a criminal offence;	
(c) victims of a criminal offence, or persons with regard to whom certain facts give reasons for believing that he or she could be the victim of a criminal offence;	
(d) third parties to the criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, or a person who can provide information on criminal offences, or a contact or associate to one of the persons mentioned in (a) and (b); and	
(e) Persons who do not fall within any of the categories referred to above.	~~Ajout d'un article 5.2 inspiré de l'arrêt CEDH Marper :~~ ~~« Les données des personnes innocentées font l'objet de garanties spécifiques »~~ ~~Ajout d'un art. 5.3, inspiré de l'art. 5 de la décision cadre 2008/977 :~~ ~~« Des délais appropriés sont prévus pour effacer les données à caractère personnel ou vérifier régulièrement s'il est nécessaire de conserver les données. Des règles procédurales permettent d'assurer le respect de ces délais »~~

BE/ Ajout d'un article 5.2 inspiré de l'arrêt CEDH Marper : « Les données des personnes acquittés par une décision judiciaire font l'objet de garanties spécifiques »	
BE/ Ajout d'un artt. 5.3 inspiré de l'art. 5 de la décision-cadre 2008/977 : « Des délais appropriés sont prévus pour effacer les données à caractère personnel ou vérifier régulièrement s'il est nécessaire de conserver les données. Des règles procédurales permettent d'assurer le respect de ces délais »	
Lawfulness of processing	
Art.7 Member States shall provide that the processing of personal data is lawful only if and to the extent that processing is necessary:	
(a) for the performance of a task carried out by a competent authority, based on law for the purposes set out in Article 1(1); or	

(b) for compliance with a legal obligation to which the controller is subject; or	Afin de clarté elle souhaite rajouter un considérant disant : L'obligation légale prévue à l'article 7 (b) comprend également le maintien de l'ordre et de la sécurité publics au sens de l'article 17 de la décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière, avec cette précision que, vu que cette directive sera aussi d'application aux traitements effectués par les autorités compétentes au niveau strictement national, tout traitement en vue de maintenir l'ordre et la sécurité publics au niveau strictement national est également visé. L'article 59 exclut la décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière. Cependant, les missions de maintien d'ordre public et de sécurité contraint les services de police de traiter des données à des fins de maintien d'ordre public et de sécurité. Le traitement de ces données à ces fins constitue donc une obligation légale.
(c) 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.	

GREECE

A)Article 1 -Subject matter and objectives

In para 1, we would like to have further clarification on the term "competent authorities", in order to ensure that an investigator and prosecutor is being included since the scope of the proposed Directive is also the processing of personal data for the purpose of prosecution of crimes. This will further clarify the meaning of Article 17 regarding the criminal procedure and the phase of prosecution and in which phase of prosecution the proposed Directive also applies.

Also, we would like to know whether for the purpose of the execution of criminal penalties, the processing of the data in criminal records is included?

B) Article 2- we have no further comments

C) Article 3-Definitions

We would like to mention that the definitions must be in alignment with the corresponding Art. 4 of the proposed General Regulation.

D) Article 4-Principles relating to personal data processing

We would like to make the following suggestions:

The wording of Article 4 should be in alignment with the wording of the proposed General Regulation (Article 5). The wording of Article should include important elements regarding the retention of personal data (including retention periods), transparency towards individuals, keeping personal data up to date, and ensuring it is adequate, relevant and not excessive. The reference to accountability deemed to be also necessary.

-Point (d): the phrase "**where necessary**" must be deleted, because it is important to have always updated data. This is also important for the different categories of data subjects because the status of a person may change during the investigation proceedings.

E)Article 5-Distinction between different categories of data subjects

The inclusion of a provision in the proposal for this Directive of different categories of data subjects (criminals, suspects, victims, witnesses, etc) is necessary for the protection of the personal data of individuals and for the ability of the competent authorities to make full use of this data. The accuracy of this distinction is closely related to the respect of the principles included in Art. 4 of the Directive and also to the principle of the presumption of innocence for the data subjects.

Considering that Art. 5 should keep the proper balance between the public interest in law enforcement and citizens' fundamental rights, we would like to make the following suggestions:

-In the introductory proposition the phrase "**as far as possible**" comes to contradiction to the clear distinction that the controller makes and diminishes the notion of the whole article. So, further clarification should be made on this phrase or it should be deleted.

-Point (a): Further clarification need the phrases:

"…serious grounds.." : It is vague.

"..**are about to commit..**": this aspect of prevention needs further elaboration because it is not possible to prove such a presumption. So it is needed a wording which will limit the vagueness of the phrase, some suggestions are: to add the words "*or there are serious grounds based on real facts that* are about to commit.."

and "**criminal offence**": the term needs further clarification

-**Point (b**): it should be further clarification in order to be in line with Art. 9 para 2 point (j) of the proposal for a General Regulation on Data Protection about "security measures".

It should be made further distinction between the cases which the processing is made for the purposes of prevention/ investigation/ detection/prosecution of criminal offences from the cases of the processing made for the purposes of the execution of criminal penalties. Particularly, we suggest distinction for the cases of processing data included in criminal records, because the criminal records, among other data, include irrevocable court decisions for some criminal offences and for instance, the security measures which may included as data they are not sanctions.

-**Point (c):** the phrase "…to whom certain facts give reasons **for believing** that he or she could be the victim…" The phrase "for believing" needs further clarification regarding the facts that establish a belief.

- **Point (d):** We would like to mention that the category of "associate" is covered by point (a) and (b) of the Article. So the distinctions in this point (d) must be further clarified. We also suggest further clarification about the meaning of "….a **contact** to one of the persons…"

-**Point (e):** It is not clear whether the provision refers to the non-suspected persons for whom specific safeguards should be included for a proportionate use of data.

F) Article 6-Different degrees of accuracy and reliability of personal data

The phrase **"as far as possible"** in both 1 & 2 paragraphs is suggested to be deleted because it limits the distinction.

For para 2, we note that there is difficulty in distinguishing between data based on facts and data based on personal assessments.

G) Article 7-Lawfulness of processing

-Point (c): The phrase "**vital interests**" must be further clarified.

-We would like to suggest an addition of further processing for historical, statistical and scientific purposes, under specific safeguards as provided in the same article of Framework Decision 2008/977/JAI.

E) Article 8-Processing of special categories of personal data

-Para 2, point (a**):** The phrase **"<u>appropriate safeguards</u>"** needs further clarification

-Para 2, point (b): The phrase "**<u>vital interests</u>**" needs further clarification.

-Para 2, point (c): The word **"<u>manifestly</u>**" needs explanation.

For all the above derogations of the prohibition of the processing of personal data we suggest more safeguards to be included.

We suggest the inclusion of special provisions for children regarding the processing of data that concern them and their retention period.

SPAIN

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 authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties **within the framework of the police and judicial cooperation provided for by Title V of the Treaty on the Functioning of the European Union.**

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

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

(b) ensure that the exchange of personal data by competent authorities within the Union is neither restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.

3. This Directive shall not preclude Member States from providing, for the protection of personal data collected or processed at national level for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, higher safeguards than thos established in this Directive.

Article *2*

Scope

1. This Directive applies to the processing of personal data by competent 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, in particular concerning national security, **the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security;**

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

Article 3

Definitions

For the purposes of this Directive:

(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifiers or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

(2) 'persona¬ data' means any information relating to a data subject;

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

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

(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, **natural or legal person,** which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; ~~where the purposes, conditions 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;~~ **It is not clear so far that the formule of the draft Regulation can be automatically used here; we suggest the deletion**

(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 to which the personal data are disclosed;

(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;)) ~~–~~ **we have misgivings towards the linguistic accuracy between the term "breach" and the spanish one "violación". In general terms, since DAPIX has dealt very slightly with this article , we suggest we'd wait further to consider the consequences of including such a definition**

(10) 'genetic data' means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development;

(11) 'biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data;

(12) 'data concerning health' means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;

(13) 'child' means any person below the age of 18 years**; the Spanish version should read "menor" (no "niño").**

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

(15) 'supervisory authority' means a 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

Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

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

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

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

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

(f) processed under the responsibility and liability of the controller, who shall ensure compliance with the provisions adopted pursuant to this Directive.

Article 5

Distinction between different categories of data subjects

At the light of the debate held in DAPIX (26.09.12) we are of the view that this article should be deleted. If the text were to be kept, we suggest the insertion of the following sentence in par.1:

1. Member States shall provide that, as far as possible, **and to the extent that it is relevant for the implementation of the tasks legally conferred to a competent authority**, the controllermakes a clear distinction between personal data of different categories of data subjects such as:

(a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;

(b) persons convicted of a criminal offence;

(c) victims of a criminal offence, or persons with regard to whom certain facts give reasons for believing that he or she could be the victim of a criminal offence;

(d) third parties to the criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, or a person who can provide information on criminal offences, or a contact or associate to one of the persons mentioned in (a) and (b);

(e) persons involved in police activities, investigations and operations aimed to prevent crime and

(f) persons who do not fall within any of the categories referred to above.

Article 6

Different degrees of accuracy and reliability of personal data

1. Member States shall ensure that, as far as possible, the different categories of personal data undergoing processing are distinguished in accordance with their degree of accuracy and reliability.

2. Member States shall ensure that, as far as possible, personal data based on facts are distinguished from personal data based on personal assessments. By definition, personal data, in the sense given to the term by this draft, cannot be based on personal assessments.

Article 7

Lawfulness of processing

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

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

(b) for compliance with a legal obligation to which the controller is subject; or

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

(d) for the prevention of a ~~immediate~~ **direct** and serious threat to public security; or

(e) to protect other fundamental rights of the data subject or another person that deserve a higher degree of protection.

Article 8

Processing of special categories of personal data

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

2. Paragraph 1 shall not apply where:

(a) the processing is authorised by a law providing appropriate safeguards; or

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

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

(d) the data subject has given his consent.

FRANCE

A titre de remarque générale, à chaque mention de l'obligation pour les Etats membres d'adopter « **une** loi », les autorités françaises demandent la modification de la rédaction et le remplacement de ces termes par « **la** loi », vocable déconnecté d'un critère organique.

Article 1 - Objet et objectifs

Les autorités françaises s'interrogent toujours sur la délimitation précise des champs d'application de la proposition de règlement et de la proposition de directive.

En effet, avec la proposition de règlement, les dispositions seront directement applicables et remplaceront les dispositions législatives des Etats membres, tandis que les dispositions de la proposition de directive devront être transposées dans le droit national des Etats membres. Il est donc primordial que la délimitation des champs d'application soit clarifiée, puisque des règles différentes devront être mises en œuvre en fonction de l'instrument européen qui régira le traitement de données concerné.

En particulier concernant le sens des termes « *autorités compétentes* » retenus au paragraphe 1 de l'article 1er, les autorités françaises souhaitent que certaines activités de police administrative spéciale visant la prévention d'une atteinte ou d'un trouble à la sécurité publique soient couvertes par la proposition de directive, et non par la proposition de règlement.

Ainsi, par exemple, en France, le Fichier National des Interdits de Stade (FNIS), le Fichier des Personnes Recherchées (FPR), le Fichier National des personnes Interdites d'Acquisition et de Détention d'Armes (FINIADA) ou encore l'application de gestion du répertoire informatisé des propriétaires et possesseurs d'armes (AGRIPPA) doivent relever de la proposition de directive.

Enfin, toujours au paragraphe 1, les autorités françaises demandent que la phrase soit modifiée pour que la liste des finalités soit alternative et non cumulative, en remplaçant les « et » par des « ou » :
« *aux fins de la prévention ~~et~~* **ou** *de la détection des infractions pénales, d'enquêtes ~~et~~* **ou** *de poursuites en la matière, ou de l'exécution de sanctions pénales* ».

Afin d'intégrer ces remarques, les autorités françaises proposent la rédaction alternative suivante :

« ***Article premier***

Objet et objectifs

1. La présente directive établit les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes au sein des Etats membres en matière :
- de prévention, de recherche, de constatation ou de la poursuite des infractions pénales ;
- d'exécution de sanctions pénales ;
- de maintien ou de rétablissement de la sécurité publique.

2. Conformément à la présente directive, les États membres:
a) protègent les libertés et droits fondamentaux des personnes physiques, et notamment leur droit à la protection des données à caractère personnel; et
b) veillent à ce que l'échange de données à caractère personnel par les autorités compétentes au sein de l'Union ne soit ni limité ni interdit pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. »

Article 2 : Champ d'application

Les autorités françaises soulignent que les domaines exclus du champ d'application de la directive au paragraphe 3 de l'article 2 ne sont pas assez clairement identifiés avec la rédaction actuelle. Elles demandent donc à ce qu'elle soit modifiée de la manière suivante, pour intégrer clairement l'exclusion des activités de sécurité nationale et de renseignement qui figure à l'article 1er, paragraphe 4 de la décision-cadre 2008/977, et l'exclusion de la PESC :

« *La présente directive ne s'applique pas au traitement de données à caractère personnel effectué :*

a) dans le cadre des activités qui concernent la sécurité nationale et les activités de renseignement spécifiques dans le domaine de la sécurité nationale ;

a') par les Etats membres dans l'exercice d'activités qui relèvent du champ d'application du chapitre 2 du traité sur l'Union européenne

b) par les institutions, organes et organismes de l'Union. »

Article 3 : Définitions

Sur les définitions de « *personne concernée* » et de « *données à caractère personnelles* », les autorités françaises formulent les mêmes remarques que celles qu'elle a déjà exprimées au sujet de la proposition de règlement :

De manière générale, les autorités françaises considèrent que les définitions du point (1) (« personne concernée ») et du point (2) (« données à caractère personnel ») sont inadaptées, dans la mesure où c'est la donnée qui doit être « identifiante ». Les autorités françaises demandent donc que la **présentation retenue par la directive soit inversée** et que le texte revienne aux définitions de la directive 95/46[1]. Cette modification ayant d'ailleurs été déjà intégrée dans le cadre de la proposition de règlement (document 11326/12), les autorités françaises demandent donc, par symétrie, que la même modification soit intégrée à la proposition de directive.

Concernant le point (1), définissant la « *personne concernée* », les autorités françaises s'interrogent sur l'inclusion des personnes physiques pouvant être identifiées « ***par des moyens raisonnablement susceptibles*** *d'être utilisés par le responsable du traitement ou par toute autre personne* ».

Cette extension par rapport à la directive 95/46 est source d'insécurité juridique en ce qu'elle constituerait une extension beaucoup trop large du champ d'application puisqu'elle aboutirait à prendre en compte l'usage que « toute autre personne » pourrait faire d'une information qui ne serait pas « identifiante » pour le responsable de traitement lui-même.

[1] *«données à caractère personnel»: toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.*

Toujours au point (1), les autorités françaises s'interrogent également sur les « *éléments spécifiques, propres à son identité* (…) *psychique* » et souhaitent des explications sur ce que recouvre cette nouvelle notion.

Concernant le paragraphe (4), qui doit définir la « *limitation du traitement* », celui-ci traite en réalité du marquage. Ce paragraphe devrait donc être modifié. Les autorités françaises relèvent que la définition retenue au point (4) reprend exactement les termes de celle du terme « *verrouillage* » de la décision-cadre 2008/977 (article 2, point c). Si cette définition devait être conservée telle quelle, il faudrait qu'il s'agisse de la même notion et donc de celle de « *verrouillage* » et non de celle de « *limitation du traitement* ».

Egalement en conformité avec les demandes formulées par les autorités françaises dans le cadre des négociations sur la proposition de règlement, la notion de « *tiers autorisés* » devrait être réintégrée dans la proposition de directive. Ainsi, concernant le point (8), sur la notion de « *destinataire* », la définition retenue dans la proposition de directive ne comprend pas les « *tiers autorisés* », qui figurent dans la directive 95/46. Or, les autorités françaises soulignent que ce concept est fondamental dans la pratique des organismes à qui la loi a donné un droit de « communication ».

En effet, avec la définition proposée dans le projet de directive, le responsable de traitement aurait aujourd'hui à sa charge des obligations contradictoires ou inapplicables en pratique. Ainsi le tiers autorisé ne peut être défini a priori comme destinataire d'un traitement puisqu'il fonde son accès aux données sur un texte légal extérieur au traitement lui-même (antérieur ou postérieur à l'existence de ce traitement). Pour les mêmes raisons, les obligations liées aux droits des personnes concernées ne peuvent peser sur le responsable de traitement. Ces droits iraient d'ailleurs souvent à l'encontre du but visé par le législateur lorsqu'il a octroyé un droit de communication au tiers autorisé.

Enfin, et toujours dans une démarche de cohérence avec les discussions sur la proposition de règlement, les définitions des données biométriques et des données concernant la santé font l'objet des remarques suivantes :

Concernant le point (11), sur la définition des « données biométriques », les autorités françaises souhaitent des explications sur la signification des « *caractéristiques comportementales d'une personne physique qui permettent son identification unique* ».

Concernant le point (12), sur la définition des « données concernant la santé », les autorités françaises relèvent que la notion de « *prestation de service à la santé* » parait extrêmement large à la lecture du considérant 17. Toutes les informations relatives à la santé d'une personne physique ne devraient peut être pas être traitées avec le même degré de protection.

Article 5 : Distinction entre différentes catégories de personnes concernées

Les autorités françaises demandent la suppression de cet article.

Subsidiairement, les dispositions de cet article 5 pourraient figurer comme considérant explicatif de l'article 4 que dans le corps de la proposition de directive.

Article 6 : Niveaux de précision et de fiabilité des données à caractère personnel

Les autorités françaises demandent également la suppression de cet article.

De même, subsidiairement, les dispositions de cet article 6 pourraient figurer comme considérant explicatif de l'article 4 que dans le corps de la proposition de directive.

Article 7 : Licéité du traitement

Les autorités françaises relèvent que cet article semble incohérent avec l'article 1er sur le champ d'application de la proposition de directive.

En effet, l'article 7 élargit le champ d'application de l'instrument puisque le point (a) de celui-ci renvoie à l'article 1er du texte, lequel couvre le champ d'application de l'instrument, tandis que les points (b), (c) et (d) concernent des situations hors de ce champ d'application (compte tenu de l'emploi de la conjonction de coordination « ou »). Cet élargissement est donc source d'insécurité juridique, et les autorités françaises s'interrogent sur sa plus-value.

Les autorités françaises rappellent ainsi leur proposition de rédaction alternative concernant l'article 1er (cf supra), et demandent la suppression de l'article 7, dans la mesure où le principe de licéité des traitements est déjà prévu à l'article 4, point a) de la proposition de directive.

En outre, les autorités françaises ont pris bonne note des débats sur cet article au sein du groupe de travail DAPIX le 26 septembre dernier et soulignent qu'elles sont tout à fait opposées à ce que le critère de consentement de la personne concernée soit introduit dans cet article et puisse constituer le fondement de la licéité des traitements dans les domaines spécifiques de la proposition de directive.

Article 8 : Traitements portant sur des catégories particulières de données à caractère personnel

La définition proposée ne correspond pas à celle retenue dans la directive 95/46, ni à celle de la décision-cadre 2008/977, ni à celle de la Charte des Droits Fondamentaux. Les autorités françaises s'interrogent donc sur les raisons ayant poussé la Commission à proposer une nouvelle définition des données sensibles et sur les choix des nouveaux termes retenus (en particulier le terme « *croyances* »).

Les autorités françaises souhaitent donc le retour à la définition retenue dans la décision-cadre 2008/977, en son article 6, qui mentionne « *les convictions religieuses ou philosophiques* » (et non les « *croyances* »).

IRELAND

Article 2 (Scope)

1. In paragraph 3(a), it is not clear if the exemption for 'national security' is intended to include 'defence' and 'public security'. Moreover, there is a further need to clarify the scope of the Directive vis-à-vis the scope of the Framework Decision which provides that it 'is without prejudice to essential national security interests and specific intelligence activities in the field of national security'.

Article 3 (Definitions)

2. The definitions should, where appropriate, be amended in line with any proposed amendments to the definitions in the Regulation.

3. Ireland is not convinced that the definition of 'child' should be included; the specific reference to children in article 45.2 does not appear to be relevant since this matter is already covered in article 52.2 of the proposed Regulation.

Article 4 (Principles relating to personal data processing)

4. The reference in paragraph (a) that personal data must be processed 'fairly' should be deleted. This principle has not been included in the existing Framework Decision and its inclusion in the proposed Directive could restrict police activities relating to the detection and investigation of offences.

5. Additional provisions are required to permit further processing in line with article 3.2 of the Framework Decision.

Article 5 (Distinction between different categories of data subjects)

6. It is not clear how far these rules can be implemented in practice because a data subject's categorisation may change in the course of an investigation. In any event, it is not clear how this article would result in increased protection of personal data and its added-value is therefore questionable.

Article 6 (Different degrees of accuracy and reliability of personal data)

7. It is not clear how this article could be implemented in practice. Whether or not personal data are accurate is frequently a matter for the courts to decide. Furthermore, it may not always be possible to classify personal data as fact or opinion; we therefore question the usefulness of the inclusion of this article in the Directive.

Article 7 (Lawfulness of processing)

8. The Directive should also allow for the processing of personal data on the basis of consent and for historical, statistical and scientific purposes where Member States provide appropriate safeguards.

9. The reference to 'immediate' in point (d) is too restrictive; it should be replaced with 'direct'.

10. Article 8 (Processing of special categories of personal data)

11. In paragraph 1 the word 'beliefs' is too vague and should be limited to 'philosophical beliefs' in line with the proposed amendment to article 9.1 of the Regulation. In paragraph 2, processing on the basis of data subject consent should also be permitted.

ITALY

- **Articolo 1**

  Appare necessario chiarire il concetto di "autorità competente ai fini di prevenzione, indagine, accertamento e perseguimento dei reati o esecuzione delle sanzione penali", per definire esattamente l'ambito di applicazione dei principi della direttiva. Si ritiene, inoltre, che sarebbe opportuno che fossero chiarite le interazioni tra direttiva e regolamento per tutti i casi in cui una stessa autorità svolga attività che ricadano in più ambiti, disciplinati in parte dalla direttiva ed in parte dal regolamento.

- **Articolo 2**

  Si richiede che venga specificato il concetto di 'autorità competente' per definire esattamente l'ambito di applicazione dei principi della direttiva.

  Con riferimento al secondo comma, il campo di applicazione dovrebbe essere inteso in maniera inclusiva rispetto ai trattamenti effettuati da organi e organismi dell'Unione.

  Si ritiene, inoltre, necessario un chiarimento sul concetto di 'sicurezza nazionale' previsto dal comma 3 lett. a).

  Si chiede, infine, di definire i rapporti tra l'art. 2, comma 3 lett.b) e l'art. 59.

- **Articolo 3**

  Si richiede che venga specificato il concetto di "autorità competente" per definire esattamente l'ambito di applicazione dei principi della direttiva.

  La delegazione italiana segnala, inoltre, l'opportunità che le definizioni presenti nella direttiva siano identiche a quelle previste dal regolamento.

- **Articolo 4**

  Si chiede la soppressione dell'avverbio 'tempestivamente' previsto dalla lett. d).

  Si segnala poi il disallineamento della previsione della lett. f) della direttiva, rispetto a quella contenuta nell'art. 5 lett. f) del regolamento.

- **Articolo 5**

  La delegazione italiana chiede chiarimenti in relazione alla categoria di cui alla lett. e) e, in particolare, chiede che venga espressamente prevista la residualità e provvisorietà dell'inserimento nella stessa.

  Appare anche opportuno prevedere espressamente quali siano le conseguenze collegate all'introduzione nelle varie categorie.

- **Articolo 6**

  Si chiede l'eliminazione della norma, ritenendosi sufficiente la previsione contenuta nel considerando 24.

- **Articolo 7**

  Poiché le previsioni di cui alle lett. b), c), d) sembrano già ricomprese in quella di cui alla lett. a), si chiede che la Commissione chiarisca il valore aggiunto delle previsioni di cui alle lett. b), c), d).

- **Articolo 8**

  Si chiede che la norma, di cui si condivide il contenuto, venga redatta in termini più precisi e chiari, per evidenziare che le garanzie previste dalla legge in ordine al trattamento dei dati sensibili, non si applicano nel settore di operatività della direttiva.

LITHUANIA

General remarks

Lithuania expresses its appreciation for the invitation to provide comments and proposals for a Directive. The Directive and the General Regulation presented by the Commission is an opportunity to modernize and harmonize European data protection legislation and to improve execution of rights of data subject which is a key element to boost individuals' trust in the digital environment and thereby a potential driver of economic growth and innovation.

Lithuania would like to draw attention that developing of a common framework for the data protection in European Union (further – EU) is value however that does not create a situation when the same issues might be treated differently in the regulation and the directive. Also situations then the same personal data at different stages of their processing will be regulated by two legal acts.

Lithuania supports the goal for creating a coherent and more uniform set of data protection rules consistently applied across the EU. It would be instrumental in eliminating the current costs and administrative burden for business deriving from different national data protection rules and requirements.

Lithuania asked a scrutiny reservation on the nature of the proposal of the Commission and particularly the use of two legal acts – the regulation and a directive. Lithuanian proposal is to regulate data protection issues by only one legal act – the directive in both in the public, including enforcement bodies, and private sector.

Comments and proposals on the Regulation article by article

1. Article 1 Paragraph 1

The wording of the paragraph might be confusing since the word "prosecution" may be understand as implying application of the Directive to the courts. However the regulatory authorities usually do not have a jurisdiction to supervise the activities of courts. Lithuania suggests clarifying the application of the Directive providing in Paragraph 3 of Article 2 that the Directive is not applicable in the courts case handling activities.

2. Article 2 Paragraph 3 Subparagraph b)

From the wording of this subparagraph one might get the impression that the Directive will not apply to the processing of personal data processed, for example in the Schengen system. In this case, it may be difficult to distinguish between information relating to Schengen and not, therefore in the Directive it should be clearly distinguished.

3. Article 3 Paragraphs 1 and 2

Since in both projects – the Regulation and the Directive, the definitions of personal data and the data subject are the same, Lithuania proposes to take into account Danish presidency's proposal on definition, indicating that the Lithuanian delegation is of the opinion that the addition of the provision that a person should be regarded as non-identifiable if the identification requires a disproportionate effort, time, cost and material resources are of evaluative nature and it is suggested to have them explained in more detail, specifying when a particular time consumption and (or) physical resources shall be considered as a disproportionate.

4. Article 3 Paragraph 8

The definition of the recipient does not provide an exception to regulatory and supervisory authorities. Lithuania is concerned that in case authorities mentioned will be regarded as data recipients, it can hamper effective performance of their functions. Lithuania proposes to supplement this paragraph as follows "**The authorities provided in Article 39 of the Directive as well as other state and municipal institutions and agencies shall not be regarded as data recipients when they obtain personal data in response to a specific request for the purposes of fulfilling their control functions laid down in laws.**"

5. Article 3 Paragraph 9

In the interpretation of the definition of the personal data breach is provided that it is a breach of security, so Lithuania would like to propose amend definition providing by this way "~~personal~~ data **security** breach…".

6. Article 3 Paragraph 11

In the definition of the biometric data is provided that they allow the unique identification of an individual, but the biometric data can be used for authentication, without any identification, so Lithuania proposes to adjust the definition accordingly.

7. Article 3 Paragraph 11

In the Directive is provided definition of the child, however unlike the Regulation, the Directive do not provide different child data processing regulation. Lithuania suggests considering whether in such case the definition of a child shall be left in the Directive. Also we would like to pay attention to the fact that the child's biometric data, such as image, change very quickly, so, probably it should also be reflected in the Directive.

8. Article 5 Paragraph 1

Lithuania proposes to delete the words “so far as possible” whereas it must be possible to identify specific category to which data subject belongs. In addition, at the moment it is unclear how the categorization will help to better personal data protection and taking into account the fact that it will be subject also to non-automatic data processing Lithuania considers it as a significant increase in the administrative burden and costly reconfiguration of existing systems, and therefore proposes to delete this Article or introduce a very clear categorization criteria, further diversification of processing of different data subjects categories data in the Directive and provide the funds for the reconfiguration of existing systems. The same applies to Paragraph 1 of Article 6.

9. Article 6 Paragraph 2

The wording of the paragraph might be confusing because it is not clear what might be data based on a personal assessment and what would be the reliability and accuracy of such data. It is questionable whether such data – personal assessment at all can be considered as personal data. Therefore Lithuania suggests deleting this article or having it clarified.

10. Article 7

In the Article 7 of the Directive are established grounds for lawful processing of personal data, but the consent is not among them. Lithuania considers that consent might be provided as a legal ground for personal data processing, because it is doubtful whether in all cases the victim’s data can be processed without consent. The same can be for police informers and in other situations where grounds provided in the Article 7 may not be proper.

Furthermore, the article does not provide the ground, where the data is needed for a court hearing, which may cause problems when, for example, in a civil case for damages against the perpetrator of crime will be required data from the criminal case.

Therefore Lithuania suggests include in the Article 7 those two grounds of a lawful processing.

11. Article 8 Paragraph 1 and Paragraph 2 Subparagraph c)

The wording of the paragraph 1 might be understood twofold: even though it is not defining sensitive data, but according to the title of the Article 8 it can be considered as doing such. In fact, in this paragraph sensitive data listed is consistent with the one in Article 9 of the Regulation, with the exception of criminal convictions. Therefore, it seems that what shall be considered as a sensitive data in the Regulation and the Directive are not the same and this may lead to legal uncertainty, especially when the question of application of the Regulation or the Directive will occur, for example in case of such data transfer in one country data will be regulated by the Regulation and in another by the Directive.

Also the wording of the paragraph 2 c) might be confusing, because it is not clear when the data shall be considered as a "manifestly made public" and what would be a legal basis and the reliability of such data to the processing for law enforcement purposes.

Lithuanian suggestion is to discuss once again the wording of Article 8 Paragraph 1 and Paragraph 2 Subparagraph c) in order to change it in more practical and harmonized with the Regulation way.

HUNGARY

The legislative instrument

Hungary does not see any substantial legal reason why the Commission's proposal for the new data protection framework does not manifest itself in a single legislative instrument that is applicable to every data processing operations falling into the competence of the European Union, including the area of police and criminal justice. Moreover no convincing legal argument is seen by Hungary that supports the Commission's proposal to regulate the data protection rules in diverging legal instruments, i.e. a regulation and a directive.

Hungary is of the opinion that Art 8 of the Charter of Fundamental Rights and Art 16 of the TFEU call for a comprehensive, consistent data protection framework that is applicable horizontally, providing with the same level of data protection throughout the Union, irrespective of the field of application of these rules.

Hungary notes and agrees the necessity of specific rules concerning the area of police and criminal justice as it stems also from *Declaration 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation*, however in Hungary's understanding this need does not justify the difference of the chosen legal instrument concerning the general data protection rules and the specific rules concerning the area of police and criminal justice.

In Hungary's view these latter specific rules could be part of the very same instrument – according to the position of Hungary a directive – the generally applicable provisions are part of.

Chapter I

Scope

According to Article 2 (1) of the of the draft directive the "*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.*".

Article 3 (5) defines a filing system as "*any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis*".

In addition Article 3(3) defines processing as "***any operation*** *or set of operations which is performed upon personal data or sets of personal data,* ***whether or not by automated means***".

Hungary doubts that either Art 8 of the Charter of Fundamental Rights or Art 16 of the TFEU may be interpreted so that data processing other than by automated means of personal data which **does not** form part of a filing system or are **not** intended to form part of a filing system is excluded of the scope of the EU-wide regulation concerning data protection in the field falling into the scope of the draft directive.

The distinction of data processing by automated means and other means seems to run counter to the goal of a consistent data protection legislative framework. Being a fundamental right the protection of individuals with regard to the processing of personal data may not depend on the means by which this fundamental right might be infringed.

On the contrary: Hungary believes that the particular importance of data protection makes it inevitable to provide data subjects with the protection as universal and holistic as possible and that the principles of data protection shall apply regardless of the means of data processing. Nevertheless, if circumstances concerning the various means of data processing make it necessary specific rules should be drafted to be applicable to automated and non-automated (manual) means of data processing operations.

Therefore Hungary suggests the following wording in Article 2 (1) of the draft directive:

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~~ irrespective of the means by which personal data are processed.

As a consequence Article 3 (3) should read as follows:

option Nr. 1

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

option Nr. 2

'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,~~ *irrespective of the means by which personal data are processed*, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Definitions

Hungary proposes to consider adding the definition of 'depersonalising through masking out of data' to the present set of definitions. This definition is contained in the *Proposal for a Directive of the Council and the European Parliament on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime* however it might be useful to be stated also in the draft directive as this technique can be applied to any data processing falling into the scope of the draft directive.

Article 3 (8)

Hungary is of the opinion that further clarification would be helpful regarding the definition of 'recipient' as the current definition may be interpreted so that a recipient may also be the data subject, the data controller or the data processor which persons should not be covered by the definition.

'recipient' means a natural or legal person, public authority, agency or any other body *other than the data subject, the data controller or the data processor* to which the personal data are disclosed;

Alternatively the definition of 'third party' may be added to the current set of definitions:

'recipient' means a ~~natural or legal person, public authority, agency or any other body~~ *third party* to which the personal data are disclosed; '*third party' means a natural or legal person, public authority, agency or any other body other than the data subject, the data controller or the data processor;*

Article 3 (9)

The present definition of 'personal data breach' deals only with data security breaches however serious consequences may arise due to accidental or unlawful misconducts by the data controller or the data processor other than those relating to data security provisions. For example in Hungary's view it is not evident whether such a case is also covered according to the current wording when despite appropriate technical and organisational measures were implemented to protect personal data – thus data security provisions were fully met – the data processor processes personal data in a way incompatible with the legitimate purpose or processes personal data for a longer period than it would be legitimate.

Hence, Hungary suggests to draft a clear-cut definition so that it covers each and every incidents stemming from the breach of the provisions of the directive and leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

'personal data breach' means a breach of ~~security~~ the provisions of this directive leading to any unlawful operation or set of operations performed upon personal data such as the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Article 3 (10) and (11)

In Hungary's opinion further clarification would be helpful concerning the definition of 'genetic data' and 'biometric data' as the present wording seems to be not sufficiently precise thus it might cause difficulties to determine whether a personal data is a biometric data or a genetic data or both biometric and genetic data.

Article 5

Distinction between different categories of data subjects

Article 5 sets out the obligation of the Member States to "*provide that, as far as possible, the controller makes a clear distinction between personal data of different categories of data subjects"*.

Hungary has reservations about the current wording of Article 5 as it seems to lack the sufficient clarity. On the one hand the provision does not define the essence of the obligation: it does not define *how* the distinction should be made between the categories of data subjects.

On the other hand it is not clear to which persons the text "*associate to one of the persons mentioned in (a) and (b)*" is applicable. If this text refers to persons who are associates of the suspected perpetrator of the criminal offence, it is not clear why a distinction shall be made between the associates' personal data and the personal data of the suspected perpetrator [i.e. between the categories drafted in points (a) and (d) of Article 5].

Based on the above mentioned comments, Hungary suggests redrafting Article 5 accordingly.

Article 6 (1)

Different degrees of accuracy and reliability of personal data

Article 6 (1) sets out the obligation for Member States to "*ensure that, as far as possible, the different categories of personal data undergoing processing are distinguished in accordance with their degree of accuracy and reliability"*.

According to point (d) of Article 4 "*Member States shall provide that personal data must be […] accurate […]"*.

Hence, in Hungary's understanding the requirement that the processed personal data shall be accurate when processed is a fundamental principle that is applicable to each and every data processing irrespective of the nature of the processing. As a consequence inaccurate personal data may not be processed and the provision enshrined in Article 6 (1) and the obligation thereof to distinguish between the processed personal data in accordance with the degree of accuracy seems to run counter with the mentioned fundamental principle.

Hungary advocates to clarify the wording of Article 6 (1) in order the ensure consistency with point (d) of Article 4.

Article 7

Lawfulness of processing

Article 7 lists the grounds based on which a data processing falling into the scope of the draft directive may be deemed lawful.

Hungary wishes to draw attention to the fact that the ground for processing set out in points (a) and (b) of Article 7 are not accompanied by a provision stipulating that the basis of such processing must be provided for in either Union law or the law of the Member State to which the controller is subject. The omission of such a provision seems rather unjustifiable as a similar provision is set out in Article 6 (3) of the draft general data protection regulation.

Therefore Hungary advises to add a paragraph to Article 7 with the following wording:

2. The basis of the processing referred to in points (a) and (b) of paragraph 1 must be provided for in: (a) Union law, or (b) the law of the Member State to which the controller is subject.

Article 8 (2)

Processing of special categories of personal data

Article 8 (2) exhaustively lists the cases where the processing of special categories of personal data are exempted from the general prohibition to process such data.

Hungary is of the opinion that it should be made entirely clear in the text that special categories of personal data might also be processed if the data subject has given his/her explicit consent to the processing. Unless such a ground for processing is not inserted into Article 8 (2) the right for informational self-determination of the data subject might be infringed without any valid reason.

Hungary suggests the following wording for Article 8 (2):

Paragraph 1 shall not apply where: (a) the processing is authorised by a law providing appropriate safeguards; or (b) the processing is necessary to protect the vital interests of the data subject or of another person; or (c) the processing relates to data which are manifestly made public by the data subject, (d) the data subject has given consent to the processing of their personal data for one or more specific purposes.

Processing personal data for historical, statistical and scientific research purposes

The draft directive does not regulate the specific conditions for processing personal data for historical, statistical and scientific research purposes.

In Hungary's view such provisions are needed with regard to data processing operations falling into the scope of the draft directive hence it deems necessary to draft and add these rules to Chapter II of the draft directive.

AUSTRIA

Österreich bedankt sich bei der Präsidentschaft für die Gelegenheit zur Stellungnahme. Die Anmerkungen erfolgen in deutscher und in englischer Sprache und verstehen sich als Ergänzung zu den in den Sitzungen der Ratsarbeitsgruppe DAPIX bereits mündlich vorgetragenen Positionen.

Austria would like to thank the Presidency for the possibility to comment on the footnotes concerning Articles 1 to 8. Below, please find our comments in German as well as in English. These comments shall constitute a supplement to the comments already expressed orally during the DAPIX-meetings.

Zu Artikel 2:

Zu Artikel 2 Absatz 3 ist neuerlich festzuhalten, dass eine klarere Umschreibung des Anwendungsbereichs der Richtlinie möglich und wünschenswert wäre. Von besonderer Bedeutung ist dabei die präzise Abgrenzung des Anwendungsbereichs des Richtlinienentwurfs vom Anwendungsbereich des Verordnungsentwurfs. Es wird angeregt, in einem Erwägungsgrund anhand von Beispielen darzulegen, in welchen Konstellationen von der Vollziehung des Unionsrechts auszugehen ist.

Zu Artikel 5:

Die Republik Österreich wiederholt weiters ihre Anmerkung, dass der Richtlinienvorschlag keine unmittelbar erkennbaren Rechtsfolgen an die Unterscheidungen von Kategorien von Daten knüpft, wie sie durch die Unterteilung in Artikel 5 Absatz 1 a) bis e) vorgenommen wird. Die Sinnhaftigkeit dieser Unterteilung wird daher in Frage gestellt, zumal es ohnehin einen allgemeinen Grundsatz der Richtlinie darstellen wird, dass die jeweils verantwortliche Stelle auf die Aktualität und die Richtigkeit der von ihr verarbeiteten Daten achtet (siehe Artikel 4 d). Soweit die gegenständliche Bestimmung daher konkrete Kategorien festlegt, stellt sich die Frage nach den konkreten Rechtsfolgen dieser Kategorien, beziehungsweise nach den Konsequenzen für den Fall, dass sich der Status einer Person ändert.

Sollte Artikel 5 lediglich bezwecken, eine nähere Konkretisierung des in Artikel 4 d) verankerten Grundsatzes der Aktualität und Richtigkeit der Daten vorzunehmen, müsste dies zur Vermeidung von Missverständnissen in den Erwägungsgründen klargestellt werden.

Weiters wird angeregt, die in Artikel 5 e) genannte Kategorie in Erwägungsgrund 23 anhand von Beispielen näher zu darzulegen.

Zu Artikel 7:

Es sollte entsprechend Art. 3 Abs. 2 letzter Satz des Rahmenbeschlusses Datenschutz eine Regelung betreffend die Datenverarbeitung zu statistischen bzw. wissenschaftlichen Zwecken innerhalb des Anwendungsbereichs der Richtlinie aufgenommen werden.

Zu Artikel 8:

Im Sinne der Einheitlichkeit des Schutzstandards wäre es zweckmäßig, (allenfalls in den Erwägungsgründen) Anhaltspunkte dafür zu geben, was unter „geeigneten Garantien“ im Sinne von Artikel 8 Absatz 2 a zu verstehen ist.

Ad Article 2:

Concerning article 2, paragraph 3, it should be noted that the scope of the Directive must be defined in a clear and precise way. Therefore the precise definition and distinction of the scope of the draft directive and the regulation is of particular importance in order to prevent difficulties in establishing which instrument is applicable. We suggest furthermore a clarification in a recital (possibly with examples) to illustrate which activities fall inside the scope of Union Law. To avoid future doubt it is strongly suggested that this should be clarified in the recitals.

Ad Article 5:

We would also like to repeat our comment that no legal consequences are connected to the distinction between different categories of data subjects (Article 5). The usefulness of this distinction is questionable, especially because it is already a general principle that every controller is responsible to keep data accurate and up to date (see Article 4d). In view of this principle there seems to be no need for a specific enumeration of categories. As to the legal consequences of this distinction the question arises what shall happen in the event that the status of a person changes.

If the sole purpose of Article 5 is the concretization of Article 4 d (accurate and up to date data) this should explained in a recital in order to avoid misunderstandings.

Furthermore, we suggest to clarify Article 5 e and to give some examples in recital 23.

Ad Article 7:

According to Art. 7 para 2 last sentence of the Framework Decision the data processing for statistical and scientific purposes within the scope of the Directive should be included.

Ad Article 8:

For consistency of standards of protection it would be appropriate to give (possibly in the recitals) guidance on what is meant by 'appropriate safeguards' within the meaning of Article 8, paragraph 2 a)

POLAND

As a general comment, we would like to highlight that information provided below are tailored in a way so as not to mention again what the PL delegation already stated on DAPIX meetings (as requested in doc. CM 4718/12). Still we would like to reaffirm that we uphold the comments made by the PL delegation on DAPIX meetings up until now, including those concerning doubt on the practical execution and purposefulness of rules set up in art. 5 and 6 of the proposal.
Simultaneously, the PL general scrutiny reservation concerning the proposal is uphold.

Charter I General provisions

Art.1.

- PL believes it will be useful to make the wording of art.1 par.1 more precise according to the below mention suggestion:

  "This Directive lays down the rules relating to the protection of individuals with regard to the processing of personal data of ***the individuals*** by competent authorities for the purposes of the prevention, investigation, ***detection of crime and perpetrators*** or prosecution ***of perpetrators*** of criminal offences or the execution of criminal penalties."
  „Niniejsza dyrektywa ustanawia przepisy dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych ***tych osób*** przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ***przestępstw*** i ich ***sprawców*** lub ścigania ***sprawców*** i wykonywania kar kryminalnych."

- Keeping in mind that the legal basis for the proposal in art.16 (2) TFUE, it is doubtful the scope expressed in art.1 par.2 letter (a). The provision of the draft directive refers generally to fundamental rights and freedoms of a natural person, whether the art.16(2) TFUE refers exclusively to data protection.

Art.2

- PL considers it doubtful whether the directive covers the field of information protectively marked as classified. On the one hand the exclusion referred to in art.2 par.3 letter a should be taken into account (national security), on the other hand the directive sets an obligation of professional secrecy on confidential information (art.43 of the proposal). PL seeks for clarification of this issue.

Art.2 in connection with art.7

- PL seeks for clarification on issue of applicable rules for processing of data for a statistical, historical and scientific purposes that are connected with crime prevention and/ or execution of criminal penalties – which legal act (directive – regulation) is to regulate this specific processing situation (the issue arises as the draft directive lacks of provision similar to art.83 of the draft regulation, while the latter is restricted by the art.2 par.2 letter (e)).

Art.3

- **Definition of „data subject" in art. 3 point 1 – comment similar to the comment made by PL delegation concerning art.4 par. 1 of the draft regulation**
  According to the definition "data subject" means "an identified natural person or a natural person who can be identified". A natural person can be considered as "identified" when, within a group of persons, he or she is "distinguished" from all other members of the group and consequently can be treated in the other way. It was defined in the adopted opinion of the Data Protection Working Party[1] (WP136). Therefore the recital 16 should be amended so as to explain that the traceability covers also distinction (identification).

[1] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pl.pdf

Chapter II – Principles (excluding art.9)

Art.4

- Letter (b) – there is a need for clarification whether the provision allows for making data collected in conformity with law available to other authorities which do not perform tasks related to the purposes described in art.1 par.1 of the proposal, in a situation where law sets an obligation to transmit the data for the purposes different then those which were applied for collation of data (assuming that purposes for making the data available are also set by the law).

Art. 5:

- As a general remark, it should be kept in mind that the authorities may have various other distinctions than those referred to in the catalogue of art.5 – depending on the tasks they are oblige to perform (categories of data processed by the Police will differ from those processed by the Prosecution or the Prison Service). Thus, it may pose a problem to identify the complete catalogue of categories of data subject.
- It is still not clear whether the category of distinction is "personal data" or "data subjects".

Art. 6

- PL seeks for further clarifications whether the obligation for distinction between different degrees of accuracy and reliability of personal data concerns each single information separately stored in a filling system. In other words, if there is a number of information concerning a data subject processed in a filling system, should it mean that the assessment of accuracy and reliability concerns a data subject or separately each information on the data subject.
- PL seeks for confirmation whether the provisions of art.5 and art.6 should be interpreted together as a whole.

Art. 7 in conjuction with art.1 and 4

- PL seeks for clarification on the issue of transfer of data between Member States, in particular: 1/ whether the receiving MS can process a received data for the purpose other then purpose which was the ground for collection of the data in sending MS; 2/ whether the sending MS has a possibility to restrict the scope of processing of the data in a receiving MS.

Art.7

- Letter (a) refers to phrase *„based on law"*. It is not clear what is the scope of the term. In an explanatory note it s stated that *"Article 7 sets out the grounds for lawful processing, when necessary for the performance of a task carried out by a competent authority based on national law(…)"*. It seems that restricting this reference only to national law is too narrow interpretation, as such an obligation may arise for instance on the ground of the EU legislation.

ROMANIA

Romania would hereby like to express its proposals on **art 1-8 of the above Directive Proposal,** as follows:

Article 1 - Subject matter and objectives

Paragraph (1): *" This Directive lays down the rules relating to the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties."*

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

Explanation:

RO would like that all the activities of the Police be covered by one instrument – the Directive, otherwise the police authorities would end up in situations where provisions of both the Regulation and the Directive apply and that would lead to uncertainty in implementing the legislation on data protection field.

Moreover, as the Article 29 Working Party stated in its opinion on the reform package *"situations must be avoided where the same data processing operation, such as in relation to maintaining public order in one country is covered by the Regulation, where in other Member States the laws based on the Directive apply."*

For example, when referring to road legislation, the same deed may be considered an offence in Romania, according to RO legislation, but in Spain it may be considered a crime, according to ES legislation. In this case, in Romania the Regulation would apply, whereas in Spain the Directive would be applicable. Firstly, in this case we notice the lack of consistency in applying the data protection legislation at the EU level. Secondly, we could easily understand that when a transfer of this personal data between Romania and Spain takes place, these countries would treat the data differently (RO would apply the provisions of the Regulation and Spain the provisions of the Directive) instead of applying unitary provisions.

That is why we truly believe that it is necessary that all the police activities should be governed by only one instrument.

Article 3 – **Definitions**

Paragraph (3) (definition of processing) - RO would like to ask for clarifications regarding the practical meaning of terms "**structuring**" and "**alignment**".

Explanation:

In order to put this paragraph into practice it is important to understand the practical operation of the processing that the terms refer to.

Article 6 – Different degrees of accuracy and reliability of personal data

Paragraph (1) - RO would like some clarifications and explanations regarding the meaning of „**reliability**" of personal data.

Article 8 - Processing of special categories of personal data

In paragraph (2), point a,

RO would like to bring to attention that paragraph 2a is too wide and general and does not provide the minimum safeguards when the special categories of personal data may be processed, in order to ensure a unitary application of the directive at EU level. If the text of the directive remains as it is presently, then, for example, Romania will provide in the national law a series of safeguards that permit the processing of special categories of personal data, whereas other MS may provide different safeguards, that can be more or less restrictive than those of RO national law. In this case, this article isn't applied unitary at EU level.

In this context, RO proposes that a minimum set of safeguards be provided in art 8(2a) which must be observed by all MS, and then, during the transposal of the Directive in the national law, adding extra safeguards to ensure a more restrictive processing of these special categories of personal data, being let to the decision of each MS.

In paragraph (2), point a - RO would like some clarifications, explanations and examples regarding the meaning of expression „**appropriate safeguards**", based on the scope of the directive.

FINLAND

General comment:
In the negotiations on the Framework Decision, FI supported its application to the national processing of personal data. FI observes that the provisions of the proposed Directive are more detailed than those of the Framework Decision, and there are new types of provisions. Therefore, the final view on whether the Directive should apply to purely national processing of data will be formed once the final outcome of the working party discussions is available.

Article 1
The exact coverage of the expression “prosecution” should be clarified as to whether it covers court and to what extent. The same question concerns Article 3, point (14). In the Framework Decision, the definition of ‘competent authorities’ expressly covers judicial authorities, when they are processing personal data, inter alia, for the purpose of prosecution of criminal offences. It is somewhat unclear whether the competent authorities in the proposed Directive are intended to cover both prosecutors and courts of law.

Article 2
Paragraph 3(a) should be supplemented in the same way as the corresponding provision of the proposed Regulation has been supplemented, by adding reference to other activities falling outside the scope of Union law. Preference should be given to the wording used in the Treaty (public security, defence and State security).

Article 3

The definition of ‘personal data’ appears to be very wide and should be made more precise. FI proposes that the definitions of ‘data subject’ and ‘personal data’ in points (1) and (2) be at this stage aligned with the proposed new drafting of the same definitions in the proposed Regulation. However the definitions need further consideration.

FI notes that the concepts of ‘referencing’ and ‘blocking’ used in the Framework Decision have been replaced with ‘restriction of processing’. FI does not object to the change, but points out that in Article 16(3), the expression used is ‘marking’, whereas the term defined in Article 3 is ‘restriction of processing’. Article 3, point (4), and Article 16 should be aligned so that the term defined is that used in Article 16.

FI notes that the definition of ‘child’ has been deleted in the new drafting of the proposed Regulation. The proposed Directive should be aligned with that drafting.

Article 5

FI observes that many delegations found Article 5 problematic. FI does not object to the principle of drawing a distinction between different categories of data subjects, in the understanding that flexibility is left to Member States as to how it is technically done. However, points (c) and (d) of Article 5 should be clarified as to whether the provision is intended to cover potential victims of a criminal offence and as to the exact meaning of “contacts” and “associates”.

Article 7

FI suggests that Article 7 be placed after Article 4 in the text.Article 7 defines the principle of lawfulness in point (a) of Article 4, and thus those two Articles would belong logically together.

FI considers that the proposed Directive should also allow the further processing of data for historical, statistical or scientific purposes in the same way as the Framework Decision does, provided that Member States provide appropriate safeguards (such as making the data anonymous). That further purpose could be included in Article 7. The further processing of personal data for statistical purposes should be possible irrespective of the origin of the data (national/ foreign).

Article 8

FI observes that 'genetic data' was not included in the Article on the processing of special categories of personal data. FI does not find its inclusion in Article 8 of the proposed Directive problematic. However, provided that DNA data are considered to fall within the category of genetic data, it is important to ensure that efficient exchange of DNA data between the police authorities is not jeopardised. The current wording appears to take that need into account. Addition of reference to DNA data could be considered in Article 3 (e.g. by including it in the definition of genetic data) as it also includes a definition of 'biometric data'. DNA data is the most common type of genetic data processed by the law enforcement authorities.

SWEDEN

Sweden welcomes the possibility to send in comments and proposals for amendments. In this document, after some general remarks, relevant parts of the draft directive are reproduced with our comments and proposals for changes and clarifications inserted in ***bold italics*.**

No summaries of the discussions and no new versions of the text with MS opinions included have yet been distributed. Thus we cannot foresee which of the comments made by Sweden during the negotiations have been noted and will be reflected in the documentation. This explains why many of the comments in this document do reiterate what Sweden has expressed in the negotiations. We also reserve the right to review our comments and proposals in the light of further discussions. Comments and proposals in this paper should therefore still be considered as preliminary.

General remarks

Sweden welcomes that the law enforcement part of the reform package is presented as a separate directive. In order to strike a proper balance between the interests involved it is necessary to have customized data protection rules for law enforcement and criminal justice. The relationship between the directive and the general data protection regulation needs clarification and a fully coherent terminology must be assured.

It is far too early to draw any conclusions about the effectiveness of the framework decision. There are very few indications that its limited scope has caused any problems to member states authorities. It is therefore difficult to see today the justification for expanding the area of application of EU legislation to purely national processing of data in law enforcement and criminal justice.

It is important that the proposed directive does not prevent law enforcement from using modern technology in the fight against crime. Rules on data protection in the area of law enforcement and criminal justice run a real risk of coming into conflict with member state legislation on investigation and criminal procedure. Due to the complexity and differences between national legal systems, legislation in this field can only be harmonised at the EU level to a limited extent. Sweden believes that the proposed level of harmonisation goes too far and does not leave enough room for manoeuvre to Member States. Moreover, it is necessary to examine whether the proposed directive is clearly within the legislative competence of the Union.

Sweden's standpoint right now is that the proposed extension of the directive beyond the area of application of the framework decision is not in conformity with the subsidiarity principle. Finally, there are a number of provisions where the conformity with the principle of proportionality may be questioned.

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 authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

Comment: A thorough analysis is needed of the implications of the wording "…by the Member States when carrying out activities which fall within the scope of Union law" in Article 16 TFEU for EU legislative competence in the area of criminal justice and law enforcement.

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

(b) ensure that the exchange of personal data by competent authorities within the Union is neither restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.

Comment: The meaning of Article 1.2 b and its effect for Member States needs to be clarified. Possibly the paragraph needs re-wording.

Article *2*

Scope

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

Comment: EU-regulation of national processing of personal data in the area of law enforcement and criminal justice is not in conformity with the principle of subsidiarity. A thorough analysis is needed of the implications of the wording "…by the Member States when carrying out activities which fall within the scope of Union law" in Article 16 TFEU for EU legislative competence in the area of criminal justice and law enforcement.

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;

Comment: It is not clear which change is meant with the new wording "… concerning national security." In absence of compelling reasons for change the wording of the DPFD should be retained ("essential national security interests and specific intelligence activities in the field of national security.").

As in the DPFD, there should be an article stating that "This [Directive] shall not preclude Member States from providing, for the protection of personal data collected or processed at national level, higher safeguards than in this [Directive]."

Article 3

Definitions

Comment: Generally, the definitions should be the same in the Directive and in the Regulation. This is particularly important since Member States will issue complementary legislation to implement the Directive.

For the purposes of this Directive:

(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifiers or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

(2) 'personal data' means any information relating to a data subject;

Comment: Points (1) and (2) should have the same wording as in the latest version of the DPFD, i.e. points (1) and (2) should be merged to one definition of "personal data"('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, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to 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 . If identification requires a disproportionate amount of time, effort or material resources the natural living person shall not be considered identifiable).

If points (1) and (2) are not merged, the second part of point (1) ('in particular by reference to an identification number, location data, online identifiers or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person') should be moved to point (2).

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

Comment: A definition of 'restriction of processing' might be useful. However, we do not recommend the current definition ("marking….with the aim of limiting their processing…"), since such a definition results in a circular argument. Further, since the proposed directive does not contain any substantial provisions on the "restriction of processing", a definition of that wording is unnecessary.

Another alternative would be to let the definition (or a similar definition) in Article 3 (4) define the term "marking" instead of "restriction of processing". This solution would be more adequate, since Article 16.3 says that the controller shall (in certain cases) mark the personal data instead of erasing them, for example where the data subject opposes their erasure and asks the restriction of their use (Article 16.3 c).

(10) 'genetic data' means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development;

Comment: The scope of this definition needs to be narrowed and clarified. In our view it is far too wide since it could include many of the information types usually processed by the competent authorities for identification of persons (DNA-profiles, physically distinguishing features such as colour of skin, hair and eyes or even fingerprints, which are developed during prenatal development!) Many of these data do not require a genetic analysis and these categories of data should not fall within the "special" categories in Article 8. DNA profiles are the result of an analysis (of non coding or "trash" DNA) but the profile such as it is stored in the forensic registers does not allow any other conclusions than an eventual identity match with another profile from the same person.

(11) 'biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data;

Comment: The scope and the purpose of this definition need to be clarified. The term does not appear anywhere else in the text of the Directive.

If the definition is to be kept, the meaning of 'behavioural characteristics' needs clarifying.

(12) 'data concerning health' means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;

Comment: The scope of this definition needs to be narrowed and clarified. Some types of data commonly used for identification (scars, limp etc.) would fall within this definition and thus under the limitations of Article 8, which cannot be the intention.

(13) 'child' means any person below the age of 18 years;

Comment: This definition is not needed. The word does only appear in Article 45, in connection with the duties of supervisory authorities (where it would unnecessarily limit the target group).

CHAPTER II

PRINCIPLES

Article 4

Principles relating to personal data processing

Member States shall provide that personal data must be:

(c) adequate, relevant, and not ***excessive*** ***(translation error in the Swedish version: "too extensive")*** in relation to the purposes for which they are processed;

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

Comment: The words "in a form which permits identification of data subjects" should be deleted since data which does not permit identification of persons is not personal data (c.f. Art. 3.1).

(f) processed under the responsibility and liability of the controller, who shall ensure compliance with the provisions adopted pursuant to this Directive.

Comment: Art. 3.2 of the DPFD dealing with processing for "historical, statistical or scientific purposes" must be included in the directive. This is important for those purposes and also for the right of public access to official documents.

~~*Article 5*~~

~~*Distinction between different categories of data subjects*~~

~~*1. Member States shall provide that, as far as possible, the controller makes a clear distinction between personal data of different categories of data subjects, such as:*~~

~~*(a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;*~~

~~*(b) persons convicted of a criminal offence;*~~

~~*(c) victims of a criminal offence, or persons with regard to whom certain facts give reasons for believing that he or she could be the victim of a criminal offence;*~~

~~*(d) third parties to the criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, or a person who can provide information on criminal offences, or a contact or associate to one of the persons mentioned in (a) and (b); and*~~

~~*(e) persons who do not fall within any of the categories referred to above.*~~

Comment: SE proposes to delete this article. The meaning of "clear distinction between personal data of different categories of data subjects" is not clear, neither are the practical and legal consequences.

It may cause major difficulties in the exchange of information between Member States for a number of reasons put forward in the September meeting. It would probably increase costs and administrative burdens.

Courts need to be neutral and impartial and cannot classify persons according to "status" other than in the sentence.

SE sees no added value in the proposal. It should be left to Member States to decide whether they want to categorise data subjects or information.

Comments IN CASE THE ARTICLE IS TO BE KEPT:

The definition of different levels of suspicion (the words "serious grounds for believing") should be avoided. Levels of suspicion are regulated and defined in various ways in Member States legislation of criminal procedure, where they form prerequisites and conditions for different judicial actions, including the appointment of a lawyer or decisions about coercive measures.

The last three paragraphs (c-e) should be merged to one.

Finally, it should be clarified that it is sufficient that the status of a person in the process is clear from the context.

~~***Article 6***~~

~~***Different degrees of accuracy and reliability of personal data***~~

~~***1. Member States shall ensure that, as far as possible, the different categories of personal data undergoing processing are distinguished in accordance with their degree of accuracy and reliability.***~~

~~***2. Member States shall ensure that, as far as possible, personal data based on facts are distinguished from personal data based on personal assessments.***~~

Comment: SE proposes to delete this article. The meaning of "clear distinction" is not clear, neither are the practical and legal consequences.

Criminal intelligence, investigation and court procedures deal with the verification and refinement of information. The degree of correctness and value of the information at any given moment are by necessity clear from its context, which in turn is regulated by Member States legislation of criminal procedure.

Article 4 c) and d) establish a demand for adequacy, relevance and correctness. Article 6 therefore does not bring any added value. It may however cause major difficulties in the exchange of information between Member States for a number of reasons put forward in the September meeting. It would probably increase costs and administrative burdens.

Courts need to be neutral and impartial and cannot classify information according to its "accuracy and reliability" other than in the sentence.

Article 7

Lawfulness of processing

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

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

(g) for compliance with a legal obligation to which the controller is subject; or

(h) in order to protect the vital interests of the data subject or of another person; or

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

Comment: The article is too restrictive if the aim is an exhaustive description. The word "necessary" may be to narrow and the words "task /…/ based on law" may be more limiting than "legal obligation".

The meaning of "vital interests" needs clarifying.

Article 8

Processing of special categories of personal data

1. ***~~Member States shall prohibit t~~The*** processing of personal data revealing race or ethnic origin, political opinions, ***~~religion or beliefs~~ religious or philosophical beliefs***, trade-union membership, of genetic data or of data concerning health or sex life ***shall be permitted only when this is strictly necessary and when the national law provides adequate safeguards.***

2. Paragraph 1 shall not apply where:

   (a) the processing is authorised by a law providing appropriate safeguards; or

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

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

Comment: The article shows the problematic consequences of the definitions of "genetic data" and "health" proposed in Article 3(10 and 12): Many of the information types commonly used by the competent authorities in the area of the directive for identification of persons (DNA-profiles, fingerprints, physically distinguishing features such as colour of skin, hair, eyes, scars or limp) may fall within these "special categories" of Article 8.

It goes without saying that there is a strong need for secure identification of persons in the whole area covered by the proposed directive. Therefore, Article 8 should not be expressed as a prohibition. SE prefers to keep the wording of the DPFD ("The processing of personal data /…/ shall be permitted only when this is strictly necessary and when the national law provides adequate safeguards."

In the absence of compelling reasons for change the wording "religious or philosophical beliefs" of Article 6 of the DPFD should be retained.

The meaning of "vital interests" needs clarifying.

SWITZERLAND

Art. 1, para 1:

In the light of the Directive's objective to harmonize the rules on data protection, Switzerland wonders whether it is justified to limit the scope of application to natural persons or whether it would not be more judicious to extend it also to legal persons.

Art. 1, para 2b:

Switzerland is of the opinion that the Member States should have the possibility to foresee more restrictive provisions with regard to the purposes for which data can be used, and which could apply when data are transmitted to the authority of another State Party.

Therefore Switzerland proposes to clarify this aspect in the recitals as follows:
"The transmitting Member State should have the possibility to subject the processing by the receiving Member State to conditions, but he 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".

Furthermore Switzerland proposes to introduce a new paragraph 3 along the lines of art. 1 para. 5 of the framework decision:
"This Directive shall not preclude Member States from providing, for the protection of personal data collected or processed at national level, higher safeguards than those established in this Directive".

Art. 2:

As indicated on the occasion of the CATS meeting of 3 March 2012, since Switzerland is an associated State, the directive can apply to it only insofar as the data processing takes place within the framework of the Schengen cooperation.

Switzerland therefore proposes to complete recital 78 as follows: “(...) insofar as the data processing within the fields covered by the Schengen cooperation is concerned.”

As a matter of fact, the provisions of the Schengen acquis as taken over under the Schengen Association Agreement between Switzerland and the European Union inherently relate to crossborder situations only. As an example, the provisions on police cooperation deal with crossborder police cooperation only. The regulation of national procedures remains in the competence of the Swiss government.

Art. 3:

For the reasons indicated below with regard to art. 7, Switzerland proposes to add in art. 3 with a additional definition according to art. 4(8) of the proposal for a regulation:

'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by
a clear affirmative action, signifies agreement to personal data relating to them being processed”.

Art. 5:

Switzerland has its doubts with regard to the utility and the viability of such a provision in practice. This especially in view of the fact that it is not uncommon that, in the course of a criminal proceeding, a person changes his "role"; he can for instance in a first stage be a witness, later a defendant. Also, a clear classification is not always easy. Even if such a provision would be viable, it threatens to put an excessive burden on the authorities involved, thereby possibly impeding their work.

In the light of these considerations, Switzerland proposes to delete article 5.

Art. 6:

Switzerland has its doubts with regard to the added value of this provision. In its opinion, in particular article 4(d) constitutes a sufficient provision in order to guarantee the accuracy and reliability of the data.

Furthermore we are of the opinion that this provision could encroach on certain rules on criminal proceedings and might also question the competences of courts. Finally such a provision might put an excessive burden on the authorities involved.

Therefore, Switzerland proposes to delete article 6, replacing it by a provision along the line of articles 4 and 8 of the Framework Decision.

Art. 7:

Switzerland stresses that the Directive should not jeopardize criminal proceedings. In certain cases, it is not excluded that data can only be processed with the consent of the data subject (e.g. art. 11(d) of the Framework Decision). It is therefore important to include the consent of the data subject as a possible motive for the lawfulness of processing.

Switzerland proposes to complete article 7 with a new paragraph 2: “The processing of personal data is also lawful if the data subject agrees to personal data relating to him being processed.”

Art. 8, para 2:

Switzerland is of the opinion that the exceptions foreseen in paragraph 2 are not sufficient. As mentioned above, the Directive should not jeopardize criminal proceedings.

Article 8, paragraph 2 should therefore be complemented with a lit. d and e as follows:

“(d) the processing is necessary for the prevention of an immediate and serious threat to public security”; or
(e) the data subject agrees to personal data relating to him being processed.”