COUNCIL OF THE EUROPEAN UNION

Brussels, 10 October 2012

14147/1/12 REV 1

LIMITE

Interinstitutional File: 2012/0011 (COD)

DATAPROTECT 107
JAI 636
MI 574
DRS 108
DAPIX 112
FREMP 116
COMIX 516
CODEC 2211

NOTE

from:	General Secretariat
to:	Working Group on Information Exchange and Data Protection (DAPIX)
No. Cion prop.:	5853/12 DATAPROTECT 9 JAI 44 MI 58 DRS 9 DAPIX 12 FREMP 7 COMIX 61 CODEC 219
Subject:	Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Comments on Articles 11-27

Further to the invitation by the Presidency (CM 3942/1/12 REV 1) delegations have sent in written comments on Chapters III and Articles 22 - 27 of Chapter IV of the proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

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

TABLE OF CONTENTS

BELGIUM

CHAPTER III: RIGHTS OF THE DATA SUBJECT

SECTION 1: TRANSPARENCY AND MODALITIES

Article 12 Procedures and mechanisms for exercising the rights of the data subject

12.2 The controller shall inform the data subject without delay and, at the latest within ~~one~~ two months of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.

BE considers that the period of one month is too short. BE would like to change it to 2 months.

12.4 The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.

For BE, the criteria for assessing whether a request is « *manifestly excessive*» are not clear. BE asks COM to specify those criteria in a recital.

Article 13 Rights in relation to recipients

The controller shall communicate any rectification or erasure carried out in accordance with Articles 16 and 17 to each recipient to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort.

For BE, the notion « disproportionate effort » is not clear. BE asks COM to specify the criteria in a recital.

SECTION 2: INFORMATION AND ACCESS TO DATA

Article 14 Information to the data subject

14.1 Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:

(c) the period for which the personal data will be stored, where known;

BE considers that it is not always possible to determine the retention period of the data.
BE wants to complete point (c) and article 15.1 d) with “where known”.

(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data

This paragraph shall not apply where data are collected for historical, statistical or scientific research purposes and the conditions in Article 83 (1A) are met.

BE supports the exemption request of the Working Party on Statistics. BE requests the creation of a second paragraph in point (d).

(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.

BE considers that the wording of paragraph (h) is too broad. BE asks COM to clarify the scope of this paragraph.

14.3 Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which <u>categories of</u> source the personal data originate.

BE considers that it is impossible to inform the data subject of the entire source and proposes to add the wording "categories of".

During the DAPIX meeting, COM said that article 14.3 is general information while article 15.1 g) is a more detailed information on request of the data subject.
BE asks COM to specify the link between article 14.3 and 15.1 g) in a recital.

14.4 The controller shall provide the information referred to in paragraphs 1, 2 and 3:

(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.

<u>14.4 bis The controller shall provide the information referred to in paragraphs 1, 2 and 3 through a single point of contact easily accessible where the data subject may consult his/her data.</u>

BE proposes the creation of a new paragraph 14.4 bis to allow for a new way to provide information.

<u>Article 15 Right of access for the data subject</u>

15.1 The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information:

(c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries, as long as the data subject has the right of access;

BE proposes to add "*as long as the data subject has the right of access*" in paragraph (c) in order to comply with the case-law of the Court of Justice and more particularly with the case C553/07 (Rijkeboer) which states that « *Rules limiting the storage of information on the recipients or categories of recipient of personal data and on the content of the data disclosed to a period of one year and correspondingly limiting access to that information, while basic data is stored for a much longer period, do not constitute a fair balance of the interest and obligation at issue, unless it can be shown that longer storage of that information would constitute an excessive burden on the controller. It is, however, for national courts to make the determinations necessary.* »

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

See comment on article 14.1 c)

(g) communication of the personal data undergoing processing and of any available information as to their source;

BE notes that paragraphs 15.1 g) and 15.2 are the same. What is the link between the two?

(h) the significance and envisaged consequences of such processing and the knowledge of the reasoning involved in any automatic processing of data concerning him, at least in the case of measures referred to in Article 20.

BE asks to add the wording of article 12, a) indent 3 of Directive 95/46/EC to paragraph (h) with a small modification (underlined): «*knowledge of the reasoning involved in any automatic processing of data concerning him.* »

2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.

5. The rights provided for in Article 15 do not apply when data are processed only for historical, statistical or scientific research purposes and the conditions in Article 83 (1A) are met.

BE supports the exemption request of the Working Party on Statistics. BE requests the creation of a point 5 in article 15.

SECTION 3 : RECTIFICATION AND ERASURE

Article 16 Right to rectification

1. The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement.

BE asks COM to explain the link between the word « rectification » and « completion ».

BE considers that the data subject should have the right to supplement subjective assessments by its own opinion.

2. The rights provided for in Article 16 do not apply when data are processed only for historical, statistical or scientific research purposes and the conditions in Article 83 (1A) are met.

BE supports the exemption request of the Working Party on Statistics. BE requests the creation of a point 2 in article 16.

Article 17 Right to be forgotten and to erasure

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:

(e) the data have to be erased for compliance with a legal obligation.

In BE, some laws require the deletion of the data after a certain period, for example, the case of a minor who has reached the age of majority. BE asks COM to include this possibility by creating a new paragraph (e).

2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.

BE is of the opinion that this section should not apply to the public sector and therefore asks for an exception for the public sector.

BE asks to foresee the practical application of the right to be forgotten:
- to social networks ;
- to search engines.

The question of the repartition of the responsibilities rises in this context, particularly when the data subject has himself put his/her data online.

BE considers that this right should be limited to the on-line environment and not extended to the off-line environment.

What's the meaning of « *has made the personal data public* »?

BE notes that DIR 2000/31 must be taken into account. This point should be put in a recital.

3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:

(a) for exercising the right of freedom of expression in accordance with Article 80;

(b) for reasons of public interest in the area of public health in accordance with Article 81;

(c) for historical, statistical and scientific research purposes in accordance with Article 83;

(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; ~~Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;~~

To be consistent with the modification of article 6.3 (previous comments of the Belgian delegation), BE proposes to delete the end of paragraph (d).

4. Instead of erasure, the controller shall restrict processing of personal data where:

(b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained ~~for purposes of proof~~ for the establishment, exercise or defence of legal claim;

BE proposes to change the words « *for the purpose of proof* » into « *for the establishment, exercise or defence of legal claim* », in articles 17.4 (b) and 17.5.

5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed ~~for purposes of proof~~ for the establishment, exercise or defence of legal claim or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.

See comment above on the 17.4 (b)

Article 18 Right to data portability

1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.

2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data ~~and any other information~~ provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.

BE underlines the difficulties to apply this right to the public sector.
BE considers that this point is problematic regarding intellectual property rights.

BE asks to delete the words « and any other information » and asks COM to explain in a recital that only data provided by the data subject should be given back.
BE wants to be assured that the aggregated data will not be transmitted.

4. The rights provided for in Article 18 do not apply when data are processed only for historical, statistical or scientific research purposes and the conditions in Article 83 (1A) are met.

BE supports the exemption request of the Working Party on Statistics. BE requests the creation of a point 4 in article 18.

SECTION 4: RIGHT TO OBJECT AND PROFILING

Article 19 Right to object

1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), ~~(e)~~ and (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.

BE refuses the application of this section to the public sector and asks COM for an exception for the public sector.

BE proposes to delete the reference to article 6.1 e) which states that: « 6.1 *Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:*
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller".

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object ***free of charge*** *to the processing of their personal data for such marketing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information.*

BE notes that in the FR version, the wording « free of charge » is not translated.

3. Where an objection is upheld pursuant to paragraphs 1 and 2, the controller shall no longer use or otherwise process the personal data concerned, except for the establishment, exercise or defence of a legal claim.

BE proposes to introduce an exception similar to Article 17.4.

The words « use » and « process » have no meaning insofar as the processing contains the use of the data.

4. The rights provided for in Article 19 do not apply when data are processed only for historical, statistical or scientific research purposes and the conditions in Article 83 (1A) are met.

BE supports the exemption request of the Working Party on Statistics. BE requests the creation of a point 4 in article 19.

Article 20 ~~Measures~~ Decision based on profiling

1. Every natural person shall have the right not to be subject to a ~~measure~~ decision which produces or legal effects ~~concerning this natural person or significantly~~ or that gravely and adversely affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person, ~~or to analyse or predict~~ in particular the natural person's performance at work, economic situation~~, location~~, health, ~~personal preferences~~, reliability or behaviour.

BE proposes to change the word “Measures” into “Decision” which is more precise. The words « significantly affects » are problematic for the interpretation. BE proposes to change into “*produces or legal effects or that gravely and adversely affects*”.

2. Subject to the other provisions of this Regulation, a person may be subjected to a ~~measure~~ decision of the kind referred to in paragraph 1 only if the processing:

(a) is linked to and carried out in the course of the entering into, or performance of, a contract between the data subject and the data controller or a third party, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, and as the right to obtain human intervention; or

The aim of all the modifications is to be more precise.

(b) is ~~expressly~~ authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests ; or

(b)bis is carried out for the purpose of the legitimate interests pursued by a data controller as specified in Article 6(1)(f), including for fraud monitoring and prevention purposes and to ensure the security and reliability of a service provided by the controller.

BE raises the question of whether the pre-contractual measures are affected by this paragraph and makes proposals to amend the text to allow the fight against fraud by creating a b (bis).

(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.

In each case referred in paragraph 2, the data subject shall have the right to put his point of view.

BE asks to add a paragraph that allows the data subject to make his point of view.

Those proposals result in changes to 2 recitals:

(39) *The processing of personal data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these net-works and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the concerned data controller. This could, for example, include preventing unauthorized access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems. The processing of personal data to the extent strictly necessary for the purposes of preventing and monitoring fraud also constitutes a legitimate interest of the concerned data controller.*

(58) *Every natural person should have the right not to be subject to a ~~measure~~ decision which is based on profiling by means of automated processing. However, such measure should be allowed when ~~expressly~~ authorised by law, <u>when linked to and</u> carried out in the course of entering or performance of a contract <u>between the data subject and the data controller or a third party</u>, or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child.*

3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.

BE: Quid for the insurance companies and for the anti-doping control?

SECTION 5: RESTRICTIONS

<u>Article 21 Restrictions</u>

1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in ~~points (a) to (e) of Article 5~~ ~~and~~ Articles 11 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:

BE considers that restrictions cannot focus on the basis of the data protection principles of article 5. BE wants to delete the words « *points (a) to (e) of article 5 and* ».

(a) public security;

(b) the prevention, investigation, detection and prosecution of criminal offences;

(c) other public interests of the Union or of a Member State, in particular an important economic or financial interest <u>or an important health interest</u> of the Union or of a Member State, including monetary, budgetary and taxation matters and the protection of market stability and integrity;

BE notes that the translation in FR is not consistent with the EN version, particularly for the words: « public interest ».

BE asks to take into account the health area in paragraph (c).

CHAPTER IV: CONTROLLER AND PROCESSOR

BE has 2 general remarks:

1. BE recalls the need to reduce administrative burden. BE has a scrutiny reservation on Chapter IV to enable her to evaluate the impact of the different provisions of this chapter on business enterprises.

2. BE considers that in the era of « Web 2.0 »:
- the notion of controller and processor are no longer adequate, particularly in the cloud computing ;
- the notion of controller may cover a private person who adds content

This means that all obligations relating to the data controller should theoretically apply (in absence of the domestic exemption), which is in practice not feasible. BE considers that exceptions should be created when a controller is a private person.
- the situation is much more complicated when the private person is also a data subject.

BE wants COM to rethink the concepts (and maybe find new concepts) of data controller, processor and data subject in the light of the Internet reality and all the services linked to internet.

SECTION 1: GENERAL OBLIGATIONS

Article 22 Responsibility of the controller

BE considers that, in this section, the administrative burden is not reduced.

1. The controller shall adopt policies and implement appropriate measures to ~~ensure and~~ be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.

BE considers that this provision introduces an absolute obligation instead of an obligation of means. BE proposes to turn "*who shall ensure and demonstrate*" into "*who shall be able to demonstrate*". This is consistent with the changes already made in article 5 (f) of the present Regulation. *5 (f) processed under the responsibility and liability of the controller, who shall be able to ~~ensure and~~ demonstrate for each processing operation the compliance with the provisions of this Regulation.*

~~3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.~~

BE considers that this paragraph is not clear. There is a lack of predictability. BE asks COM to delete this paragraph.

Article 23 Data protection by design and by default

1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

BE: How to complete the upgrade of existing systems?

2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals. The data subject should have the choice to authorize the use of his own data.

For BE, the wording paragraph 2 of article 23 is almost the same as article 5. Why?

BE considers that the position of the data subject should be added in paragraph 2 and in recital 61.

Article 24 Joint controllers

Where a controller determines the purposes ~~conditions and means~~ of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them. The arrangement shall duly reflect the joint controllers' respective effective roles vis-à-vis data subjects. The arrangement shall designate the supervisory authority in accordance with Article 51[…].The arrangement shall designate which of the joint controllers shall act as single point of contact for data subjects to exercise their rights.

BE proposes to change articles 24 and 77 to better reflect the economic reality:

"*Art. 24 Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities* ***vis-à-vis data subjects*** *for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.* ***The arrangement shall duly reflect the joint controllers' respective effective roles vis-à-vis data subjects. The arrangement shall designate the supervisory authority in accordance with Article 51[…]. The arrangement shall designate which of the joint controllers shall act as single point of contact for data subjects to exercise their rights****.*

Art. 77(2) Where more than one controller or processor is involved in the processing ***is under a joint controllership****, each* ***joint*** *controller or processor shall be jointly and severally liable for the entire amount of the damage* ***in accordance with the joint controllers' respective responsibilities as set out in the legal arrangement referred to in Article 24.***

Article 25 Representatives of controllers not established in the Union

1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.

BE considers that the entire article is not clear. Indeed, we have no indication on the way of designation, the mission, the responsibilities, the information of the data subject …
This article 25 should be rewritten.

2. This obligation shall not apply to:

(a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or

It is not clear for BE to know if the criteria of the recognition of an adequate level of protection is suitable to justify the designation of a representative in the Union. BE fears that the data subjects cannot exercise their rights easily.

BE thinks that a solution could be to foresee a collaboration between EU DPAs and DPAs of third countries (which ensures an adequate level of protection) in order to facilitate the exercise of the rights by the data subjects.

(b) an enterprise employing fewer than 250 persons; or

For BE the distinction should not only be based on the number of the employees but on the quantity and the quality of the data processed.
This remark applies to all the provisions of the Regulation which make a reference to the number of persons/employees.

Article 26 Processor

1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.

2. The carrying out of processing by a processor shall be governed by a contract, by law or other legal act binding the processor to the controller and stipulating in particular that the processor shall:

BE asks to add "by law" in paragraph 2 in order to cover practices in the public sector.

(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited unless required to do so by Union or Member State law;

See explanation for article 27.

4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.

BE considers that § 4 is not adequate. There is no reason to make the original data controller jointly liable with the processor which processed the data other than as instructed by the controller.

~~Article 27 Processing under the authority of the controller and processor~~

~~The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.~~

In order to avoid confusion, BE wants to put the end of this article ("*unless required to do so by Union or Member State law)* in article 26.2.a. The consequence is that article 27 is deleted.

Article 28 Documentation

1. Each controller ~~and processor~~ and, if any, the controller's representative, shall maintain documentation of ~~all~~ the categories of processing ~~operations~~ under its responsibility.

Lors de la consultation publique, Mastercard a expliqué qu'il n'est pas possible de maintenir une documentation de tous les traitements. Cela imposerait une charge administrative trop importante et participa à la confusion des rôles entre responsable du traitement et sous-traitant.

BE considers that article 28 imposes an excessive administrative burden for businesses and creates confusion between the role of the controller and the processor.
BE proposes some modifications to reduce this burden.

BULGARIA

In connection with the invitation provided by the Presidency for written comments on Chapter III and Chapter IV of the Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, please find below the comments of the Bulgarian delegation to DAPIX, represented by the Commission for Personal Data Protection.

We hope that our comments will be taken under consideration in the context of the ongoing discussions on the proposed General Data Protection Regulation.

1. We assess positively the proposed mechanisms for strengthening individuals' rights and support the opinion of the European Commission in connection with the reducing of the data controllers' administrative burden as well.

2. With regard to article 16 of the Proposal which regulates the supplementation of incorrect personal data, we share the common position that this article gives the opportunity for extending interpretation on the amount of the processed personal data. In this connection, we consider that it is necessary additionally to be improved the texts on the data subject access to, correction and erasure of his/her personal data.

3. We consider it appropriate to simplify the procedure for informing the individuals and to additionally discuss the practice of informing third parties in accordance with article 17, paragraph II.

4. We express our general support about the introduction of the right to be forgotten, the right to erasure and the right to data portability following the information society development. In connection with this we propose additional specifying and assessment of the risk of their practical application.

5. We express our reservations on the application of the "right of data portability" which can harm specific data controller's interests because he has invested both financial and intellectual resources while structuring the data, used by him/her.

6. We consider it necessary to clarify the texts in the regulation proposal, regarding the data controller's obligation to undertake technical and organizational data protection measures. ("All reasonable measures" are mentioned in article 17, paragraph II ; but other articles in the Regulation refer to "all reasonable measures including technical", "appropriate measures", "technical and organizational measures", etc.).

7. We express our general support about the compulsory appointing of a data protection officer depending on the number of the personnel (250 employees), which supports the European Commission's idea to relieve the small and medium-size enterprises. We propose the supplement the rule by appointing data protection officer when the personal data of a minimum of 250 individuals are processed. It should be considered that companies with less than 250 employees could process personal data of thousands of individuals.

8. We support the idea for the introduction of delegated acts as an opportunity for the European Commission to express opinion on certain aspects of the Regulation, with the specification that the basic data protection principles and mechanisms, individuals' rights and the data controllers' obligations should be written only in the Regulation. We consider that the adoption of delegated acts should be reduced.

9. In connection with article 29 of the Regulation on the cooperation between the data controller and the data processor and the supervisory authority, we consider that it is necessary to clarify the text with regard to its practical application, including the "reasonable time limits".

10. Article 38 of the Regulation foresees that the supervisory authority can only issue opinions. We think that the scope of the article can be expanded including the right of the supervisory authority to give compulsory instructions and guidelines on the Codes of conduct.

CZECH REPUBLIC

CZ focuses on Articles only, as the recitals would have to be adapted later.

In general

CZ wishes to point out that comments given below are without prejudice to horizontal questions and issues, such as delegated and implementing acts or legal form of the proposal. Given the fact that these horizontal issues are being discussed separately, CZ did not specifically comment e.g. on provisions establishing implementing or delegated powers.

Article 11

- The first paragraph should be deleted or redrafted in much more restricted way.

The first paragraph contains specific general duty to have accessible policies without regard to the nature of controller and to ways in which controller interacts with data subjects. (Not every controller has web pages or internet presence at all. For such controllers this represents disproportionate administrative burden.) CZ believes that in appropriate circumstances, it is in the interest of controllers to proactively inform data subjects on data processing (e.g. large IT companies, social networks etc.) to improve customer trust and address competitive concerns. Therefore, establishment of a legal duty to do so is superfluous, Article 14 is fully sufficient.

Article 12

- The last sentence in paragraph 2 should be redrafted to allow controller and data subject to agree on the form of response. Electronic form should not be forced upon them (even with possible opt-out for data subject).

There is no reason to force controller to use electronic communication in cases when other forms of communication may be much safer and more appropriate with regard to categories of personal data processed. It is better to leave the form of response more flexible.

- The paragraph 4 should be redrafted to include few simple rules for dealing with requests. Such rules could include: one request per time period is free, third request per time period need not be answered etc.

The regulation of requests is unreasonably complicated. The controllers cannot use small fees to filter out abusive requests. There is no time period in which the repeated request could be deemed repetitive. They face the burden of proving that request is not only excessive, but manifestly excessive if they take no action. It is not clear whether this burden applies also when a fee is charged. All this translates into costs for everyone involved.

Article 14

- Paragraph 1 should enumerate definite amount of information. The words "at least" should be deleted in the chapeau. The open-ended paragraph 1(h) should be deleted as well.

It follows from the requirement to clearly explain duties subject to enforcement by sanctions.

- In paragraph 1(a) the words "and of the data protection officer" should be deleted.

Not necessary.

- In paragraph 1(b) the words "contract terms and general conditions" should be deleted.

The data subject may of course be informed just about everything upon his/her request, but overwhelming data subject with long obligatory descriptions would just decrease his/her willingness and readiness to familiarize him/herself with at least the most important information.

- Paragraph 1(c) should be redrafted to clearly indicate that it concerns the intended or envisaged period of storage. The controller should be able to express this period in relation to the purposes of processing (e.g. "up to two years after life insurance has been paid in full"). Less preferably, recital 48 should clarify this.

Because in some cases the insistence on numbers would cause only formal compliance or cause controllers to estimate too long time periods just to be on the safe side.

- In paragraph 5 the letters (c) and (d) should apply also when data are collected from the data subject. The words "the data are not collected from the data subject and" should be deleted in both cases.

Exempting such cases does not appear to be justified.

Article 15

- Right of access to personal data undergoing processing should be clearly established. Paragraph 1(b) and paragraph 2 should be deleted.

It is enough to require the access to personal data once, according to paragraph 1(g). Access to categories of personal data is superfluous. Requirement of paragraph 2 to provide data in electronic form is superfluous. Controllers should be able to choose appropriate and secure form of communication with regard to sensitivity of personal data concerned.

- Paragraph 1(d) should be redrafted to clearly indicate that it concerns the intended or envisaged period of storage. The controller should be able to express this period in relation to the purposes of processing (e.g. "up to two years after life insurance has been paid in full"). Less preferably, recital 51 should clarify this.

Because in some cases the insistence on numbers would cause only formal compliance or cause controllers to estimate too long time periods just to be on the safe side.

- Paragraph 1(h) should refer only to existence or purpose of profiling pursuant to Article 20.

The "significance and envisaged consequences" are too vague and uncertain categories.

- The forms in paragraph 4 should be used only voluntarily. The words "for voluntary use" should be added after the words "standard forms" in the first line.

There is no reason to create artificial administrative burdens by making lots of obligatory forms. Rules requiring clarity, simplicity and transparency still apply pursuant to Article 11(2).

Article 17

- This Article is based on right to erasure, but is phrased more generally. Its implications and relation to other rights must be considered further. Also, the reasoning how this Article is intended to apply should be elaborated upon with respect to basic situations (published or unpublished data, on-line or off-line or hard copy data etc.).

- In paragraph 1, the reference to child should be moved from the chapeau of Article to an appropriate recital, or it should be phrased as a clear example ("such as"), not as a preferred reason to be forgotten.

Normative text should be clear rather than cuddly. Saying that something applies "especially" in some cases in effect might cause uncertainty with regard to other requests which may be motivated by arguably weaker situations, puts in doubt burden of proof, appropriate sanctions etc. CZ believes that right to be forgotten should have the same force for everyone subject to conditions in (a)-(d).

- Paragraph 1(d) should be more restricted.

Insignificant cases of non-compliance should not give rise to erasure of data – e.g. when policies according to Article 11 are not accessible enough, or where small-scale data breach has occurred.

- Paragraphs 2 and 3 should be subject to the same exceptions given in paragraph 3(a)-(e).

- Paragraph 3(d) should be deleted after the word "subject".

CZ objects to quasi-constitutional requirements of public interest, proportionality etc. This is not for mere Regulation to provide for. Domestic law is subject to review by constitutional courts in these and other regards.

Article 19

- Relationship of paragraph (1) to Article 6(1)(e) should be clarified; CZ prefers the omission of the reference to Article 6(1)(e) from the first paragraph.

Since the Article 6(1)(e) establishes lawfulness of the processing due to public interests, burden of proving compelling legitimate grounds overriding "the interests" of the data subject should not be shifted to controller.

- Paragraph 3 should be redrafted to prohibit just the processing that has been objected to (possibly including similar processing based on the same point of Article 6(1)).

The controller may have another valid titles for processing (e.g. according to Article 6(1)(a)). Therefore, the controller should not be forced to "no longer use or otherwise process" data concerned, but to cease and desist from the operations (processing) that has been objected to by the data subject, and from similar processing, if necessary. This is also in the interests of data subject, who would otherwise be rendered unable to object to some feature of processing that is otherwise beneficial to him.

Article 20

- In paragraph 2(b) the word "expressly" should be deleted.

This is purely formal requirement that just increases administrative burden for legislator and for all addressees of the law in question. It is completely unnecessary even for data subject, as he or she will obtain the information about such measures pursuant to paragraph (4).

- Power to adopt delegated acts in paragraph 5 should be limited to cases referred to in paragraph 2(a).

Cases falling under paragraph 2(b) should be left to EU or national law in question. Cases falling under paragraph 2(c) are based on the data subject's consent and should not be further regulated.

Article 21

- In the chapeau of the paragraph (1), the words "and proportionate" and "in a democratic society" should be deleted.

The Regulation should not provide for quasi-constitutional requirements, the word "necessary" is all that is needed in this regard.

- Within the categories (a) to (f), the reference to "national security" and to "defence" should be added.

Article 13 of the 1995 Directive expressly covers "national security" and "defence". Omitting those terms here would make matter uncertain as those exemptions might or might not be covered by "other public interests" pursuant to paragraph 1(c). As the Regulation is already three times longer than Directive, it surely does not harm to be little bit more explicit here.

Article 22

- Paragraph 1 is too vague and its added value is not clear in comparison to Article 5(f) and to other duties in this Chapter. It should be reconsidered.

Is a natural person posting on social network required to have policies to this effect?

- Paragraph 3 is excessive administrative burden and should be deleted.

Controllers should focus on the substance of their obligations rather than be burdened with ever more procedural and formal requirements.

Article 24

- CZ believes that this Article should contain a safeguard to prevent "outsourcing of responsibility".

CZ does not share optimistic expectations as regards the enforcement of this Regulation outside of the EU. Therefore, motivating factors (not much different from country-specific differences in administrative burden and costs) may cause the responsibility (and liability) to be lead outside of the EU. CZ believes that a safeguard is advisable. For example, data protection authorities should be able to disregard clearly abusive arrangements that significantly diminish the availability or exercise of rights for data subject.

Article 25

- CZ believes that this Article should be reconsidered in relation to reconsideration of Article 3(2).

CZ considers Article 4(1) of 1995 Directive to be a better solution. The Regulation does not offer any real or practical instruments to enforce rules outside the EU. In particular, it is not clear how the Member States (who will be responsible for it) are to enforce the obligation to designate a representative against a controller that is offering services remotely (electronically) and that has no property or other interests within EU that could be subject to enforcement measures. Formal solutions such as this Article just reinforce the expectations of level playing field based on unrealistic views of EU's ability to apply its data protection rules effectively across the globe. In fact, administrative costs are bound to increase most for European controllers and processors and therefore should be checked within whole Regulation.

Article 26

- The whole Article should be deleted.

CZ finds it quite problematic to make distinctions between controller and processor.

- In paragraph 3 the documentation should be allowed in electronic form as well.

CZ believes that in some cases the instructions of controller may be made ad hoc in electronic form e.g. as a part of the process of transmitting the personal data. This should be allowed, as it does not decrease the requirements on controller and processor to demonstrate compliance.

GERMANY

Mit Schreiben vom 5. September 2012 lädt die Präsidentschaft die Mitgliedstaaten ein, vor dem 20. September 2012 Änderungsvorschläge und Anmerkungen, unabhängig von den in der Ratsarbeitsgruppe DAPIX bereits gemachten, zu Kapitel III und Artikel 22 bis 27 von Kapitel IV des Vorschlags der Kommission für eine Datenschutz-Grundverordnung zu übermitteln.

A. Vorbemerkung

Deutschland dankt der Präsidentschaft für die Gelegenheit zur Stellungnahme. Wie in der Vorbemerkung zur Stellungnahme vom 9. Mai 2012 ausgeführt, hat Deutschland zu dem Rechtsakt allgemeine Fragen, die noch einer vertieften Erörterung bedürfen. Wie andere Mitgliedstaaten spricht sich auch Deutschland vor dem Hintergrund der bisherigen Erörterungen in der Ratsarbeitsgruppe DAPIX weiterhin dafür aus, dass der Regelungsvorschlag möglichst klar zwischen der Datenverarbeitung im öffentlichen und privaten Bereich sowie stärker zwischen risikoarmen und risikoreichen Datenverarbeitungen differenziert und darüber hinaus einen angemessenen Ausgleich zwischen den Schutzinteressen der Betroffenen und dem bürokratischen Aufwand herstellt. Die hier vorgelegten Vorschläge sind nur als vorläufige und nicht abschließende Beiträge zur weiteren Erörterung des Rechtsaktes anzusehen. Deutschland behält sich weiteren Vortrag, auch zu grundsätzlichen, artikelübergreifenden Themen ausdrücklich vor. Redaktionelle Hinweise und Anmerkungen zur deutschen Sprachfassung werden zu einem späteren Zeitpunkt erfolgen. Zu den Erwägungsgründen wird gesondert Stellung genommen. Die weiteren von Deutschland in der Ratsarbeitsgruppe DAPIX vorgetragenen Anmerkungen werden vorsorglich auch zum Gegenstand der Stellungnahme gemacht und im Folgenden zum Teil erneut aufgeführt.

B. Anmerkungen zu den Artikeln 11 bis 27

I.

Allgemeine Prüfvorbehalte sowie Vorbehalte zu einzelnen Regelungen, wie sie in der Ratsarbeitsgruppe DAPIX und in der Stellungnahme zu den Artikeln 1 – 10 vorgetragen worden sind, bleiben bestehen.

II.

Kapitel III enthält entgegen seinem Titel nicht nur Rechte der betroffenen Person, sondern auch Pflichten des für die Verarbeitung Verantwortlichen, siehe etwa Artikel 11, 12, 13. Titel und Aufbau des Kapitels sollten auch mit Blick auf Kapitel IV überprüft werden.

1. zu Artikel 11:

Artikel 11 zur Transparenz sollte präzisiert werden. Deutschland ist wie eine Reihe anderer Mitgliedstaaten in der DAPIX besorgt über die mit der sehr allgemein gehaltenen Formulierung („Strategie“) in Artikel 11 gegebenenfalls verbundenen Bürokratiekosten und die fehlende risikobasierte Differenzierung. Deutschland hätte sich eine belastbare Berechnung der Bürokratiekosten seitens der Kommission gewünscht. Es sollte geprüft werden, ob für bestimmte, näher zu definierende Bereiche, Ausnahmen vorgesehen werden können. Aus Sicht von Deutschland bedürfen die Pflichten des für die Verarbeitung Verantwortlichen, u.a. die in Artikel 12 vorgesehenen, in den Fällen der Erörterung, in denen eine natürliche Person für die Verarbeitung Verantwortlicher ist, z.B. in den Fällen des Artikel 2 Absatz 2 Buchstabe d oder im Gesundheitsbereich bei elektronischen Patientenakten.

- Absatz 1 enthält gegenüber Absatz 2 und Artikel 12 keinen erkennbaren Mehrwert und könnte daher gestrichen werden.

- Absatz 2 sollte mit den Pflichten des für die Verarbeitung Verantwortlichen bei der Rechteausübung der betroffenen Person in Artikel 12 zusammengeführt werden. Es sollte klargestellt werden, wann mit dem „zur Verfügung stellen“ von Informationen und Mitteilungen eine Bringschuld des für die Verarbeitung Verantwortlichen und wann eine Holschuld der betroffenen Person verbunden ist.

- Deutschland unterstützt, wie mehrere andere Mitgliedstaaten in der DAPIX eine Information „*in verständlicher Form unter Verwendung einer klaren, einfachen und altersgerechten Sprache*“.

2. zu Artikel 12:

- Absatz 1 Satz 2 sollte gestrichen werden. Der Begriff „erleichtern“ ist unbestimmt und das erforderlich Maß an „Erleichterung“ streitanfällig.

- Absatz 1 Satz 3 sollte auf die Fälle begrenzt werden, in denen der für die Verarbeitung Verantwortliche elektronisch kommuniziert. Eine automatisierte Verarbeitung personenbezogener Daten (z.B. an einem PC) bietet noch keine Gewähr, dass auch eine elektronische Kommunikation (z.B. eine E-Mail-Adresse) besteht.

- Absatz 2 Satz 1 ist in der deutschen Sprachfassung in mehfacher Hinsicht unklar und sollte dahin formuliert werden, dass der für die Verarbeitung Verantwortliche seinen Pflichten und den Rechten der betroffenen Person nach Kapitel III unverzüglich, d.h. ohne schuldhaftes Verzögern, nachkommt.

– Absatz 2 Satz 2 sollte an Satz 1 anschließen („Dabei …“) und Fälle benennen, die - abhängig von den Möglichkeiten des für die Verarbeitung Verantwortlichen - eine längere Bearbeitungsdauer rechtfertigen können, z.B. unter bestimmten Voraussetzungen die Häufung von Anträgen bei kleineren und mittleren Unternehmen oder bei komplexen Sachverhalten.

– Absatz 2 Satz 3 sollte dahin formuliert werden, dass der für die Verarbeitung Verantwortliche die betroffene Person auf Verlangen schriftlich unterrichtet, dass er seinen Pflichten nach Satz 1 nachgekommen ist.

– Absatz 2 Satz 4 sollte dahin formuliert werden, dass die Unterrichtung in elektronischer Form erfolgen soll, wenn die betroffene Person es wünscht und das erforderliche Schutzniveau zur elektronischen Übermittlung von personenbezogenen Daten einschließlich einer zuverlässigen Authentifizierung des Empfängers eingehalten wird (vergleiche Erwägungsgrund 52).

– In Absatz 4 Satz 1 sollte die Unentgeltlichkeit der Pflichten des für die Verarbeitung Verantwortlichen und der Rechte der betroffenen Person in Kapitel III durch Bezugnahme auf die konkreten Artikel oder das Kapitel erfolgen, nicht durch Verweis auf Artikel 12 Absatz 1. Für Auskünfte nach Artikel 15, die die betroffene Person gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann, sollte aufgenommen werden, dass einmal je Kalenderjahr eine unentgeltliche Auskunft in Textform und für jede weitere Auskunft ein angemessenes, nicht prohibitives Entgelt verlangt werden kann. Ein Entgelt darf nicht verlangt werden, wenn eine Unrichtigkeit oder Unzulässigkeit der Daten zu vermuten ist oder die Auskunft dies ergibt. Die betroffene Person muss die Möglichkeit haben, sich unentgeltlich persönlich Kenntnis zu verschaffen.

– Im Falle offenkundig unverhältnismäßiger Anträge nach Absatz 4 Satz 2 sollte durch die Streichung der Worte „ein Entgelt für die Unterrichtung oder“ lediglich vorgesehen werden, dass die beantragte Maßnahme unterbleiben kann. Eine Regelung zu Entgelten erscheint unangemessen und insbesondere zwischen nicht-öffentlichen Stellen sehr streitanfällig. Zur „Häufung“ von Anträgen sollte klargestellt werden, dass es um Anträge einer Person geht. Eine Vielzahl von Anträgen an sich muss nicht offenkundig unverhältnismäßig sein, sondern ist gegebenenfalls nur Folge der Unternehmensgröße oder des Umfangs der Datenverarbeitung.

– Die Beweislastregelung in Absatz 4 Satz 3 kann nach deutschem Rechtsverständnis gestrichen werden. Grundsätzlich hat jede Seite die für sie günstigen Umstände zu beweisen, vorliegend also der für die Verarbeitung Verantwortliche den offenkundig unverhältnismäßigen Charakter eines Antrags, weswegen er von der beantragten Maßnahme absehen will.

– Die Ermächtigung der Kommission in Absatz 5 ist zu streichen. Die Kommission würde durch die Bestimmung, wann ein Betroffenenrecht offenkundig unverhältnismäßig ausgeübt wird, weitreichend in die Rechte der Betroffenen eingreifen. Es handelt sich zudem um eine eng umgrenzte Thematik, so dass eine Regelung in der Verordnung erfolgen und ansonsten der Aufsichts- und Gerichtspraxis überlassen bleiben sollte.

– Die Ermächtigung der Kommission in Absatz 6 ist zu streichen, da sie den laufenden Beratungen des Entwurfs einer Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt vorgreift. Die Festlegung von Standardvorlagen und -verfahren für Mitteilungen in elektronischer Form greift sehr weitreichend in technische Standardisierungen auch im öffentlichen Bereich ein (z.B. gibt es in Deutschland mit De-Mail einen besonders gesicherten E-Mail-Verkehr mit Behörden). Maßnahmen, die auch KMU zu Gute kommen, sollten unmittelbar in der Verordnung geregelt werden und nicht einer künftigen, ungewissen Regelung überlassen bleiben.

3. zu Artikel 13:

– Eine Nachberichtspflicht gegenüber den Empfängern von Daten ist grundsätzlich zu begrüßen.

– Artikel 13 enthält keine Rechte gegenüber Empfängern. Die Überschrift sollte in „Benachrichtigungspflicht bei Berichtigungen und Löschungen“ geändert werden.

– Es sollte klargestellt werden, dass die Benachrichtigungspflicht nicht bei der Weitergabe innerhalb des für die Verarbeitung Verantwortlichen besteht.

– Die Benachrichtigungspflicht sollte - vorbehaltlich der weiteren Erörterung - auch die Mitteilung von Widersprüchen nach Artikel 19 Absatz 3 umfassen, sofern der Widerspruch zur Unzulässigkeit der weiteren Verarbeitung führt.

– Die Benachrichtigungspflicht sollte zusätzlich nur dann bestehen, wenn schutzwürdige Interessen des Betroffenen nicht entgegenstehen, z.B. also nicht, wenn der Empfänger erstmals Kenntnis von negativen Daten über die betroffene Person erhielte, an denen er kein berechtigtes Interesse hat. Entsprechende Beispiele sollten in einem Erwägungsgrund erläutert werden.

4. zu Artikel 14:

Wie andere Mitgliedstaaten in der DAPIX ist auch Deutschland der Auffassung, dass Artikel 14 insgesamt zu viele Informationen vorsieht.

Es fehlt in Artikel 14 eine risikobasierte Differenzierung. Artikel 14 legt – insoweit weniger flexibel als Artikel 10 und 11 der Richtlinie 95/46/EG – stets die Notwendigkeit einer Information zugrunde. Dies wird der Realität nicht gerecht, wie die in der DAPIX genannten Fälle der „Bäckerei um die Ecke“ und der telefonischen Reservierung eines Tisches im Restaurant gezeigt haben. Hier sollte geprüft werden, wie Ausnahmefälle definiert werden können, in denen die in Artikel 14 geregelte aktive Informationspflicht nicht besteht. Eine solche Ausnahme könnte nicht nur Bürokratiekosten gerade für kleine Betriebe vermeiden. Primäres Ziel der Informationen sollte es sein, dass der Nutzer die Folgen der Datenverarbeitung abschätzen kann.

Es sollte klarer zum Ausdruck gebracht werden, dass die Information der betroffenen Person nach Artikel 14 eine Bringschuld des für die Verarbeitung Verantwortlichen ist. Dabei sollte Artikel 14 allerdings zwischen Basisinformationen, die eine Einschätzung der Datenverarbeitung erlauben, z.B. wie in Artikel 10 und 11 der Richtlinie 95/46/EG die Informationen nach Absatz 1 Buchstabe a und b, und weiterführenden Datenschutzinformationen unterscheiden. Die Basisinformationen sollten dem Betroffenen in geeigneter Weise direkt zur Verfügung gestellt werden, z.B. durch ein Pop-Up Fenster, am Telefon oder auf einer Postkarte, für weiterführende Datenschutzinformationen sollte der Betroffene auf einen leicht zugänglichen Ort verwiesen werden können, z.B. über eine Verlinkung oder durch Benennung einer Webseite. Dies trägt den unterschiedlichen Verarbeitungssituationen und praktischen Gegebenheiten Rechnung, z.B. im Fall einer Videoüberwachung oder telefonischen Ansprache, einem Bestellschein oder der Displaygröße eines Mobilfunkgerätes. Zu berücksichtigen ist, dass es sich bei der Information nach Artikel 14 regelmäßig nur um standardisierte und nicht individualisierte Informationen handeln kann, da Aufwand und Komplexität sonst zu sehr erhöht würden.

– Absatz 1 Buchstabe a: Die Worte „und des Datenschutzbeauftragten“ sind zu streichen. Die Angaben sind bereits nach Artikel 35 Absatz 9 zu veröffentlichen. Dort sollte zudem geprüft werden, ob eine namentliche Individualisierung tatsächlich notwendig ist oder ob die Angabe der Kontaktdaten ausreichend ist.

– In Absatz 1 Buchstabe b sollte auf die verpflichtende Angabe zu Geschäfts- und allgemeinen Vertragsbedingungen verzichtet werden, jedenfalls soweit diese nicht datenschutzrelevant sind und ihre Einbeziehung anderen (zivilrechtlichen) Vorgaben unterliegt. Zudem sind diese Informationen in aller Regel so lang, dass verschiedene Informationsformen und Wege ausgeschlossen wären bzw. die Information eine Länge erreichte, die vom Betroffenen nicht mehr wahrgenommen oder als reine Förmelei betrachtet wird. Die Angabe des „verfolgten berechtigten Interesses“ sollte gestrichen werden, da sie neben dem Verarbeitungszweck keinen praktischen Informationsmehrwert erzeugt und die Information unnötig verlängert.

– Zu Absatz 1 Buchstabe c haben eine Reihe von Staaten sich in der DAPIX für die Ergänzung der Worte „soweit bekannt“ ausgesprochen. Deutschland stimmt dem zu.

– Bei Absatz 1 Buchstabe d sollte der Begriff „or“ (englisch), in der deutschen Sprachfassung „beziehungsweise“, durch ein „and“ („und“) ersetzt werden, da er fälschlich suggeriert, das Widerspruchsrecht sei eine Alternative zu den übrigen Betroffenenrechten.

– Der Hinweis nach Absatz 1 Buchstabe e zum „Bestehen eines Beschwerderechts bei der Aufsichtsbehörde“ sollte dahin formuliert werden, dass der Betroffene sich entsprechend Artikel 73 Absatz 1 an jede Aufsichtsbehörde wenden kann. Die weitergehende Information über die Kontaktdaten der jeweils zuständigen Aufsichtsbehörde sollte gestrichen werden.

– Die Information nach Absatz 1 Buchstabe f sollte um die Worte „soweit der Betroffene nach den Umständen des Einzelfalls nicht mit der Übermittlung an diese rechnen muss“ ergänzt werden.

– In Absatz 1 Buchstabe g sollte redaktionell klargestellt werden, dass es um die Übermittlung von Daten an einen Empfänger in einem Drittland geht. Der zweite Satzteil ab dem Wort „sowie“ zum geltenden Datenschutzniveau im Drittland bedarf der weiteren Prüfung. Eine derartige Information kann von einem für die Verarbeitung Verantwortlichen nicht immer geleistet werden.

– Absatz 1 Buchstabe h sollte gestrichen werden. Die Vorschrift ist für eine unmittelbar anwendbare Verordnung zu unbestimmt.

– Über die Folgen der Verweigerung der Daten sollte bei Absatz 2 - vergleichbar Artikel 10 Buchstabe c der Richtlinie 95/46/EG - nur informiert werden, soweit dies nach den Umständen des Einzelfalles erforderlich ist oder der Betroffene dies verlangt. Im Privatrechtsverkehr ist die Information entbehrlich, weil die Folgen in aller Regel selbstverständlich sind, z.B. ein Vertrag kommt nicht zustande oder eine Belieferung ist nicht möglich.

– Die Information sollte nach Absatz 4 Buchstabe b „zum Zeitpunkt der Erhebung der personenbezogenen Daten oder unverzüglich nach der Erhebung“ erfolgen. Es bedarf einer Beschränkung der Information auf die *erstmalige* Verarbeitung. Andernfalls müsste z.B. bei einer Auskunftei die betroffene Person bei jeder Einmeldung und Beauskunftung erneut benachrichtigt werden. Zum Begriff des „Empfängers“ ist klarzustellen, dass Empfänger innerhalb der verantwortlichen Stelle nicht eingeschlossen sind (vergleiche Anmerkung zu Artikel 4).

– Bei Absatz 5 Buchstabe a sollte klargestellt werden, dass die Regelung bereits für die *jeweilige* Information zur Anwendung kommt und nicht nur dann, wenn der Betroffene über alle Informationen verfügt.

– In Absatz 5 Buchstabe b bis d sind die Worte „die Daten werden nicht bei der betroffenen Person erhoben und“ zu streichen. Die Ausnahmen greifen auch bei einer Erhebung beim Betroffenen.

– Es sollte klargestellt werden, dass Absatz 5 Buchstabe b greift, wenn die betroffene Person aufgrund der Verwendung eines Pseudonyms nicht bestimmbar ist („unmöglich“).

– Absatz 5 Buchstabe d sollte - entsprechend Artikel 13 der Richtlinie 95/46/EG - nicht auf Buchstabe f (die Rechte und Freiheiten anderer Personen) des Artikel 21 Absatz 1 beschränkt sein, da insbesondere im öffentlichen Bereich auch die öffentliche Sicherheit entgegenstehen kann.

– In einem Absatz 5 Buchstabe e-neu sollte die Pflicht zur Benachrichtigung ausgeschlossen werden, wenn die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen eines überwiegenden berechtigten Interesses eines Dritten, geheim gehalten werden müssen.

– Absatz 6 ist zu unbestimmt für eine unmittelbar anwendbare Verordnung.

– Zu Absatz 7 und 8 besteht ein Vorbehalt. Die der Kommission eingeräumte Ermächtigung ist sehr weitgehend, z.B. mit Blick auf die Ausgestaltung des Absatz 1 Buchstabe h für verschiedene Bereiche und Verarbeitungssituationen, aber auch umgekehrt mit Blick auf die Ausnahmen von der Information nach Absatz 5. Die Ermächtigung der Kommission in Absatz 8 ist zu streichen, da sie den laufenden Beratungen des Entwurfs einer Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt vorgreift. Die Bemerkungen zu Art. 12 Abs. 6 gelten hier analog.

5. zu Artikel 15:

– Das Auskunftsrecht sollte in Absatz 1 „jederzeit“, jedoch „vorbehaltlich Artikel 12 Absatz 4 Satz 2“ verlangt werden können. Es sollte eine Regelung zur Mitwirkung des Betroffenen vorgesehen werden, die Auskunft zu ermöglichen, z.B. durch Angaben zu einer Vertragsbeziehung oder zu einem Kontakt mit der öffentlichen Stelle.

– In Absatz 1 Buchstabe c sollte das Wort „müssen“ gestrichen werden.

– In Absatz 1 Buchstabe d sollten die Worte „soweit bekannt“ ergänzt werden. Es kann vorkommen, dass die konkrete Dauer der Speicherung zum Zeitpunkt der Auskunft nicht oder noch nicht angegeben werden kann.

– Die Auskunft nach Absatz 1 Buchstabe f zum „Bestehen eines Beschwerderechts bei der Aufsichtsbehörde“ sollte dahin formuliert werden, dass der Betroffene sich entsprechend Artikel 73 Absatz 1 an jede Aufsichtsbehörde wenden kann. Die weitergehende Information über die Kontaktdaten der jeweils zuständigen Aufsichtsbehörde sollte gestrichen werden.

– Absatz 1 Buchstabe g: Es sollte klargestellt werden, dass die Herkunft der Daten nicht beauskunftet werden muss, wenn die Erhebung beim Betroffenen erfolgt ist.

– Absatz 1 lit. h: Die Begriffe „Tragweite der Verarbeitung“ und „angestrebten Auswirkungen“ sind unklar. Es sollte entsprechend der Richtlinie 95/46/EG und Erwägungsgrund 51 eine Auskunft zum „logischen Aufbau der Verarbeitung“ oder besser zu „Aufbau, Struktur und Ablauf der Datenverarbeitung“ erfolgen. Die Formulierung „zumindest im Fall der Maßnahmen gemäß Artikel 20“ sollte lauten „zumindest im Fall des Artikel 20“, um auch Fälle der Profilbildung zu erfassen.

– In Bezug auf „Scorewerte“ zur Zahlungsbereitschaft und -fähigkeit sollte ein gesondertes Auskunftsrecht bestehen. Dies sollte im Wesentlichen wie folgt gestaltet sein: Der Verwender des Scorewerts, z.B. eine Bank, sollte Auskunft über die Scorewerte der letzten sechs Monate, die zur Berechnung genutzten Datenarten, das Zustandekommen und die Bedeutung des Scorewertes einzelfallbezogen, nachvollziehbar und in allgemein verständlicher Form erteilen. Soweit der Scorewert oder ein Bestandteil von Dritten berechnet wurde, muss dieser die erforderlichen Angaben zuliefern. Hat der Dritte den Scorewert insgesamt berechnet, kann für die Auskunft an ihn verwiesen werden. Daneben sollte gegenüber dem Dritten ein vergleichbares eigenes Auskunftsrecht bestehen, dass die übermittelten Scorewerte und Empfänger der letzten zwölf Monate, einen aktuell berechneten Scorewert, die genutzte Datenarten, das Zustandekommen und die Bedeutung des Scorewertes umfasst.

– Es sollte entsprechend Erwägungsgrund 51 ergänzt werden, ob und in welchen Fällen die Herkunft der Daten nach Buchstabe g und die Empfänger nach Buchstabe c im Bereich der Wirtschaft ggf. nicht beauskunftet werden müssen, soweit im Einzelfall das Interesse an der Wahrung von Betriebs- oder Geschäftsgeheimnisses das Interesse des Betroffenen an der Information überwiegt. Es sollte – vorbehaltlich eines eigenen Abschnitts für öffentliche Stellen - ergänzt werden, dass eine Pflicht zur Auskunft nicht besteht, wenn

- im öffentlichen und nicht-öffentlichen Bereich:

  – die Daten nur aufgrund gesetzlicher Aufbewahrungsvorschriften gespeichert sind und die Auskunft einen unverhältnismäßigen Aufwand bedeuten würden,

  – die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen, z.B. bei Rechtsanwälten aufgrund einer Schweigepflicht zugunsten ihres Mandanten,

- im nicht-öffentlichen Bereich:

  – die zuständige öffentliche Stelle gegenüber dem für die Verarbeitung Verantwortlichen festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle eines Mitgliedsstaates Nachteile bereiten würde,

  – die Auskunft die Geschäftszwecke des für die Verarbeitung Verantwortlichen erheblich gefährden würde, es sei denn, dass das Interesse an der Benachrichtigung die Gefährdung überwiegt,

  – die Verarbeitung für Zwecke der wissenschaftlichen Forschung erforderlich ist und die Auskunft einen unverhältnismäßigen Aufwand erfordern würde,

  – die Daten aus allgemein zugänglichen Quellen entnommen sind und eine Auskunft wegen der Vielzahl der betroffenen Fälle einen unverhältnismäßigen Aufwand bedeuten würde,

- im öffentlichen Bereich:

  – das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Mitgliedstaates Nachteile bereiten würde,

  – die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit des für die Verarbeitung Verantwortlichen liegenden Aufgabe gefährden würde es sei denn, dass das Interesse an der Benachrichtigung die Gefährdung überwiegt.

Für den öffentlichen Bereich sollte ergänzt werden, dass die Ablehnung der Auskunftserteilung keiner Begründung darf, soweit dadurch der mit ihr verfolgte Zweck gefährdet würde. In diesem Fall ist der Betroffene darauf hinzuweisen, dass er sich an die Aufsichtsbehörde wenden kann. Der Aufsichtsbehörde ist die Auskunft auf Verlangen des Betroffenen zu erteilen, soweit nicht im Einzelfall festgestellt wird, dass dadurch die Sicherheit des Mitgliedstaates gefährdet würde. Die Mitteilung der Aufsichtsbehörde an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand des für die Verarbeitung Verantwortlichen zulassen, sofern dieser nicht einer weitergehenden Mitteilung zustimmt.

- Absatz 2 sollte gestrichen werden. Satz 1 bietet keinen erkennbaren Mehrwert gegenüber Absatz 1 Buchstabe g. Satz 2 ist bereits in Artikel 12 Absatz 2 Satz 4 allgemein geregelt. Die o.a. Bemerkungen gelten hier analog.

- Absatz 3 sollte gestrichen werden. Die Ermächtigung bezieht sich nur auf Einzelheiten der Auskunft nach Absatz 1 Buchstabe g. Eine Regelung zu diesem umgrenzten Inhalt sollte bereits in der Verordnung erfolgen.

- Die Ermächtigung der Kommission in Absatz 4 ist zu streichen, da sie den laufenden Beratungen des Entwurfs einer Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt vorgreift Die Festlegung von Standardvorlagen und -verfahren für die Überprüfung der Identität der betroffenen Person greift sehr weitreichend in technische Standardisierungen auch im öffentlichen Bereich ein (z.B. gibt es in Deutschland etablierte Verfahren zur Identifizierung durch den neuen elektronischen Personalausweis). Auch ist die Frage der sektorspezifischen Regelungen im Rahmen der o.a. Beratungen noch offen. Die Bemerkungen zu Art. 12 Abs. 2 Satz 4 zu Mitteilungen auf elektronischem Wege gelten analog.

6. zu Artikel 16:

Satz 1 sollte mit Blick auf Artikel 5 Buchstabe d nicht von einem Verlangen der betroffenen Person abhängen und lauten:
„Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.“
Ergänzt werden sollte, dass bestrittene Daten, deren Richtigkeit oder Unrichtigkeit sich nicht feststellen lässt, zu sperren sind. Ergänzt werden sollte auch, dass an die Stelle des Berichtigungsrechts ein Recht auf Gegendarstellung tritt, wenn die personenbezogenen Daten geschäftsmäßig verarbeitet werden, aus allgemein zugänglichen Quellen stammen und zu

Dokumentationszwecken gespeichert sind, z.B. Datenbanken mit Presseauswertungen, die durch eine Berichtigung selbst unrichtig würden. Die Daten dürfen nur mit der Gegendarstellung übermittelt werden. Daten nach Artikel 9 sollten allerdings auch in diesen Fällen berichtigt werden. Satz 2 bedarf weiterer Erörterung. Der Inhalt des Rechts auf Vervollständigung neben dem Berichtigungsrechts bleibt unklar, etwa im öffentlichen Bereich bei einer Verarbeitung auf Grundlage einer Rechtsvorschrift.

7. zu Artikel 17:

Die Ausgestaltung der Löschungspflichten gehört zu den zentralen Punkten des Verordnungsvorschlags. Deutschland unterstützt das Ziel einer Stärkung der Löschungsrechte. Dies gilt insbesondere für selbst ins Internet gestellte Inhalte.

Wie eine Reihe anderer Mitgliedstaaten in der DAPIX sieht auch Deutschland noch weiteren Erörterungsbedarf, inwieweit ein „Recht auf Vergessenwerden“ als Rechtsprinzip eingeführt werden sollte. Insbesondere stellt sich die Frage, welche rechtlichen und praktischen Folgen an den in der Überschrift gewählten Begriff des „Vergessenwerden“ geknüpft werden. Nach den Aussagen der Kommission in der DAPIX sollen nur begrenzte Fallgruppen, vor allem soziale Netzwerke, erfasst werden. Im Regelungstext sollte klar geregelt werden, welche Pflichten generell und welche nur für bestimmte Bereiche gelten sollen. Vor allem mit Blick auf Anwendungen im Internet ist zum Teil bereits unklar, wer nach dem Verordnungsvorschlag als für die Verarbeitung Verantwortlicher und damit als Normadressat gesehen wird, z.B. bei der Veröffentlichung von Daten in einem sozialen Netzwerk: (nur) die veröffentlichende Person oder (auch) der Betreiber des Portals bzw. bei Postings auf der Seite eines Dritten gegebenenfalls auch dieser? Ohne eine eindeutige Klarstellung des Adressaten der Löschungspflichten besteht die Gefahr, dass gerade die zentrale Vorschrift des Artikel 17 gegenüber den Marktteilnehmern, die man im Blick hat, ins Leere läuft.

Des weiteren ist unklar, was „vertretbare Schritte auch technischer Art“ sind. Was ist mit Querverweisen, Kopien und Replikationen, die nach der Information erstellt werden, was passiert, wenn der ursprünglich für die Verarbeitung Verantwortliche nicht mehr existiert, identifiziert oder kontaktiert werden kann? Es bestehen insgesamt Zweifel an der Praktikabilität, vor allem bei Daten, die bereits aus öffentlichen Quellen stammen oder bei denen der Erstveröffentlichende nicht bekannt ist. Unklar ist auch, inwieweit die Regelung für Veröffentlichungen außerhalb des Internets zur Anwendung kommen soll.

Die Systematik des Artikel 17 ist, wie eine Reihe von Mitgliedstaten in der DAPIX hervorgehoben hat, unklar: Absatz 1 enthält ein subjektives Recht des Betroffenen auf Löschung, z.B. in Buchstabe a, wenn die personenbezogenen Daten für den Zweck der Verarbeitung nicht mehr notwendig sind. Es fehlt jedoch eine entsprechende allgemeine Löschungspflicht des für die Verarbeitung Verantwortlichen. Absatz 3 enthält dagegen eine allgemeine Löschungspflicht, selbst wenn die personenbezogenen Daten für den Zweck der Verarbeitung notwendig sind, sofern nicht einer der Buchstaben a bis d greift. Auch das Verhältnis zu den allgemeinen Verarbeitungsgrundsätzen in Artikel 5 und 7 bleibt unklar.

Aus Sicht der Bundesregierung sollte Artikel 17 Absatz 1 und 3 des Verordnungsvorschlags im Ergebnis ersetzt werden durch eine allgemeine Löschungspflicht des für die Verarbeitung Verantwortlichen, unabhängig von einem Verlangen der betroffenen Person, wenn die Speicherung des personenbezogenen Datums unzulässig oder seine Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Dies sollte sich auch in der Überschrift widerspiegeln. Die derzeit in Artikel 17 Absatz 3 a bis d geregelten Ausnahmen sollten dabei inhaltlich sichergestellt sein.

Zu Absatz 1 und 3:

- Absatz 1 sieht ein Recht auf Löschung und auf Unterlassung der weiteren Verbreitung vor. Es bleibt unklar, wie eine solche Unterlassung der weiteren Verbreitung nach bzw. neben einer Löschung aussehen soll und weshalb das Unterlassen sich nur auf das Verbreiten und nicht die weitere Verarbeitung bezieht.

  Deutschland unterstützt Bemühungen um einen verstärkten Schutz für Kinder. Allerdings ist die Bezugnahme „speziell“ auf im Kindesalter öffentlich gemachte Daten unsystematisch. Besteht das Recht auf Löschung und Unterlassung der Verbreitung uneingeschränkt, kann dies systematisch nicht „speziell“ für im Kindesalter öffentlich gemachte Daten gelten. Sprachlich bedeutet dies eine graduelle Entwertung des Löschungsrechts in anderen Fällen und sollte daher gestrichen und an anderer Stelle, z.B. im Zusammenhang mit der Veröffentlichung, im Rahmen einer Interessenabwägung bei Artikel 19 oder in einem eigenen Absatz, geregelt werden.

- Buchstabe b 2. Alternative sieht indirekt vor, dass eine Einwilligung befristet erteilt werden kann. Dies wäre in Artikel 7 zu regeln. Die gewählte Formulierung („Ablauf der Speicherfrist der Einwilligung“) bringt die Befristungsmöglichkeit auch nur unzureichend zum Ausdruck. Der Widerruf erfolgt ex nunc und darf durch eine Löschung der personenbezogengen Daten keine Wirkung ex tunc erlangen. Dies stünde im Widerspruch zu Artikel 7 Absatz 3 Satz 2.

– Buchstabe c ist missverständlich formuliert, weil ein Löschungsanspruch nicht mit dem Einlegen eines Widerspruchs nach Artikel 19 einher geht, sondern nur, sofern dessen materiellen Tatbestandsvoraussetzungen zur Unzulässigkeit der Datenverarbeitung führen. Zudem darf die Möglichkeit einer Sperrung statt Löschung nicht ausgeschlossen werden. Ziel eines z.B. Werbewiderspruchs ist die Unterbindung der weiteren (Adress-)Datenverarbeitung. Um dies sicherzustellen, dürfen die Daten gerade nicht gelöscht, sondern müssen in Bezug auf Werbezwecke gesperrt werden können (vergleiche Anmerkung zu Artikel 19 Absatz 3).

– Buchstabe d, die Unvereinbarkeit aus anderen Gründen, ist zu weitgehend. Wenn im Umkehrschluss zu Buchstaben a bis c die personenbezogenen Daten für den Verarbeitungszweck notwendig sind, eine Einwilligung oder anderweitige Rechtsgrundlage besteht und der Betroffene auch nicht widersprochen hat, können andere Gründe, z.B. ein Verstoß gegen formale Pflichten, nicht pauschal einen Löschungsanspruch begründen.

Zu Absatz 4 bis 6:

– Das Konzept des „Sperrens“ sollte in der Verordnung verankert werden. „Sperren“ sollte in Artikel 4 definiert werden, z.B. als „*das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung einzuschränken*“. Der für die Verarbeitung Verantwortliche sollte bei Vorliegen der Voraussetzungen zur Sperrung verpflichtet sein, was nach der deutschen Sprachfassung nicht der Fall ist („kann“). Unklar ist, wie eine Beschränkung oder Sperrung bei bereits veröffentlichen Daten erfolgen soll.

– Bei Buchstabe a sollte berücksichtigt werden, dass die Richtigkeit oder Unrichtigkeit sich gegebenenfalls nicht feststellen lässt.

– Bei Buchstabe b sollte eine Sperrung erfolgen, wenn die Daten für den Zweck der Speicherung nicht mehr erforderlich sind, der Löschung aber gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen. Eine hierüber hinausgehende Speicherung zu bloßen Beweiszwecken würde mit Blick auf etwaige künftige Streitverfahren „auf Vorrat“ geschehen und sollte nicht möglich sein.

– Buchstabe c erscheint als ein seltener Spezialfall. Geregelt werden sollte allgemein eine Sperrpflicht, wenn Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden.

– Buchstabe d ist nicht immer ein Fall der Sperrung. Nicht immer wollen Nutzer einen Dienst vollständig wechseln. Wenn der Wechsel zur Sperrung führt, würde ein neues Wechselhindernis geschaffen, wenn ein Nutzer zunächst einmal einen neuen Dienst ausprobieren will oder zwei Dienste parallel nutzen möchte.

– Neu geregelt werden sollte, dass eine Sperrung erfolgt, wenn eine Löschung wegen der besonderen Art der Speicherung (z.B. WORM-Systeme, Papierakten) nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

– Eine Verarbeitung gesperrter Daten sollte ohne Einwilligung der betroffenen Person nach Absatz 5 nur zulässig sein, wenn es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse des für die Verarbeitung Verantwortlichen oder eines Dritten liegenden Gründen unerlässlich ist und die Daten hierfür verarbeitet werden dürften, wenn sie nicht gesperrt wären. Es sollten zumindest die Anforderungen erfüllt sein, die an eine Verarbeitung gestellt worden wären, wenn die Daten nicht gesperrt gewesen wären.

– Absatz 6 setzt voraus, dass eine Aufhebung der Sperrung grundsätzlich möglich ist. Dies sollte in der Verordnung klargestellt, und es sollten zulässige Fälle benannt werden, z.B. wenn nach einer Unklarheit über die Richtigkeit der Daten deren Richtigkeit belegt ist.

Zu Absatz 7 bis 9:

– Absatz 7 wird unterstützt, ist jedoch eine Querschnittsregelung, die wie Artikel 5 des Rahmenbeschlusses 2008/977/JI für öffentliche Stellen als eigener Artikel gestaltet werden sollte.

– Absatz 8 sollte gestrichen werden. Nach der Löschung stehen die Daten für eine Verarbeitung in sonstiger Weise nicht mehr zur Verfügung, so dass die Regelung überflüssig erscheint. Ggf. könnte eine entsprechende Klarstellung auch in einem Erwägungsgrund erfolgen. Eine Definition des Löschens sollte aufgrund der unmittelbaren Anwendbarkeit der Verordnung in Artikel 4 vorgenommen werden, z.B. als „*das Unkenntlichmachen gespeicherter personenbezogener Daten*“.

– Zu Absatz 9 besteht ein Vorbehalt. Die Ermächtigung der Kommission ist sehr weitgehend und zudem unbestimmt formuliert. Regelungen zur Löschungspflicht oder Beschränkung der Verarbeitung wirken unmittelbar auf die Möglichkeiten einer zulässigen Datenverarbeitung ein. Eine Regelung sollte in der Verordnung getroffen oder den Mitgliedstaaten eingeräumt werden.

8. zu Artikel 18:

Wie eine Reihe anderer Mitgliedstaaten in der DAPIX sieht auch Deutschland bezüglich Anwendungsbereich und Umsetzbarkeit des Artikel 18 weiterhin starken Erörterungsbedarf. Es stellt sich die Frage, ob es sich beim Recht auf Datenübertragbarkeit um eine datenschutzrechtliche oder nicht vielmehr um eine wettbewerbs- oder urheberrechtliche Frage handelt. Die Vorschrift trifft eine sehr spezifische Regelung, die z.B. bei sozialen Netzwerken, Cloud- oder E-Mail-Diensten eine Berechtigung hat, als generelle Regelung jedoch unangemessen erscheint, z.B. auch mit Blick auf die Anwendbarkeit im öffentlichen Bereich, im Gesundheitsbereich, im Forschungsbereich oder bei Privatpersonen. Im öffentlichen Bereich können hochrangige öffentliche Interessen bestehen, die einer Kopie über die verarbeiteten Daten entgegenstehen. Im Bereich der Wirtschaft kann die Vorschrift Probleme mit sich bringen, z.B. wenn der Betroffene mit seiner Einkaufshistorie zu einem konkurrierenden (Online-) Händler oder mit seinen Kundendaten zu einer konkurrierenden Bank wechselt und mit der Herausgabe einer Kopie des Datensatzes geschützte Unternehmenspositionen oder Betriebs- und Geschäftsgeheimnisse offen gelegt werden müssten. Gerade im Online-Handel könnte die Regelung sogar neue Gefahren für den Datenschutz schaffen, wenn Unternehmen bei Neukunden Anreize dafür schaffen würden, ihnen die Kundenhistorie aus anderen Geschäftsbeziehungen zur Verfügung zu stellen. Betroffen sein dürften oft auch die personenbezogenen Daten anderer Personen (z.B. Empfänger einer Überweisung oder E-Mail, Lieferant einer Ware, Freunde auf Facebook). Zusätzliche datenschutzrechtliche Risiken entstehen, wenn der Anbieter, zu dem die betroffene Person personenbezogene Daten auch anderer Personen überführt, niedrigeren datenschutzrechtlichen Vorschriften oder Anforderungen unterliegt, etwa in einem Drittland. Zusätzliche datenschutzrechtliche Risiken können auch dadurch hervorgerufen werden, dass der für die Verarbeitung Verantwortliche, um Artikel 18 nachzukommen, dezentral verarbeitete Daten an einer Stelle zusammenführen muss. Die Umsetzung der Vorschrift wäre technisch anspruchsvoll und birgt die Gefahr erheblicher neuer bürokratischer Belastungen.

– Unklar ist, was in Absatz 1 mit einer „elektronischen Verarbeitung“ in Abgrenzung zur „automatisierten Verarbeitung“ gemeint ist.

  Der Begriff des „strukturierten gängigen elektronischen Formats“ ist unklar. Es ist nicht erkennbar, warum ein „Recht“ des Betroffenen von einer rein technischen Gestaltung abhängig sein soll. Unklar ist, wer bestimmt, wann ein Format „gängig“ ist. Ein in bestimmten Bereichen „gängiges Format“ kann in anderen Bereichen oder Staaten nicht verbreitet sein. Im Gesundheitsbereich etwa sind gängige Formate häufig nicht für eine weitere Bearbeitung durch die betroffene Person geeignet und eine Umstrukturierung ist nicht immer möglich. Unklar ist auch das Kriterium „strukturiert“. Bezugspunkt sind hier eher die Daten als das Format.

Unklar ist die Anforderung, dass die betroffene Person die Daten in einem „von ihr weiter verwendbaren … Format“ verlangen kann. Für den für die Verarbeitung Verantwortlichen ist nicht erkennbar, welches Format die betroffene Person weiter verwenden kann. Es bleibt auch offen, was „weiter verwenden“ bedeutet, ob dies z.B. eine automatisierte Verarbeitung verlangt oder die Möglichkeit eines Ausdrucks und weiteren Verwendung im Papier-Format genügt. Generell hängt die weitere Verwendung von ungewissen Faktoren und Vorgaben anderer Stellen ab. Insofern sollte hier ein objektiver Maßstab angelegt werden, z.B. indem man auf ein „üblicherweise elektronisch weiter verwendbares Format“ abstellt.

– In Absatz 2 erscheint es mit Blick auf das Schutzziel nicht konsistent, ein solches Recht nur zu gewähren, wenn die Verarbeitung auf einer Einwilligung oder einem Vertrag basiert und die betroffene Person die Daten zur Verfügung gestellt hat. Was bedeutet letzteres z.B. mit Blick auf das soziale Netzwerke, Cloud- oder E-Mail-Dienste, wenn der Diensteanwender dem Diensteanbieter personenbezogene Daten zur Verfügung stellt, die (auch) andere Personen betreffen (Freunde, Kunden, Empfänger). Des weiteren sollte auf den Begriff „entzogen“ verzichtet werden, da dieser zum einen unklar ist und zum anderen die Übertragung auch möglich sein sollte, wenn die betroffene Person den alten und den neuen Dienst nutzen möchte, die Daten also gerade nicht entziehen will.

  Unklar sind die Rechtsfolgen, z.B. wenn der für die Verarbeitung Verantwortliche auch nach Geltendmachung des Rechts nach Absatz 2 aufgrund eines Erlaubnistatbestandes berechtigt ist, die personenbezogenen Daten zu verarbeiten. Die Ausübung des Rechts nach Absatz 2 darf i.V.m. Artikel 17 Absatz 4 Buchstabe d und Absatz 5 dem für die Verarbeitung Verantwortlichen die weitere Vertragserfüllung nicht unmöglich machen.

  Unklar ist, was mit „etwaigen sonstigen von ihr zur Verfügung gestellten Informationen“ gemeint ist. Sollten hiermit auch nicht personenbezogene Daten gemeint sein, bestünden Zweifel an der Reichweite des Artikel 16 AEUV.

  Unklar ist, inwieweit der für das Empfängersystem für die Verarbeitung Verantwortliche verpflichtet ist, an der Überführung der Daten mitzuwirken, und inwieweit der für die Verarbeitung Veranwortliche des Ausgangssystems den Entzug der Daten „behindert“, wenn er an der Überführung lediglich nicht mitwirkt, z.B. keine Export-Funktion vorsieht.

– Zu Absatz 3 besteht ein Vorbehalt. Der Regelungsgehalt ist wesentlich. Erst durch die delegierten Rechtsakte würden der Anwendungsbereich und die Umsetzung der in den Absätzen 1 und 2 aufgestellten Anforderungen für die betroffenen Rechtsanwender präzise bestimmt. Eine solche Regelung sollte soweit wie möglich in der Verordnung selbst erfolgen. Berührt wären auch technische Standards und Verfahren, die bestehende Formate und Infrastruktur in den Mitgliedstaaten berühren. Soweit die Kommission festlegen könnte, in welchem Format ein für die Verarbeitung Verantwortlicher personenbezogene Daten vorhalten muss, wäre dies ein Eingriff in den Geschäftsbetrieb und grundrechtsrelevant.

9. zu Artikel 19:

Deutschland begrüßt die Aufnahme einer Regelung zum Widerspruchsrecht, hat jedoch einen Prüfvorbehalt zu der Formulierung der Regelung. Artikel 19 weist gegenüber Artikel 14 der Richtlinie 95/46/EG einige Änderungen auf:

– Die Formulierung der Abwägung in Absatz 1 weicht von der Formulierung der Abwägung in Artikel 6 Absatz 1 Buchstabe f ab, anders als in der Richtlinie 95/46/EG der Artikel 14 Buchstabe a von Artikel 7 Buchstabe f. Bislang muss der Betroffene „überwiegende, schutzwürdige, sich aus seiner besonderen Situation ergebende Gründe“ angeben, um eine rechtmäßige Datenverarbeitung mit seinem Widerspruch zu unterbinden. Künftig genügen „Gründe, die sich aus seiner besonderen Situation ergeben“, während die verarbeitende Stelle nun überwiegende, zwingende schutzwürdige Gründe für die Verarbeitung nachweisen muss.

  Beim Widerspruchsrecht ist auf eine Differenzierung zwischen dem nicht-öffentlichen und dem öffentlichen Bereich zu achten,

  Statt von „schutzwürdigen Gründen für die Verarbeitung“ zu sprechen, sollte - wie in Erwägungsgrund 56 und 38 - von „berechtigten Interessen für die Verarbeitung“ gesprochen werden.

  Unklar ist, welche zusätzlichen Anforderungen sich aus dem Begriff „zwingende“ Gründe ergeben, ob es also nicht genügt, dass die Gründe für die Verarbeitung überwiegen, sofern sie nicht auch „zwingend“ sind. Erwägungsgrund 56 nennt dieses Kriterium nicht. Das Wort „zwingende“ sollte daher gestrichen werden.

  Ein Widerspruchsrecht sollte im öffentlichen und nicht-öffentlichen Bereich dann nicht bestehen, wenn eine Rechtsvorschrift zur Verarbeitung verpflichet.

– Deutschland sieht Klärungsbedarf beim Verhältnis von Artikel 19 Absatz 2 zu Artikel 6 Absatz 1 Buchstabe f und Artikel 6 Absatz 4. Das Widerspruchsrecht lässt darauf schließen, dass Direktwerbung ohne Einwilligung auf Grundlage einer Interessenabwägung möglich ist. Dem steht entgegen, dass Artikel 6 Absatz 1 Buchstabe f die Interessen Dritter nicht mehr nennt und dass auch Artikel 6 Absatz 4 für zweckändernde Datenverarbeitungen nicht mehr auf Artikel 6 Absatz 1 Buchstabe f verweist. Klärungsbedarf besteht insoweit auch mit Blick auf Online-Werbung und die Richtlinie 2002/58/EG bzw. Artikel 89 des Verordnungsvorschlags.

  Die Unentgeltlichkeit des Widerspruchs in Absatz 2 Satz 1 ergibt sich aus der horizontalen Regelung in Artikel 12 Absatz 4 Satz 1 und kann hier gestrichen werden. Satz 2 kann mit Blick auf Artikel 11 Absatz 2 ebenfalls gestrichen werden.

  Soweit in Satz 2 als neues Erfordernis gegenüber Artikel 14 der Richtlinie 95/46/EG eine Information über den Werbewiderspruch in „von anderen Informationen klar abgegrenzten Form“ verlangt wird, stößt dies aus Platzgründen (Bsp.: Postkarte) und aufgrund weiterer zivil- und verbraucherrechtlicher Informationen, die abgesetzt werden sollen, an gestalterische Grenzen.

  Der Zeitpunkt der Information über den Werbewiderspruch ist – anders als in Richtlinie 95/46/EG – nicht mehr gesondert geregelt. Dem insoweit maßgeblichen Artikel 14 Absatz 4 Buchstabe b i.V.m. Absatz 1 Buchstabe d fehlt allerdings die zu ergänzende Möglichkeit nach Artikel 14 Buchstabe b der Richtlinie 95/46/EG, „vor der erstmaligen Nutzung im Auftrag Dritter zu Zwecken der Direktwerbung informiert zu werden“.

  Der zugehörige Erwägungsgrund 57 bedarf der Anpassung, da dort nur von Direktwerbung für „nichtkommerzielle Zwecke“ die Rede ist.

– Absatz 3 ist mit Blick auf Artikel 17 Absatz 1 Buchstabe c und Absatz 4 Buchstabe c unklar, da dort bereits eine Löschung bzw. Sperrung vorgesehen ist.

  Absatz 3 ist auch missverständlich formuliert. Werden Daten zum Zweck einer Vertragserfüllung erhoben und zudem für Werbezwecke verwendet und widerspricht die betroffene Person dieser Verwendung, so wäre es nicht im Interesse des Widersprechenden, wenn seine Daten auch nicht mehr für die Vertragserfüllung verarbeitet werden könnten. Folge des Widerspruchs sollte nur sein, dass die Verarbeitung zum Zweck der Direktwerbung nicht mehr möglich ist. Es ist auch zu berücksichtigen, dass, um den Werbewiderspruch beachten zu können, die Daten des Widersprechenden in der Praxis weiter genutzt werden müssen, um sie aus Adressbeständen für Direktmarketingmaßnahmen herauszufiltern. Absatz 3 bedarf daher einer entsprechenen Klarstellung.

10. zu Artikel 20:

Die Bundesregierung unterstützt eine Regelung zum Profiling. Dabei müssen zwei Aspekte berücksichtigt werden, nämlich

- zum einen, ob und unter welchen Voraussetzungen ein Profil im Sinne einer Verknüpfung von Daten, die eine besondere Aussagekraft über die Persönlichkeit des Betroffenen erlaubt, gebildet und weiterverarbeitet werden darf und

- unter welchen Bedingungen eine hierauf basierende ausschließlich automatisierte Maßnahme, die einen besonderen Nachteil für den Betroffenen hat, zulässig ist.

Es erscheint sinnvoll, hierfür zwei unterschiedliche Regelungen vorzusehen. Artikel 20 erfasst in Fortführung der Regelung zur automatisierten Einzelentscheidung in Artikel 15 der Richtlinie 95/46/EG im Wesentlichen nur den zweiten Aspekt.

Die Bundesregierung wünscht insbesondere eine Profilbildungsregelung zu Verfahren zur Berechnung der Wahrscheinlichkeit eines bestimmten Verhaltens, wie sie etwa § 28b des Bundesdatenschutzgesetzes vorsieht. Dort wird insbesondere verlangt, dass ein wissenschaftlich anerkanntes mathematisch-statistisches Verfahren zugrunde liegt, das nachweisbar für die Wahrscheinlichkeit des bestimmten Verhaltens erheblich ist.

Der Begriff des Profils und der Profilbildung, gegebenenfalls auch mit Blick auf eine Differenzierung nach Datenkategorien (z.B. allgemein zugängliche Daten, sensible Daten), bedarf noch weiterer Klärung und Ausgestaltung. Daten nach Art. 9 sollten nur in sehr engen Grenzen zur Profilbildung verwendbar sein. Eine Definition in Artikel 4 könnte mehr Rechtssicherheit bringen. Dabei ist auch die Europaratsempfehlung CM/Rec(2010)13 vom 23. November 2010 einzubeziehen.

Es sollten privilegierende Regelungen zum Umgang mit pseudonymen Profilen getroffen werden, z.B. zur Erstellung von ausschließlich pseudonymen Nutzungsprofilen durch Telemedienanbieter für Zwecke der Werbung, der Marktforschung oder zur bedarfgerechten Gestaltung der Telemedien, sofern der Nutzer nicht widerspricht. Über das Widerspruchsrecht ist der Nutzer zu informieren.

– In Absatz 1 sollten die Worte „Eine natürliche Person“, wie bei den anderen Rechten der betroffenen Person in Artikel 15 bis 19, durch die Worte „Die betroffene Person“ ersetzt werden.

  Es sollte klargestellt werden, dass die Vorschrift auf die automatisierte Verarbeitung von „personenbezogenen Daten“ beschränkt sein soll (vergleiche Artikel 4 Absatz 3 und Artikel 9 des Richtlinienvorschlags KOM(2012) 10 endg.).

Unklar bleibt, wann eine Maßnahme die betroffene Person „in maßgeblicher Weise beeinträchtigt“ (nach der Richtlinie 95/46/EG: erheblich beeinträchtigt). Um die Voraussetzung eines Nachteils bei der betroffenen Person deutlicher zum Ausdruck zu bringen, sollte Absatz 1 Maßnahmen erfassen, die gegenüber der betroffenen Person „nachteilige rechtliche Folgen“ entfalten (vergleiche Artikel 7 des Rahmenbeschlusses 2008/977/JI) oder die betroffene Person „in vergleichbarer Weise erheblich beeinträchtigen können“. In einem Erwägungsgrund sollten hierzu Beispiele benannt werden.

Die Worte „oder in der Analyse bzw. Voraussage“ sollten gestrichen werden, da sie dem Tatbestandsmerkmal der „Auswertung“ bzw. in der Übersetzung der Richtlinie 95/46/EG „Bewertung“ entsprechen. Klarzustellen ist beim Begriff „Aufenthaltsort“ die Ortsgenauigkeit, ob also bereits das Land als Aufenthaltsort genügt, was z.B. bei der Geolokalisation von IP-Adressen bedeutsam wäre.

Es sollte klargestellt werden, wann von einer „ausschließlich automatisierten Verarbeitung“ auszugehen ist, etwa durch die Formulierung: „… insbesondere dann, wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat“.

– Es ist unklar welche spezifischen Anforderungen sich aus dem Wort „ausdrücklich in Absatz 2 Buchstabe b für den Gesetzgeber ergeben. Nach nationalem und EU-Recht wird etwa von Banken und Versicherungen ein angemessenes Risikomanagement oder eine Prüfung der Kreditwürdigkeit von Verbrauchern verlangt (siehe etwa § 10 Kreditwesengesetz, Artikel 44 der Richtlinie 2009/138/EG „Solvency II“, Artikel 8 der Richtlinie 2008/48/EG „Verbraucherkreditrichtlinie“), ohne dass klar ist, ob damit eine Verarbeitung, wie sie in Artikel 20 Absatz 1 vorgesehen ist, „ausdrücklich“ gestattet wird.

  Bei Buchstabe c sind die Worte „und vorbehaltlich entsprechender Garantien“ zu streichen, da diese Formulierung Rechtsunsicherheiten begründet und sich die allgemeinen Pflichten z.B. zu Datensicherheit und Zweckbindung bereits aus anderen Vorschriften ergeben.

– Das Verbot der Profilbildung von „ausschließlich“ personenbezogenen Daten nach Artikel 9 in Absatz 3 erscheint nicht sinnvoll.

  Das Merkmal „ausschließlich“ kann leicht umgangen werden, indem neben den Daten nach Artikel 9 ein weiteres Datum in das Profil einfließt. Im Werbebereich könnte dies z.B. eine Altersgruppe oder das Geschlecht der betroffenen Person sein. Auch die Verknüpfung mit dem Namen oder der Anschrift der betroffenen Person würde das Verbot nach Absatz 3 aufheben, obwohl das Gefahrenpotential eher zunähme.

Ausschließlich auf Daten nach Artikel 9 gestützte Profile sollten auch nicht in jedem Fall verboten sein. Derartige Profile können beispielsweise im Bereich der Forschung erforderlich sein. In Bezug auf öffentlich zugängliche Daten und etwa politische Meinungen sind gegenläufige Grundrechte (z.B. Meinungsfreiheit, Informationsfreiheit, Forschungsfreiheit, Religionsfreiheit) angemessen zu berücksichtigen. Allerdings sollten an die Einbeziehung von Daten nach Artikel 9 in ein Profil und auch an die Qualität der Auswerteverfahren, die Transparenz und die Regeln zur Verwendung der Ergebnisse spezifische Anforderungen gestellt werden.

Nach Erwägungsgrund 58 sollen Kinder von auf Profilbildung beruhenden Maßnahmen generell ausgeschlossen sein. Dies findet keine Entsprechung im Regelungstext des Artikel 20 und bleibt daher unklar. Es wirft zudem – wie an anderen Stellen, an denen spezifische Maßnahmen zum Schutz von Kindern vorgesehen sind – die Frage auf, wie eine Altersverifikation vorgenommen werden soll und welcher Aufwand hiermit verbunden ist (Bsp.: Suchmaschine, Webstatistiken).

– Bei Absatz 4 sollte - entsprechend den Ausführungen zu Artikel 14 - die Information über die Existenz einer profilbildenden Verarbeitung dem Betroffenen als Basisinformation in geeigneter Weise direkt zur Verfügung gestellt werden. Die Formulierung „die angestrebten Auswirkungen auf die betroffene Person“ sollte entsprechend der Regelung in Artikel 15 Absatz 1 Buchstabe h ersetzt werden. Dabei handelt es sich - entsprechend den Ausführungen zu Artikel 14 - um eine weiterführende Datenschutzinformation, bei der der Betroffene auf einen leicht zugänglichen Ort verwiesen werden kann.

– Zu Absatz 5 besteht ein Vorbehalt. Es handelt sich um eine wesentliche Regelung, die in der Verordnung selbst geregelt werden sollte. Absatz 2 Buchstabe a nennt ein Beispiel für geeignete Maßnahmen. Artikel 15 der Richtlinie nennt mit der Möglichkeit, seinen Standpunkt geltend zu machen, ein weiteres Beispiel. Bei Absatz 5 besteht zumindest die Gefahr der Kollision mit der in Beratung befindlichen Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt.

11. zu Artikel 21:

– Absatz 1 sollte nicht nur Beschränkungen von Rechten der betroffenen Personen zulassen, sondern auch deren Erweiterung. So verlangt etwa Artikel 20 Absatz 2 Buchstabe b von den Mitgliedstaaten „geeignete Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person“, die etwa in Form erweiterter Auskunftsrechte, wie sie das deutsche Recht bei der Profilbildung zur Einschätzung der Kreditwürdigkeit (Scoring) vorsieht, über den Verordnungsvorschlag hinausgehen. Die Mitgliedstaaten benötigen auch mit Blick auf Artikel 6 Absatz 3 Spielräume, gerade im öffentlichen Bereich oder etwa im Gesundheitsbereich, zur näheren Konkretisierung und Ausgestaltung von Regelungen (insbesondere bei der Zweckbindung, der Art der Daten und der Empfänger) und zum Erlass strengerer Regelungen.

Die Möglichkeit, auch die Prinzipien der Datenverarbeitung nach Artikel 5 Buchstabe a bis e einzuschränken, bedarf weiterer Erörterung. Unklar ist z.B., wie eine Einschränkung des Prinzips, Daten auf rechtmäßige Weise zu verarbeiten (Artikel 5 Buchstabe a), aussehen soll, zumal eine Einschränkung der Rechtmäßigkeit der Verarbeitung in Artikel 6 nicht vorgesehen ist. Unklar ist auch, weshalb Artikel 5 Buchstabe f von Einschränkungen ausgenommen ist.

Es sollten in neuen Buchstaben, wie in Artikel 13 Absatz 1 der Richtlinie 95/46/EG die „Sicherheit des Staates“ und die „Landesverteidigung“ aufgenommen werden.

Die in Buchstabe c geregelte Möglichkeit der Beschränkung von Rechten der betroffenen Personen „zum Schutz sonstiger öffentlicher Interessen der Union oder eines Mitgliedstaates“ ist in der Richtline 95/46/EG nicht vorgesehen. Vielmehr ist die vergleichbare Ausnahmeregelung in Art. 13 Abs. 1 Buchstabe e der Richtlinie 95/46/EG auf „ein wichtiges wirtschaftliches oder finanzielles Interesse eines Mitgliedstaats oder der Europäischen Union“ beschränkt. Hierzu hat Deutschland weiteren Prüfungsbedarf.

Ein neuer Buchstabe oder eine Regelung in Artikel 10 sollte Einschränkungen auch bei der Verwendung pseudonymisierter Daten zulassen.

Es sollte klargestellt werden, was bei Buchstabe f mit den Rechten und Freiheiten anderer Personen gemeint ist, z.B. der Schutz der Meinungsfreiheit, Geschäftsgeheimnisse oder Eigentumsrechte eines Dritten.

Es sollte klargestellt werden, dass mitgliedstaatliche Regelungen nach Artikel 21, insbesondere nach Buchstabe f zum Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen mit Artikel 1 Absatz 3 vereinbar sind, der Einschränkungen des freien Datenverkehrs aus Gründen des Schutzes natürlicher Personen gerade verbietet.

– In Absatz 2 sollte vom „Zweck der Verarbeitung“ gesprochen werden.

12. zu Artikel 22:

Artikel 22 gilt für alle für die Verarbeitung Verantwortlichen, seien es öffentliche Stellen, die „Bäckerei um die Ecke“ oder eine Privatperson, die nach Artikel 2 Absatz 2 Buchstabe d unter die Datenschutz-Grundverordnung fällt. Eine Differenzierung nach der Gefahrgeneigtheit der Datenverarbeitung oder nach Verantwortungsbereichen (z.B. im Verhältnis Anbieter und Nutzer) erfolgt nicht. Daher und aufgrund der Bußgeldbewehrung nach Artikel 79 Absatz 6 Buchstabe e sollte konkretisiert werden, was von den Normadressaten bei den „geeigneten Strategien und Maßnahmen“ erwartet wird, welche Anforderungen an den Nachweis gestellt werden, wem gegenüber und in welcher Form er zu erbringen ist. Etwa für den Gesundheitsbereich bedarf die Regelung im Hinblick auf besondere Verfahren ggf. der Anpassung (vgl. auch Stellungnahme zu Artikel 4)

– Der einleitende Satz von Absatz 2 sollte deutlicher machen, dass die Maßnahmen nach Buchstabe a bis e nur getroffen werden müssen, wenn die in dem jeweiligen Artikel vorgesehen Voraussetzungen erfüllt sind. So müssen z.B. die Maßnahmen nach Buchstabe a und e nicht durch KMU vorgenommen werden, sofern deren Tätigkeit nicht mit besonderen Gefahren in Bezug auf den Datenschutz verbunden sind.

– Es sollte zu Absatz 3 klargestellt werden, was „geeigneten Verfahren zur Überprüfung“ sind, z.B. mit Blick auf Absatz 2 Buchstabe e.

  Die Überprüfung der Wirksamkeit nach Satz 1 sollte angesichts der Breite der Normadressaten und der fehlenden Risikobasiertheit – wie in Satz 2 vorgesehen – nur verlangt werden, „wenn dies angemessen ist“. Es sollte auch konkretisiert werden, unter welchen Umständen eine Überprüfung „angemessen“ ist. Diese Einschränkung wäre allerdings entbehrlich, wenn der Anwendungsbereich auf besonders risikobehaftete Datenverarbeitungen oder auf das Verhältnis Anbieter-Nutzer beschränkt würde.

  Es bedarf der Klarstellung, was mit der „Unabhängigkeit“ der Prüfer gemeint ist, z.B. wenn diese gegen Entgelt tätig werden. Das Kriterium sollte die Einschaltung interner Stellen, wie der Revisions- oder Compliance-Abteilung, nicht ausschließen. Konkretisiert werden sollte auch das Verhältnis der unabhängigen Prüfer zu den innerbehördlichen und -betrieblichen Datenschutzbeauftragten und deren Einbindung in die Überprüfung.

Es sollte klargestellt werden, dass der Prüfer nur eine Stellungnahme abgibt, die Entscheidung über die Maßnahme und deren Wirksamkeit aber dem für die Verarbeitung Verantwortlichen obliegt. Zudem sollte klargestellt werden, dass die für die Verarbeitung Verantwortlichen das Ergebnis der Überprüfung veröffentlichen können.

– Zu Absatz 4 besteht ein Vorbehalt. Es handelt sich um eine wesentliche Regelung, insbesondere soweit der Katalog der Maßnahmen nach Absatz 2 erweitert werden kann und soweit die Bedingungen für die Überprüfungs- und Auditverfahren festgelegt werden sollen.

13. zu Artikel 23:

Deutschland begrüßt die Aufnahme einer Regelung zum Datenschutz durch Technik (by design) und durch Voreinstellungen (by default), wünscht sich aber – im Bewußtsein der Notwendigkeit von Technologieneutralität, aber auch der Bußgeldbewehrung in Artikel 79 Absatz 6 Buchstabe e – genauere Vorgaben und Ziele für die Technikgestaltung und die Voreinstellungen in die Absätze 1 und 2 aufzunehmen. Z.B. sollte mit Blick auf Artikel 5 Buchstabe c der Grundsatz der Datensparsamkeit und -vermeidung sowie die Anonymisierung und Pseudonymisierung als zentrale Möglichkeit der Umsetzung aufgeführt werden. Die Notwendigkeit der Konkretisierung besteht auch, soweit Artikel 23 Anforderungen an den für die Verarbeitung Verantwortlichen stellt, die über die in Artikel 6 festgelegten Voraussetzungen einer rechtmäßigen Datenverarbeitung hinausgehen.

Zum Normadressaten der Absätze 1 und 2 sieht die Bundesregierung noch Erörterungsbedarf. Es sollten rechtliche Anreizen dafür geschaffen werden, dass auch die Technikentwickler und Hersteller ihre Produkte und Dienstleistungen datenschutzkonform gestalten.

– Bei Absatz 1 sollten – wie bei Artikel 30 – nur „angemessene“ Maßnahmen vorgesehen werden. Bezugspunkt der Angemessenheit sollte auch das mit der Datenverarbeitung verbundene Gefährdungspotential sein.

  Vor den Worten „und die Rechte der betroffenen Person gewahrt werden“ sollte das Wort „insbesondere“ eingefügt werden.

– Notwendig erscheinen auch bei Absatz 2 konkretere Anforderungen an die Voreinstellungen, z.B. ob zunächst die höchste Sicherheitseinstellung einzustellen ist oder unter welchen Voraussetzungen die betroffene Person die Voreinstellungen ändern kann.

Unklar bleibt die Anwendung insbesondere des Satzes 2 auf natürliche Personen als für die Verarbeitung Verantwortliche nach Artikel 2 Absatz 2 Buchstabe d, z.B. bei der Gestaltung einer Webseite oder beim Bloggen.

In der deutschen Sprachfassung müssen in Absatz 2 Satz 1 und 2 die Wörter „durch Voreinstellung“ (in der englischen Fassung „by default“) ergänzt werden.

– Zu Absatz 3 und 4 besteht ein Vorbehalt. Es handelt es sich um wesentliche Regelungen, die Rückwirkungen auf in den Mitgliedstaaten bereits etablierte Verfahren der technischen Standardisierung und Zertifizierung, sowie in den Mitgliedstaaten etablierte Sicherheits-Infrastrukturen (elektronische Signaturen, neuer Personalausweis, De-Mail) haben können Die Bundesregierung wünscht sich zur Konkretisierung technischer Standards einen Ansatz, der nur ausnahmsweise „von oben“ (top-down), im Regelfall jedoch „von Unten“ (bottom-up“) erfolgt. Hierfür können die bewährten Strukturen etwa im Bereich der technischen Standardisierung (z.B. durch ISO-Normen) und Zertifizierung (einschließlich der gegenseitigen Anerkennung entsprechender Zertifikate im Sinne des „new approach“) genutzt werden. Auch das Vorgehen beim Privacy Impact Assessement für RFID-Anwendungen auf EU-Ebene könnte ein Vorbild sein. Erörterungsbedürftig ist darüber hinaus, inwieweit in der Verordnung notwendige Rahmenregelungen für Anreizsysteme etwa im Bereich des Datenschutzmanagements fehlen. Auch hierbei handelt es sich um wesentliche Regelungen, die durch die Verordnung selbst getroffen werden müssten. Bei Absatz 3 und 4 besteht zumindest die Gefahr der Kollision mit der in Beratung befindlichen Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt. Hier muss eine klare Abgrenzung erfolgen.

14. zu Artikel 24:

Deutschland hält die Regelung, wie einige andere Mitgliedstaaten in der DAPIX, für noch nicht ausreichend klar. Durch die Vereinbarung darf nicht zum Nachteil des Betroffenen Verantwortung abgewälzt werden, z.B. auf für die Verarbeitung Verantwortliche in Drittstaaten. Klärungsbedürftig ist unter anderem, ob die Vorschrift auch die Datenverarbeitung im Konzern verbundener Unternehmen erfassen soll.

– Es sollte vorgesehen werden, dass ein Betroffener sich zur Ausübung seiner Rechte an jeden der gemeinsam für die Verarbeitung Verantwortlichen wenden kann, da Absprachen im Innenverhältnis nicht zu seinen Lasten gehen dürfen. Dabei sollte eindeutig zum Ausdruck gebracht werden, dass der Verantwortliche, an den sich der Betroffene wendet, nicht an den anderen verweisen darf.

– Es sollten – neben der Ermöglichung der Rechte betroffener Personen – weitere Inhalte benannt werden, die bei einer gemeinsamen Verantwortlichkeit zu regeln sind, z.B. wer Ansprechpartner der Aufsichtsbehörde ist.

– Es fehlen Verfahrens-, Streitbeilegungs- oder Zweifelsregeln, wie die Vereinbarung zustande kommen soll und wie zu verfahren ist, wenn eine Einigung nicht erfolgt.

15. zu Artikel 25:

Die Rechts- und Pflichtenstellung des Vertreters ist unklar. Nach Artikel 4 Absatz 14 und Erwägungsgrund 63 fungiert der Vertreter nur als „Ansprechpartner“ für Aufsichtsbehörden oder sonstigen Stellen in der Union. Artikel 53 Absatz 1 Buchstabe c legt dem Vertreter, korrespondierend mit seiner Nennung in Artikel 28 und 29, eine Pflicht zur Bereitstellung von Informationen auf. Ob Artikel 78 Absatz 2 hierauf begrenzt oder allgemein zu verstehen ist, bleibt unklar. Es sollte daher klargestellt werden, dass aufsichtsbehördliche oder gerichtliche Maßnahmen und Sanktionen gegenüber dem Vertreter rechtswirksam verhängt, zugestellt und durchgesetzt werden können.

Der Vertreter sollte nach Artikel 4 Absatz 14 ausdrücklich auch als Ansprechpartner von betroffenen Personen fungieren, wie dies Artikel 14 Absatz 1 Buchstabe a voraussetzt. Artikel 4 Absatz 14 ist entsprechend zu ergänzen.

– Mit Blick auf die Ausführungen in Erwägungsgrund 20 zu Artikel 3 Absatz 2, es sei „sicherzugehen, dass Personen nicht des Schutzes beraubt werden, auf den sie nach der Verordnung ein Anrecht haben“ und den Ausnahmen nach Absatz 2 besteht Erörterungsbedarf. Deutschland hat Zweifel, ob eine effektive Durchsetzung des Artikel 3 Absatz 2 gewährleistet ist. Artikel 4 Absatz 2 der Richtlinie 95/46/EG sah keine Ausnahme von der Pflicht zur Benennung eines Vertreters vor.

  Buchstabe a sollte gestrichen werden. Die Frage, ob in einem Drittland ein angemessenes Datenschutzniveau gewährleistet wird, sollte keine Rolle spielen, da im Falle des Artikel 3 Absatz 2 die Datenschutz-Grundverordnung und nicht das Recht des Drittstaates zur Anwendung kommen soll. Zudem gewährleisten die Angemessenheitsentscheidungen der Kommission keine gleichwertige Rechtsdurchsetzung von Betroffenenrechten und aufsichtsbehördlichen Maßnahmen wie in der EU.

Bei Buchstabe b bestehen Zweifel an der Eignung des Kriteriums. Die mit der Rechtsdurchsetzung verbundenen Probleme in Drittstaaten sind nicht abhängig von der Unternehmensgröße. Der Schwellenwert bedeutet, ginge man von der in der Folgenabschätzung für die EU genannten Unternehmenszusammensetzung aus, dass 99,8% aller Unternehmen in Drittländern von der Benennungspflicht entbunden sind. Für die Aufsichtsbehörde oder Dritte ist es zudem praktisch kaum feststellbar, wie viele Mitarbeiter ein Unternehmen in einem Drittland beschäftigt.

Bei Buchstabe d wird zu dem Wort „gelegentlich“ – trotz der Erläuterungen in Erwägungsgrund 64 – Klärungssbedarf gesehen.

– Absatz 3 führt bei Unternehmen, die Dienste im Internet regelmäßig EU-weit anbieten, zur freien Wahl, wo sie innerhalb der EU den Vertreter benennen. Die Regelung sollte mit der aufsichtsbehördlichen Zuständigkeitsbestimmung in den Fällen des Artikel 3 Absatz 2 einhergehen. Zuständig sollte jedenfalls auch die Aufsichtsbehörde des Mitgliedstaates sein, in dem der Vertreter benannt wird.

16. zu Artikel 26:

Die bislang in dem Verordnungsentwurf enthaltenen Vorschriften zur Auftragsdatenverarbeitung sind nur bedingt geeignet, neue technische Entwicklungen, insbesondere Cloud Computing-Dienste, praxisnah und rechtssicher zu erfassen. Das Cloud-Computing kann nicht mit klassischen Datenverarbeitungen im Auftrag, wie z.B. großen IT-Outsorcing-Projekten, verglichen werden. Der Nutzer eines Cloud Computing-Dienstes kann regelmäßig nicht als „Herr des Verfahrens“ und Verantwortlicher für die Datenverarbeitungsvorgänge in der Cloud angesehen werden. Einige Besonderheiten von Cloud Computing-Diensten im Zusammenhang mit den Regelungen zur Auftragsdatenverarbeitung können durch die nachfolgend dargestellten Vorschläge berücksichtigt werden. Dies betrifft insbesondere differenzierte Regelungen für die Kontrolle des Auftragnehmers oder den Anforderungen an den Vertrag. Gegebenenfalls bedarf es weiterer noch zu bestimmender Regelungen.

Die Regelung bedarf weiterer Prüfung, inwieweit sie für bestehende und sich entwickelnde Verfahren und Dienstleistungen etwa im Gesundheitswesen anwendbar und sinnvoll sind, insbesondere die Verarbeitung pseudonymisierter oder verschlüsselter Daten und die Verwaltung medizinischer Aktensysteme unter Kontrolle des Patienten („google-health“, „health vault“) (vgl. Stellungnahme zu Artikel 4).

– Aus Sicht der Bundesregierung fehlt in Absatz 1, wie in Erwägungsgrund 62 gefordert, eine grundsätzliche Regelung zum Verhältnis zwischen dem für die Verarbeitung Verantwortlichen (Auftraggeber) und dem Auftragsverarbeiter (Auftragnehmer). Vorgesehen werden sollte einleitend:

> *„Werden personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet, ist der für die Verarbeitung Verantwortliche für die Einhaltung der Vorschriften über den Datenschutz verantwortlich."*

Hieraus folgend sollte in einem weiteren Satz klargestellt werden, dass die Rechte des Betroffenen sowie das Recht auf Schadensersatz gegenüber dem für die Verarbeitung Verantwortlichen geltend zu machen sind.

Um die Zuteilung der Verantwortlichkeiten klarzustellen, sollten die Pflichten, die eigenständig an den Auftragsverarbeiter adressiert sind, vor allem die Gewährleistung der Datensicherheit (Artikel 30), in einem eigenen Absatz abschließend aufgeführt werden.

Der letzte Halbsatz von Absatz 1 sollte ein eigener Satz werden und vorsehen, dass sich der Auftraggeber erstmals vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt. Es sollte dabei, vor allem auch mit Blick auf das Cloud Computing, klargestellt werden, dass es hierfür nicht erforderlich ist, dass der Auftraggeber vor Ort eine Kontrolle durchführt, was tatsächlich regelmäßig nicht zu leisten wäre, sondern dass ein geeignetes Testat eines unabhängigen, fachlich geeigneten Sachverständigen ausreicht. Auch durch eine Verschärfung der Haftung kann die dem Auftragnehmer obliegenden Gewährleistung der Datensicherheit verbessert und der Auftraggeber von deren Kontrolle entlastet werden.

– In Absatz 2 sollte am Anfang ein neuer Buchstabe zu den Essentialia des Auftrags aufgenommen werden, namentlich „Gegenstand und Dauer des Auftrags, Art und Zweck der Verarbeitung, Art der Daten und Kreis der Betroffenen". Eine solche Festlegung im Auftrag erscheint notwendig, damit der Auftragsverarbeiter die Grenzen seines Auftrags vor Augen hat.

– Mit Blick auf das Cloud Computing sollten die Anforderungen an Inhalt und Form des Vertrages so modifiziert werden, dass der Vertragsinhalt vom Auftragnehmer den gesetzlichen Vorgaben entsprechend zu einem Großteil vorbereitet und über Webformular erfüllt werden kann. Damit kann der Praxis Rechnung getragen werden, wenn wie bei Cloud Computing üblich standardisierte Dienste angeboten werden.

– Es sollte in einem eigenen Satz geregelt werden, dass „*der Auftragsverarbeiter die personenbezogenen Daten nur im Rahmen der Weisungen des für die Verarbeitung Verantwortlichen verarbeiten darf*“. Diese für die Auftragsverarbeitung zentrale Bestimmung sollte nicht nur indirekt über eine Vorgabe des Inhalts des Auftrags erfolgen. Buchstabe a sollte dann, diesen Satz aufgreifend, vorsehen, dass „die Weisungsbefugnisse, des für die Verarbeitung Verantwortlichen“ festzulegen sind. Klarzustellen ist, dass eine Weisung auch unmittelbar im Auftrag erfolgen kann. Die derzeitige Formulierung des Buchstaben a ist missverständlich. Das „insbesondere“ kann relativierend dahin verstanden werden, der Auftragsverarbeiter dürfe in bestimmten Fällen ohne Weisung handeln. Zudem wird der Anschein erweckt, der Auftragsverarbeiter solle unzulässige Datenübermittlungen nur auf Weisung des für die Verarbeitung Verantwortlichen vornehmen. Die Unzulässigkeit einer Datenverarbeitung wird durch eine Weisung aber nicht „geheilt“. Ergänzend sollte in einem neuen Satz vorgesehen werden, dass „*der Auftragnehmer den Auftraggeber unverzüglich darauf hinzuweisen hat, wenn nach seiner Auffassung eine Weisung gegen datenschutzrechtliche Vorschriften verstößt*“.

– Die in Buchstabe b vorgesehene Verpflichtung auf das Datengeheimnis sollte nicht alle Mitarbeiter erfassen, sondern nur die mit der Datenverarbeitung beschäftigten und terminologisch („employ“) keine arbeitsrechtlichen Beschränkungen enthalten.

– Buchstabe c sollte vorsehen, dass im Auftrag konkret „*die nach Artikel 30 zu treffenden technischen und organisatorischen Maßnahmen*“ festzulegen und nicht lediglich, dass Maßnahmen nach Artikel 30 zu treffen sind. Letzteres ergibt sich bereits aus Artikel 30. Die konkrete Festlegung im Auftrag erleichtert, sich, wie in Absatz 1 vorgesehen, von der Einhaltung der Maßnahmen zu überzeugen.

– Die unter Buchstabe d vorgesehene Verpflichtung auf eine vorherige Zustimmung ist in bestimmten Konstellationen nicht praktikabel, z.B. wenn ein Auftragsverarbeiter eine Vielzahl an Kunden hat und beim Wechsel eines technischen Dienstleisters mehrere tausend Zustimmungen einholen müsste. Vorgesehen werden sollte daher vor allem, dass im Auftrag „*die etwaige Berechtigung zur Begründung von Auftragsverhältnissen*“ festzulegen ist, es aber den Parteien überlassen bleibt, ob und wie sie eine Zustimmungspflicht vorsehen wollen. Klargestellt werden sollte, dass die Zustimmung auch im Auftrag selbst erteilt werden kann.

– Bei Buchstabe e sollte vorgesehen werden, dass Auftraggeber und Auftragnehmer im Rahmen der Vertragsgestaltungsfreiheit für die konkrete Auftragsverarbeitung festzulegen haben, „*ob und inwieweit der für die Verarbeitung Verantwortlichen bei der Erfüllung ihm obliegender Pflichten zu unterstützen ist*“. Dies betrifft neben der Erfüllung der Betroffenenrechte u.a. auch die unter Buchstabe f genannten Pflichten.

– Buchstabe f sollte nicht verbindlich festlegen, dass der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen bei der Einhaltung der Artikel 30 bis 34 zu unterstützen hat. In verschiedenen Fällen kann der Auftragsverarbeiter eine solche Unterstützung tatsächlich nicht leisten, etwa weil der für die Verarbeitung Verantwortliche die Zwecke, Mittel und Bedingungen der Verarbeitung festlegt. Flexibler wäre, die zu Buchstabe e vorgeschlagene Formulierung.

– Zeitlicher Anknüpfungspunkt bei Buchstabe g sollte die Beendigung des Auftrags sein, nicht der Abschluss der Verarbeitung, da bei einer mitunter langjährigen Auftragsverarbeitung eine Vielzahl von Verarbeitungen durchgeführt und abgeschlossen wird. Unklar ist, was mit dem Aushändigen „sämtlicher Ergebnisse“ gemeint ist. Derzeit erlaubt Buchstabe g auch, dass die Daten personenbezogen beim Auftragsverarbeiter verbleiben. Vorgesehen werden sollte, dass der Auftragsverarbeiter „*nach Beendigung des Auftrags die bei ihm zu dem Auftrag gespeicherten personenbezogenen Daten löscht und etwaige überlassene Daten und Datenträger zurückgibt*“.

– Die Pflicht zur Zusammenarbeit mit der Aufsichtsbehörde in Buchstabe h besteht entsprechend zu den Befugnissen der Aufsichtsbehörde in Artikel 53. Sie ist darüber hinaus in Artikel 29 geregelt und kann hier gestrichen werden. Mit Blick auf das Verhältnis zum für die Verarbeitung Verantwortlichen sollten im Auftrag allgemein „*die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungsrechte des Auftragnehmers*“, z.B. Betretensrechte, periodische Berichtspflichten durch einen zertifizierten Prüfer, geregelt werden.

– Absatz 3 sollte keinen unnötigen Verwaltungsaufwand verursachen. Sofern eine Dokumentation bereits im Vertrag oder Rechtsakt nach Absatz 2 erfolgt, sollte dies auch für Absatz 3 genügen. Für die Dokumentation sollte Textform genügen, z.B. ein Webformular. Dies sollte, vor allem auch mit Blick auf das Cloud Computing, auch für den Vertrag nach Absatz 2 gelten.

– Absatz 4 sollte gestrichen werden. Verarbeitet der Auftragsverarbeiter personenbezogene Daten anders als vom für die Verarbeitung Verantwortlichen angewiesen, liegt ein Verstoß gegen den ihr Innenverhältnis regelnden Vertrag oder Rechtsakt vor, der hierfür Regelungen, z.B. Schadensersatz oder eine Vertragsstrafe, vorsehen sollte. Der Verweis auf Artikel 24 erscheint unnötig und auch ungeeignet, weil es unwahrscheinlich ist, dass die aufgrund des weisunsgwidrigen Handelns gegebenenfalls zerstrittenen Beteiligten sich über die Pflichtenverteilung einigen.

– Zu Absatz 5 hat Deutschland einen Vorbehalt. Deutschland erachtet die Regelung als wesentlich. Insbesondere die Frage, ob spezielle Regelungen für die Verarbeitung in Unternehmensgruppen getroffen werden sollen oder nicht, hat erhebliche Auswirkungen für Unternehmen wie für die Betroffenen, so dass entsprechende Regelungen in der Verordnung getroffen werden müssten.

17. zu Artikel 27:

Unklar ist, inwieweit sich durch die neue Überschrift der Regelungsgehalt der ansonsten mit Artikel 16 der Richtlinie 95/46/EG nahezu identischen Vorschrift geändert hat. Die Pflicht des Auftragsverarbeiters, nur auf Weisung des für die Verarbeitung Verantwortlichen zu handeln, folgt bereits aus Artikel 26. In Bezug auf dem Auftragsverarbeiter unterstellte Personen kann eine sich gegebenenfalls widersprechende Weisungslage durch den für die Verarbeitung Verantwortlichen und den Auftragsverarbeiter ergeben.

Aus Sicht Deutschlands enthält Artikel 27, wie bislang Artikel 16 der Richtlinie 95/46/EG die auch in Artikel 26 Absatz 2 Buchstabe b in Bezug genommene Verpflichtung, mit der Datenverarbeitung beschäftigte Personen persönlich auf einen rechtmäßigen Datenumgang zu verpflichten, um bei Verstößen z.B. arbeitsrechtliche Konsequenzen gegenüber der beschäftigten Person ziehen zu können.

Die persönliche Verpflichtung auf einen rechtmäßigen Datenumgang wird durch die Bezugnahme auf „Anweisungen“ allerdings nicht deutlich. Zudem ist unklar, weshalb auch der Auftragsverarbeiter selbst aufgeführt wird, der eine juristische Person sein kann und insoweit persönlich nicht verpflichtet werden kann.

Die Vorschrift sollte daher wie folgt formuliert werden:
„Mit der Datenverarbeitung beschäftigten Personen ist untersagt personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). Hierauf sind sie bei Aufnahme ihrer Tätigkeit zu verpflichten. Die Pflicht wirkt nach Beendigung ihrer Tätigkeit fort.“

ESTONIA

Article 11

We welcome the idea of the transparency of the processing of personal data. However, in public sector, the rules for processing of personal data are laid down by the law and different legal acts. Therefore, art 11 should be more flexible and provide that policies shall be elaborated in cases when data subject cannot have adequate information about processing of personal data from already existing and available documents.

Also, we would support the idea of risk-based approach. So, polices are useful in the areas, where processing of the personal data is essential and day-by-day task. If the data processing is accidental, the policies are rather not necessary.

Article 12

A general provision for exercising the rights of the data subject is necessary. Nevertheless, we would suggest forming this stipulation in more abstract way. The essence of this article is that the data subject has a right to know, when and why his or her personal data is processed. The controller has an obligation to answer to this request. The regulation would be more flexible and take into account the future developments, when the form of the answer of the controller is not regulated. Already today, the controllers use many different means of communication. For example, the answer or explanation for the data subject can be given orally, while the phone calls are recorded or in Skype in messenger environment or data subject can look up logs of the data processing etc.

Article 14

Some further clarification is needed, how article 14 should be implemented. The question is, whether art 14 is concretizing art 11 and should art 14 be implemented actively or passively. To be more clear, should the controller establish easily accessible policies and describe the information given in art 14 in these polices (actively) or this information has to be made available upon request (passively). If art 14 is connected to the article 11, then we would suggest combining those articles.

Article 16

Concerning right to rectification, the term of inaccurate needs further clarification. The question is, when personal data is inaccurate – whether it is connected to different periods of time or some other characteristics. Right to rectification should be supplemented with “in cases the personal data is needed for further processing”. Inaccurate personal data can be sometimes necessary for data processing in specific areas or in specific purposes, e.g. journalistic purposes.

Article 18

If the processor is a public authority then regulation should take into account directive 2003/98/EC on the re-use of public sector information (PSI directive) and open data concept. PSI directive obliges public sector to make public sector information available in open and reusable formats. Therefore, right to data portability and precise electronic format and technical standards would not be coherent with the idea of open formats. Although, general access on information and request of the data subject are slightly different, it should be clear for Member States, if they can refuse the request of the data subject referring to PSI directive, since art 5 in PSI directive stipulates that public sector bodies shall not to create or adapt documents in order to comply with the request, nor shall it imply an obligation to provide extracts from documents where this would involve disproportionate effort, going beyond a simple operation.

Articles 22 – 27

During the Working Party meeting Member States did lots of comments concerning processor and controller. One of the concerns were, that the whole concept of the processor and controller is aged. Therefore, we would recommend revising it generally to make it usable in future.

Translation problems

Art 11 states - The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights.

In Estonian it has been translated – vastutav töötleja kehtestab läbipaistvad isikuandmete töötlemise ja andmesubjektide õiguste kaitsmise põhimõtted ja teeb need lihtsalt kättesaadavaks.

It should be – vastutaval töötlejal peavad olema läbipaistvad ja kergesti kättesaadavad andmekaitse strateegiad, mis käsitlevad isikuandmete töötlemist ja andmesubjekti õiguste teostamist.

SPAIN

This document conveys Spain's comments on Chapter III and on Articles 20 to 27 of Chapter IV of the proposal for a General Data Protection Regulation, via the Presidency of the DAPIX Working Party. It is a working document, so the conclusions it contains may change somewhat as discussions proceed.

Contents

1. Chapter III. Rights of the data subject

Article 11

We must begin by stating as we begin discussion of this article that we are in full agreement with the principles of transparency and information applied to the protection of personal data.

That said, the current wording of Article 11 raises some questions we think need to be addressed in depth.

The regulation is organised in the first instance around the concept of "policies" on personal data processing and on the rights of data subjects.

It seems clear that those "policies", which must also be transparent and easily accessible, must consist of specific procedures that each controller will apply in accordance with the activity and objectives concerned, in the framework of the general rules contained in the regulation.

Now, however clear the above may seem, the fact is that the regulation nowhere explains the interpretation of these "policies" nor, more importantly, their specific content and scope.

This creates legal uncertainty that should be avoided.

To that end it is necessary first of all to define clearly what kind of policies should be established, what their minimal content – if any – should be, and what the policies should cover. We realise that a priori this is not easy, since, obviously, their content may vary widely depending on the sector, type of processing, etc.

We should also apply flexibility and proportionality here, especially in relation to small and medium-sized operators, in both public and private sectors; we must avoid overloading them with excessive costs, especially when probably in risk terms there is no need to develop over-complex and all-embracing policies.

That is why we favour the following wording for Article 11(1):

*The controller shall **apply criteria of transparency and accessibility** with regard to the processing of personal data and for the exercise of data subjects' rights. **To that end, he or she may arrange for those criteria to be disseminated through the formulation of policies which shall be communicated to all data subjects.***

This wording affirms the principles of transparency and accessibility while leaving open the option of formulating specific policies in the framework of the regulation. The formulation of policies is not a general requirement but is a matter for each controller; recommendations and related incentives can be established by the supervisory authorities.

As for paragraph 2 of this article, we agree that the information should be provided to the data subject in an understandable form and in simple and clear language. However, we think the need for language to be adapted to the requirements of the data subject could be excessive and hard to put into practice in a general way.

Consequently, to avoid disproportionate burdens, we propose an alternative wording as follows:

The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language ***as far as possible. The above must be taken into account particularly for any information addressed specifically to children.***

In short, once amended this article would read as follows:

Article 11

Transparent information and communication

1. *The controller shall ~~have transparent and easily accessible policies~~* ***apply criteria of transparency and accessibility*** *with regard to the processing of personal data and for the exercise of data subjects' rights.* ***To that end, he or she may arrange for those criteria to be disseminated through the formulation of policies which shall be communicated to all data subjects.***

2. *The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language* ***as far as possible.*** *~~adapted to the data subject, in particular for any information addressed specifically to a child.~~* ***The above must be taken into account particularly for any information addressed specifically to children.***

Article 12

This article does not raise any general problems for us. However, in line with our comments on Article 11, we propose some changes in paragraphs 1 and 2 to avoid unnecessary burdens in certain cases.

In fact, the important thing here is that the information be obtainable and rights can be exercised. To these ends, some organisations may, given their size or complexity, require the establishment of clearly defined procedures for the exercise of the rights in question, while other smaller or simpler ones will not need procedures as such or at most will need in a very simple way to inform the data subjects as to what to do.

Thus, to avoid a need for procedures to be designed and drafted in all cases, we propose the following text:

*The controller shall ~~establish procedures for providing~~ shall **provide** the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. ~~Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.~~*

Where considered useful, all the information may be documented in the form of policies and manuals of procedure, to facilitate its understanding and handling.

In addition, this is one of the first rules in which the legislator refers to the form of applications, making a specific reference to the electronic format.

In our view the regulation should in this kind of case maintain total neutrality regarding technology, neither prohibiting nor restricting particular forms of communication between data subjects. This is important since, precisely because of the wide scope this regulation is intended to have, the realities, needs and options in the various sectors and subsectors concerned will vary very widely; it therefore seems inadvisable to lay down rules for this kind of point. We therefore propose deleting the last sentences of paragraphs 1 and 2 of Article 12.

To conclude, as amended this article would read as follows:

Article 12

Procedures and mechanisms for exercising the rights of the data subject

1. *The controller shall ~~establish procedures for providing~~* ***provide*** *the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. ~~Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.~~* ***Where considered useful, all the information may be documented in the form of policies and manuals of procedure, to facilitate its understanding and handling.***

2. *The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.*

3. *If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.*

4. *The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.*

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the manifestly excessive requests and the fees referred to in paragraph 4.

6. The Commission may lay down standard forms and specifying standard procedures for the communication referred to in paragraph 2, including the electronic format. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 13

Article 13 introduces one of the many unclear legal concepts that appear in the proposal. In this case it is that of "disproportionate effort".

There is no doubt that to apply the regulation in practice it would be very important to interpret and quantify this notion correctly, since in some manner it will determine the level of requirement in any given case, and in general terms it must be seen in terms of the administrative or bureaucratic workload that the regulation may entail for the various parties concerned.

We believe that it is appropriate to use the concept but it would be useful to try to give the clearest possible criteria, dogmatically, in the recitals to ensure that it can be applied.

Article 14

Article 14 relates to the information that has to be given to the data subject when collecting personal data.

Points (a) to (h) in paragraph 1 establish the minimum necessary information that must be provided.

Our first assessment of this article is that it is useful, and plays an important role throughout the system insofar as the information given to the data subject is one of the main guarantees of the system.

Nevertheless, on the basis of a combined analysis of points (a) to (h) we conclude that the information covered may be excessive: sometimes redundant and sometimes impossible to comply with.

First of all it may be excessive because the quantity of data supposedly to be provided to the data subject could end up diluting the data subject's interest in the truly important parts. An excess of information does not necessarily generally amount to better safeguards; it could even tend in the opposite direction.

In terms of the data subject's rights, what interests the latter is mainly knowing that his or her personal data is being processed, for some particular reason. That is the basic point enabling the data subject to exercise his or her rights.

Any additional information may indeed be of interest, but there is also the risk that the most essential information is watered down and the key message is not received, or not as clearly as it should be.

A balance must be found. That balance could be achieved by the amendments we propose below.

We said too that the information in (a) to (h) could be redundant in some cases. Thus, in (b) it is said that information must be given on the purposes of the processing, including the contract terms and general conditions where applicable, or the legitimate interests pursued. We think giving the data subject – who can, if in doubt, request any further information he or she sees fit – a clear reference to the purposes of the processing would be sufficient. So there is no need to add the contractual terms or general conditions or any further clarification of the legitimate interests pursued. All that may be important later, if the data subject wants to ask for more information or to initiate actions, but for the purposes of Article 14 we think it goes beyond what is needed and is redundant, thus creating an unnecessary administrative burden.

We also began by saying that some of the information covered in (a) to (h) could be impossible to comply with, or at least it may not be possible to provide it at first. This is true for the data storage period and for the intention to transfer the data to a third country or international organisation.

In line with the above, we do not see why there is any need to give information on the identity of the data controller, his/her representative or the data protection officer. There seems no need to reveal the personal identity of these parties in order adequately to protect the rights of the data subject; a reference to his/her institutional roles and an institutional contact should be enough. In addition, using personal rather than institutional identity will undoubtedly pose practical problems in the future, since whenever a controller, representative or data protection officer changes, the personal identity of the new holder of the position concerned would need to be provided, which is unrealistic.

Given all the above, we propose the following changes to the first part of this article:

Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:

(a) ~~*the identity and*~~ *the contact details of the controller and, if any, of the controller's representative and of the data protection officer;*

(b) *the purposes of the processing for which the personal data are intended*~~*, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1)*~~*;*

(c) ***where possible,*** *the period for which the personal data will be stored;*

(d) *the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;*

(e) *the right to lodge a complaint to the supervisory authority* ~~*and the contact details of the supervisory authority*~~*;*

(f) *the recipients or categories of recipients of the personal data;*

(g) *where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;*

(h) *any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.*

Another noteworthy point regarding this article is paragraph 4, which regulates the time when the information on the processing has to be provided to the data subject.

Point 4(a) indicates that it must be provided when the data are collected from the data subject. In general this should not pose major problems, but for some activities a minimum of flexibility may be necessary; furthermore it will be easy for the supervisory authorities to see that such flexibility is properly applied. In addition, depending on how the data are collected, it may provide the data subject with a better safeguard if the information is sent immediately afterwards, in written or electronic form, so that he or she can take proper cognizance of the situation.

We therefore propose to amend paragraph 4 as follows:

The controller shall provide the information referred to in paragraphs 1, 2 and 3:

(a) **in general** at the time when the personal data are obtained from the data subject, **or as soon as possible when the first option is not feasible, requires a disproportionate effort or reduces the safeguards to the data subject;** or

(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.

We must also comment on paragraph 5, which lists a number of exceptions regarding the provision of information.

Some sectors have referred to a need to make an express exception of cases where provision of information could compromise an investigation in progress or could be counterproductive for the prosecution of certain crimes, such as money-laundering. To deal with this it has been proposed that the legislation should include a reference to express prohibition; if we understand correctly the provisions of Article 21 may well be sufficient.

Finally, we understand that the delegated acts referred to in paragraph 7 go beyond the general restrictions for the use of this method, since if applicable they constitute matters that should be addressed in the regulation itself.

Thus, as amended, the article would read as follows:

Article 14

Information to the data subject

1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:

*(a) ~~the identity and t~~**T**he contact details of the controller and, if any, of the controller's representative and of the data protection officer;*

(b) the purposes of the processing for which the personal data are intended, ~~including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);~~

*(c) **where possible,** the period for which the personal data will be stored;*

(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;

(e) the right to lodge a complaint to the supervisory authority ~~and the contact details of the supervisory authority~~;

(f) the recipients or categories of recipients of the personal data;

(g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;

(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.

2. *Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.*

3. *Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate.*

4. *The controller shall provide the information referred to in paragraphs 1, 2 and 3:*

   (a) ***in general*** *at the time when the personal data are obtained from the data subject,* ***or as soon as possible when the first option is not feasible, requires a disproportionate effort or reduces the safeguards to the data subject; or***

   (b) *where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.*

5. *Paragraphs 1 to 4 shall not apply, where:*

   (a) *the data subject has already the information referred to in paragraphs 1, 2 and 3; or*

   (b) *the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or*

   (c) *the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or*

   (d) *the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.*

6. *In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.*

~~*7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises.*~~

8. The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 15

This article regulates the so-called right of access. This means the right of any data subject to ascertain whether personal data concerning him or her are being processed.

The first thing to be said regarding this right is that, depending on the scale of the controller and how many files it has to handle, the exercise of the right must be modulated somewhat. To request from certain controllers general information on all the data they are dealing with (e.g. the administration of a state) could give rise to an over-burdensome workload, particularly where the interest of the requesting subject will normally be limited to one or a small number of particular areas.

In accordance with the above, we think that it is in the interests of all concerned to modulate the exercise of this right such that the controller can validly request that the data subject determine what files or what specific areas the request concerns.

Besides this, we repeat here, mutatis mutandis, the considerations set out in the context of the preceding article on the amount of information to be provided.

Given the foregoing, we note a certain redundancy between points (b) and (g) of paragraph 1, to resolve which it will suffice to delete one of them, in our view (b).

As to the data storage period, again and for the same reasons set out in relation to Article 15, we think the most reasonable thing is to lay down that information need be given on this point only when possible, given the type and purpose of the data processed.

Regarding the supervisory authority's contact data, again for the same reasons set out in relation to the preceding article, we think that this point should be deleted here.

Consequently, we think the first paragraph of this article should be amended to read as follows:

The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. ***Where the controller processes a large quantity of files concerning the data subject, he may request that before the information is delivered the data subject adequately specify to which file or files or to which areas of activity the request relates.*** *Where such personal data are being processed, the controller shall provide the following information:*

(a) the purposes of the processing;

(b) ~~*the categories of personal data concerned;*~~

(c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries;

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

(e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;

(f) the right to lodge a complaint to the supervisory authority ~~*and the contact details*~~*;*

(g) communication of the personal data undergoing processing and of any available information as to their source;

(h) ~~*the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.*~~

As to the second paragraph of this article, its first sentence is redundant, since the data communication to which it refers has already been dealt with in the previous paragraph, and its second sentence again moves into areas of technological neutrality in a way contrary to our thinking as expressed above. So we propose deleting the whole paragraph.

After amending as proposed the article would read as follows:

Article 15

Right of access for the data subject

1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. ***Where the controller processes a large quantity of files concerning the data subject, he may request that before the information is delivered the data subject adequately specify to which file or files or to which areas of activity the request relates.*** *Where such personal data are being processed, the controller shall provide the following information:*

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries;

(d) the period for which the personal data will be stored;

(e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;

(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;

(g) communication of the personal data undergoing processing and of any available information as to their source;

(h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.

~~*2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.*~~

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.

4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 16

No comment.

Article 17

Article 17 governs two distinguishable rights: the right to erasure of data and the right to be forgotten.

We say the rights are distinguishable because the right to erasure of data is a logical consequence of the general principles of data protection. As such it is a standard right.

Processing of such data is justified insofar as there is a legal basis and the purposes to be achieved are covered by that basis. When one of those elements disappears, the data can no longer be processed – with some legal exceptions permitting storage – and must be deleted.

The right to be forgotten, meanwhile, is a newly minted right starting essentially from the specific issue raised by electronic processing of certain data over public networks.

The right to be forgotten arises essentially on the basis of problems arising from the internet's great capacity for disseminating personal data.

Even so, the proposal for a regulation formulates the right to be forgotten in general terms, and thus with a scope which in principle need not be restricted to the internet.
In addition, as now worded in Article 17, the right to be forgotten is sectorally independent, so its applicability extends to both private and public sectors.[1]
As such, many issues arise around this Article 17 we are discussing.
The first paragraph of the article begins by stating that *the data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child*…
As mentioned, this is a standard right of deletion or erasure, which holds, going by the wording of the rule, between the data subject, as data owner, and the data controller.
The right applies universally to any case of processing of personal data, and regarding the last quoted point from the paragraph, it is particularly important for data provided in the data subject's childhood, which we take to mean two things: (a) that the right is not subject to any time limit or expiry as time passes and (b) that the controller must deal diligently with all requests received but somehow especially so and even preferentially with the erasing of data resulting from data transfers from the data subject's childhood, which in a way gives particular importance to protecting the right of erasure as regards data provided at a time of special age-based vulnerability.
The article goes on to give the conditions for exercising the right to erasure, as follows:

(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;

(c) the data subject objects to the processing of personal data pursuant to Article 19;

(d) the processing of the data does not comply with this Regulation for other reasons.

We have no objection to these conditions, which revolve around the disappearance of the legal basis for the processing, or its initial invalidity.

[1] Obviously, without prejudice to restrictions that might be imposed on the basis of Article 21.

Regarding paragraph 1 the question arises of how to deal with the case where the initial controller has disappeared and therefore it is impossible to exercise the right vis-à-vis that controller.
In these cases there are basically two kinds of situation, namely: (a) if the initial controller has been replaced by another person or entity, in which case we see no problem in the action being taken against the successor; and (b) that technically no such succession has occurred but third parties are nevertheless processing the data. In this latter case we take it that the action will still be viable on condition that those third parties cannot successfully cite a legal basis or a case for retention.
In any case, we think it can quite well be claimed that none of these cases warrants an amendment, for the time being at least, since the reference to "*the controller*" should be sufficient, that expression being very general.
Still, to promote discussion on these questions and, perhaps, clarify the article, we suggest the possibility of including the following paragraph at the end of the present second paragraph:
Where the controller who permitted access to the personal data has disappeared, ceased to exist or cannot be contacted by the data subject for other reasons, the data subject shall have the right to have other data controllers delete any link to copies or replications thereof.
Moving now to the right of erasure *stricto sensu*, Article 17(2) provides that: *Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.*
As we said before, the right addressed in this second paragraph is substantially different from that in the first paragraph, although they are undoubtedly related.
The data subject has a right to apply for the erasure of his or her personal data, subject to certain legal conditions, by the processing *controller*, i.e. by whoever is at that point responsible for the processing. This seems to us indisputable, and to that extent it is clear that on the basis of an Article 17(1) action it is already possible to achieve what we might call an "oblivion effect".
However, what the legislator aspires to in the second paragraph is, first, to facilitate matters for the data subject, by requiring a proactive intervention by the controller in those cases where the latter has made data public, through the imposition of a requirement to act by informing those third parties of the wish to delete, and second, to establish an additional responsibility where *the controller has authorised a third party to publish the data subject's personal data*.

We shall proceed step by step in examining the practical issues this rule may raise.
As regards the obligation to act by informing, it seems that the *controller's* responsibility is exhausted by the transmission of that information. To fulfil that obligation, as the article itself says, *all reasonable steps, including technical measures*, must be taken.
We see the main issues that arise in analysing the application of this rule as:

- interpreting "*reasonable*", and whether or not that term is sufficient to avoid imposing unreasonable burdens on the controller;
- whether or not the measures, including technical measures, must be adopted in advance, with a view to a possible future "forgetting" action.

On the first point, some prior reflections are needed to reach conclusions.
First, the potential of the right to be forgotten will be very different in the electronic, digital world (byte products) compared to the physical, analogue world (atomic products).
In the electronic, digital world it is technically possible to erase any datum and its entire sequence of events or appearances. We say technically possible, though we know it can often be very difficult. What is technically possible may be impossible in practice. For instance, consider that a datum on the internet may be stored on more than one server, those servers may not be administered by the same persons or entities, and some of them may be in the hands of natural persons whom it is difficult to locate or render answerable, because of their location, use of false identities, etc.
Even so, the differences between the electronic, digital world and the "physical" world are clear from our point of view. Let us take an example: to destroy a collection of photographs on the internet merely requires an instruction to delete them from the archives, which is certainly complicated if those photographs have been disseminated widely on the web, but even so, a deletion instruction on the corresponding servers or databases is sufficient. But if that same photograph appeared in a physical magazine or newspaper, strictly speaking the right to be forgotten can be successfully exercised only by the destruction of every copy, and that is indeed impossible in practice once they have been distributed.
Consequently, the first conclusion that is obtained from these reflections is that the right to be forgotten will have major real limits. Those limits will vary with the context or medium, and in some cases the job of providing information, which the article seeks to impose on the controller, may be very onerous.

Secondly, the right to be forgotten, to look at it in the most general terms, exceeds the scope of the regulation, as defined in Article 2(1). Let us go back to the example of a photograph in a newspaper. To truly make the right to be forgotten effective in this case, it is not enough to act on a hypothetical filing system in the possession of the newspaper publisher; rather, this would have to be done to all copies, yet these are not filing systems in the sense intended in Article 2.
In short, the right to be forgotten, defined from the point of view of personal data protection, has severe limits and, if we do not want to slow down technical and economic development, we cannot operate on the basis of overburdensome responsibilities focused on the processing controller(s).
In other words, a reasonable balance must be found, and we should not completely abandon the notion of a fair balance of risks and corresponding assumption of responsibilities.
This means that someone launching information consisting of personal data onto a network as huge and complex as the internet should at all times be well informed and conscious that it may not always be possible to withdraw it, at least not 100 %. Thus we will avoid creating expectations that later cannot be met.
So, having got this far, the key questions are: how far should the data controller's obligations extend? And what exactly is meant by having made the data public?
Let us start with the second question.
We think the drafter, in using the words *made the data public*, refers to all those cases in which the data controller has not kept the data inaccessible or restrictedly accessible, so that anyone could have gained access to them or even incorporated them in other processing.
In addition, we must assume, since otherwise the responsibilities would be different, that the controller who kept the personal data accessible did so on a quite legitimate legal basis.
This being so, it seems that the obligation that may be laid on the controller must be constructed from two factors, with which we move to the second question raised above: (1) the reasonableness of the media, such that they are based on routine technologies and do not require prohibitive tools or tools in very limited use due to their developmental level and cost; and (2) the proportionality of those media, such that the requirement is fitted to the capabilities of the controller, thus protecting, in particular, small and medium-sized enterprises, which in many cases will not be able to make investments in very expensive technologies without compromising their business activity.
Having spelt this out we can now answer the other question we first raised, namely whether the measures referred to in Article 17(2) should be taken in advance, foreseeing a possible "forgetting" action , or not.

We think that on the basis of the current wording the answer must be yes. This follows from the use of the words "*to inform third parties*…". All in all, in terms of legality, probably the least important aspect is whether these measures are taken beforehand or not, if in the end the controller, when the action is initiated, is in a position entirely to fulfil the requirement laid down by the regulation to provide information to third parties.

Thus, bearing in mind the above, we think the rule should be amended as follows:

Where the controller referred to in paragraph 1 has ***expressly or tacitly allowed third parties access to*** ~~*made*~~ *the personal data* ~~*public*~~*, it shall take all reasonable steps* ***proportionate with its capabilities****, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data.* ~~*Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.*~~

The proposed amendments on the one hand clarify the basic assumption on which the imposition on the controller of an obligation to inform operates: the fact that he or she has expressly or tacitly permitted third-party access to the personal data; and the concept of proportionality is introduced, so that there can be no requirement of measures which are unfeasibly costly for certain operators.

Besides the above, we propose deleting the last sentence which refers to authorising the publication of personal data.

The responsibility or otherwise of the data transferor, for actions of the transferee, will have to be determined base by case, depending on the surrounding facts and circumstances, which is quite different from imposing a sort of objective responsibility regarding the right to be forgotten. In other words, what seems to be meant here is that one authorisation to publish suffices for the initial controller to become responsible for the erasure of data in third-party hands, such that if the third party does not or cannot achieve that erasure, the initial controller is responsible for all purposes for harm done. We find this consequence potentially excessive and that it cannot be assumed in a general way, and we therefore propose deleting the last sentence of Article 17(2).

We are in agreement regarding the data storage cases addressed in Article 17(3).

However, the data storage envisaged in this paragraph can be conceptually distinguished in some cases from its online multiplication. In other words, it is one thing for data to have to be kept for specific reasons, legally and axiologically superimposed on the right to be forgotten, and another for their dissemination necessarily to continue to be permitted. The latter cannot always be necessary, any more than it is compatible with a strict necessity for storage. We therefore propose adding the following paragraph at the end of 17(3):

In the cases covered in (a) to (d), the data subject may exercise a right to object vis-à-vis the establishment of links or the making of copies or replications of their personal data. The viability of this right shall be determined on the basis of the surrounding circumstances of the case, pains being taken not thereby to frustrate the specific purpose of the storage of the data.

Given that the data storage cases that may arise in practice may be very distinct in their details, it seems reasonable, furthermore, to provide for a margin of discretion regarding the viability of the right to object to which we refer.

As regards the rest of Article 17, apart from our final comments on delegated acts, we have no more objections, and underline the importance of Article 17(3)(d), insofar as it can be used to establish, through legislation, public-interest-based limits on the exercise of this right. This will make it possible to solve some of the problems that could arise regarding the right to be forgotten in the public-sector context and to ensure the right balance between that right and others of undeniable social interest (namely right to information and to the non-forgetting/remembrance of certain situations). To conclude, and bearing in mind those limits, we propose the following wording for point 3(d), so that the required safeguards can be applicable both to Union law and to that of the Member States:

for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; ***Union and*** *Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;*

As to delegated acts we cannot accept Article 17(9) since it covers the regulation of aspects essential to the proper understanding of the rule. If these aspects need to be addressed, they should be developed in the regulation itself.

Thus Article 17 should read as follows:

Article 17

Right to be forgotten and to erasure

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:

(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;

(c) the data subject objects to the processing of personal data pursuant to Article 19;

(d) the processing of the data does not comply with this Regulation for other reasons.

2. Where the controller referred to in paragraph 1 has ***expressly or tacitly allowed third parties access to*** ~~*made*~~ *the personal data* ~~*public*~~*, it shall take all reasonable steps* ***proportionate with its capabilities****, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data.* ~~*Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.*~~

Where the controller who permitted access to the personal data has disappeared, ceased to exist or cannot be contacted by the data subject for other reasons, the data subject shall have the right to have other data controllers delete any link to copies or replications thereof.

3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:

(a) for exercising the right of freedom of expression in accordance with Article 80;

(b) for reasons of public interest in the area of public health in accordance with Article 81;

(c) for historical, statistical and scientific research purposes in accordance with Article 83;

(d) *for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject;* ***Union and*** *Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;*

(e) *in the cases referred to in paragraph 4.*

In the cases covered in (a) to (d), the data subject may exercise a right to object vis-à-vis the establishment of links or the making of copies or replications of their personal data. The viability of this right shall be determined on the basis of the surrounding circumstances of the case, pains being taken not thereby to frustrate the specific purpose of the storage of the data.

4. *Instead of erasure, the controller shall restrict processing of personal data where:*

(a) *their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;*

(b) *the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;*

(c) *the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;*

(d) *the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2).*

5. *Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.*

6. *Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.*

7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.

8. Where the erasure is carried out, the controller shall not otherwise process such personal data.

~~*9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:*~~

~~*(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;*~~

~~*(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;*~~

~~*(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.*~~

Article 18

Article 18 concerns two different rights: the right to obtain a copy of the data, and the right to transfer the data to third parties. Both rights are covered by the legislator in the broader concept of portability. We think the way this right is regulated here is acceptable and poses no major problems. However, there are a number of points to which attention should be drawn.

As regards the first paragraph, we think the decisive point for the regulation of this right is not so much that the data be processed in a structured and commonly used format but also that where applicable they be delivered in a structured and commonly used format.

To that end the following amendment would be necessary:

The data subject shall have the right, where personal data are processed by electronic means and in a structured ~~and commonly used~~ format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.

On the above basis and bearing in mind that on occasions the formats that are used for data processing may be ones not commonly used, it seems reasonable to impose a fee for conversion of the data into a requested format. This could be done via the following amendment, which would add to this rule a new second paragraph:

Where the format requested by the data subject is not the same as that of the processing, the controller may charge a fee for conversion, which may not exceed the value of the cost of the service performed at market prices.

We think the amendment is justified by the fact that requesting a given format that is not the same as that of the processing gives rise to a new service, which must require compensation. In addition, if the option of obtaining the data in a given format is granted, it seems logical that the cost of the conversion should not fall to the controller.

Following this amendment, paragraphs 2 and 3 would become 3 and 4 respectively.

Lastly, we think there has to be some reference to the relation between this right and the erasure of data. In principle, portability, as regards obtaining copies of the data, need not imply their erasure. However, if we refer to portability in a strict sense, i.e. transfer from one controller to another, then the issue of erasure does need to be raised. Here some safeguards would be necessary for those cases where data has to be kept.

The following additional last paragraph would be sufficient:

The controller from whom the data are obtained shall delete those data, unless their continued processing is required on a separate applicable legal basis. Union law and Member States' legislation may determine those cases in which there is a legal obligation to retain data, on the basis of public interest objectives proportionate to the aim pursued and honouring the essence of personal data protection law.

This article would read as follows once amended:

Article 18

Right to data portability

1. The data subject shall have the right, where personal data are processed by electronic means and in a structured ~~and commonly used~~ format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.

Where the format requested by the data subject is not the same as that of the processing, the controller may charge a fee for conversion, which may not exceed the cost of the service performed at market prices.

2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.

The controller from whom the data are obtained shall delete those data, unless their continued processing is required on a separate applicable legal basis. Union law and Member States' legislation may determine those cases in which there is a legal obligation to retain data, on the basis of public interest objectives proportionate to the aim pursued and honouring the essence of personal data protection law.

3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 19

This article regulates a right for the data subject to object, for processing based on Article 6(1)(d), (e) and (f).

We have no objections in principle, except to the third paragraph.

If there exists in relation to the right to object a possibility that the controller can cite compelling legitimate grounds, we see no reason why the mere formulation of an objection has to initiate the consequence intended by the third paragraph[1].

[1] To some extent, this problem can be solved by applying the rule in Article 12(3), but even so, we believe it is not superfluous to try to clarify this rule further, to avoid a situation in which mere objection can by itself lead to the processing being stopped.

We therefore propose to amend this paragraph as follows:

Where an objection is upheld pursuant to paragraphs 1 and 2, the controller ***shall inform the data subject of the compelling legitimate reasons applicable as referred to in paragraph 1 above, or otherwise*** *shall no longer use or otherwise process the personal data concerned.*

Thus, there is a genuine opportunity to object, and should there be a dispute on the subject, the legally relevant actions and the applicable compensations are clear.

The article would then read as follows:

Article 19

Right to object

1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object free of charge to the processing of their personal data for such marketing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information.

3. Where an objection is upheld pursuant to paragraphs 1 and 2, the controller ***shall inform the data subject of the compelling legitimate reasons applicable as referred to in paragraph 1 above, or otherwise*** *shall no longer use or otherwise process the personal data concerned.*

Article 20

Article 20 addresses the consequences of the technique known as profiling. However, there is no definition of the term's intended meaning.

According to Recommendation CM/Rec(2010)13 of the Committee of Ministers of the Council of Europe, profiling means an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviour and attitudes.

On the above basis, one should consider the need to include a definition of this kind in Article 4 of the proposal.

While profiling offers unquestionable and numerous benefits both commercially and in the public sector, insofar as it exploits the massive data-processing capacity offered by modern technologies, there is no doubt that it also brings risks for individuals insofar as it allows them to be framed in a completely automated way in certain preset categories, without their knowledge and with major impacts that can affect both their personal lives and their wealth.

These facts demand that limits and safeguards be established as to the use of such techniques, seeking a reasonable balance between protection of privacy and other rights of the individual, and the increasing needs of a society which is ever more complex and technologised, which not infrequently demands speed and objectivity in decision-making, not only in the interests of institutions or companies but also often in the interests of the individual data subject.

In the present day, there are many and varied applications of profiling, from public safety through financial or labour-market decision-making to advertising.

The wide-ranging and ever-increasing application of profiling techniques in very diverse sectors means that it is not possible to adopt completely general regulatory solutions and that specificities and sectoral needs must be taken into account.

It is thus desirable to consider that these issues are best addressed in regulatory terms in the specific areas of rules that they may apply to (financial, employment, advertising, etc.).

The basis of the above argument is that in essence this is not a personal data protection issue[1] but rather one of how such data can be used to derive legal effects or consequences in certain areas of economic or social relations.

That being so, it could seem most reasonable to regulate the possible consequences of automated data processing case by case in the areas concerned and taking account of the specificities and needs applicable in those areas. In that way, much more coherent regulatory frameworks, better suited to each situation, would be obtained. However, the absence of a general provision, establishing the basic restrictions and safeguards, would lead to a situation in which anything was permitted insofar as matters linked to such techniques were not regulated in all sectors. To this problem would be added the fact that there would probably always be sectors left to cover, since the inexorable advance of technology opens up new possibilities which might be unforeseeable in advance.

[1] This is not indisputable, given the attractive force of data protection rights at this juncture.

For that reason it does seem to us appropriate to include in the proposal for a regulation a basic and general profiling rule.

That said, and turning now to the proposed text of Article 20, we think it should be examined in depth in the light of the previously quoted Council of Europe recommendation.

We find the expression "measure which […] significantly affects", contained in the first paragraph, too broad, and it would be desirable to narrow it down somewhat, specifying that it must relate to measures affecting an individual adversely.

Likewise, the restrictions relating to location and personal preferences should also be studied and probably refined.

We also have our doubts about the absolute limiting of profiling based on the special categories of data included in Article 9.

Lastly, we think this article must require specific sectoral developments, and it is probably just that which is contemplated in the last paragraph, with the attribution of powers to the Commission to adopt delegated acts.

For us this is not the right solution, since it involves developments of essential aspects of the regulation, which either should be covered in this instrument itself or should be left to Member States or to Union legislation covering the sectors concerned, provided there is an adequate legal basis for such legislation.

Given the foregoing we propose the following amendments to this article.

Article 20

Measures based on profiling

1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or adversely affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, <u>location</u>, health, <u>personal preferences</u>, reliability or behaviour.

Subject to the other provisions of this regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:

(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or

(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or

(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.

Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.

4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.

5.

Article 21

No comment.

2. Chapter IV. Controller and processor

Article 22

As we will clarify while investigating the articles in this chapter, our perspective includes a substantial change of orientation in some aspects.

Some way must be found to reduce the bureaucratic/administrative workload that the current wording imposes on those involved in data processing, and at the same time to find elements of flexibility. This is on the basis of the assumption that it may be more efficient to promote or incentivise taking responsibility, organisational autonomy and accountability than trying to "ensure" results on the basis of a check based on bureaucratic and intensive supervision of those concerned.

In short, compromises have to be achieved on the basis of a cost-benefit dialogue, in which all participants should be very conscious of what they stand to gain or lose from each option proposed. Thus, with the system that we propose, a greater or lesser administrative burden will depend essentially on the decisions of the participants themselves, on the basis of clear and predictable ground rules.

The options are basically:

- to incorporate elements of added value to the organisation, which clearly increase its reliability: data protection officer or certification policy. In return this would lead to a major reduction of bureaucracy and procedures would become more flexible;
- not to incorporate added-value elements. In these cases the bureaucratic workload would be increased as the sole possible means of supervision.

On this basis, we move on to amending this article and others in the chapter under discussion.

As regards Article 22 specifically, the amendments proposed are intended to adapt this rule to the philosophy previously set out, and to leave non-applicable the Commission's right to adopt delegated acts as set out in the third paragraph, which disappears, since we find it goes beyond what is needed; for the time being we do not address the need to specify other measures, which, if they existed, should be included in the text or at most left to the legislator.

We therefore set out here the amendments proposed for Article 22:

Article 22

Responsibility of the controller

1. *The controller **may** ~~shall~~ adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.*

2. *The measures laid down in paragraph 1 shall ~~in particular~~ include**, in the cases and in compliance with the rules included in this chapter**:*

   (a) *keeping the documentation pursuant to Article 28;*

   (b) *implementing the data security requirements laid down in Article 30;*

   (c) *performing a data protection impact assessment pursuant to Article 33;*

   (d) *complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);*

   (e) *designating a data protection officer pursuant to Article 35(1), **or obtaining and maintaining certification pursuant to the certification policies defined by the Commission.***

3. *The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. Provided it is not disproportionate, **if there is no data protection officer or adequate certification,** these checks shall be carried out by internal or external auditors.*

4. *~~The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.~~*

Article 23

On this point we address some of the requests of participants consulted, in the sense that data protection by design must be considered in a flexible manner, with attention to the specificities of each sector (paragraph 1).

We would draw attention to the fact that non-compliance with this rule may be penalised and to the potential difficulties, for the penalising authority, of defining or characterising non-compliance.

In addition, insofar as the principle of minimisation again arises in a way in paragraph 2, in a way consistent with what was said in the comments on Article 5, we should make an amendment here to introduce too the idea of proportionality, which in our view is less absolute and somewhat more flexible than the concept of minimum alone.

However, we think that paragraph 2 should be reassessed on the basis of a more genuine notion of privacy by default, for which reason we have underlined it.

Article 23

Data protection by design and by default

1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement technical and organisational measures and procedures ***appropriate to the activity being carried on and its objectives,*** *in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.*

2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are ~~necessary~~ ***not excessive in quantity*** *for each specific purpose of the processing and are especially not collected or retained beyond the minimum* ***proportionally*** *necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.*

~~*3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.*~~

~~*4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).*~~

Article 24

We think that in this article, two models can quite well be considered, in a flexible framework, allowing the participants in the processing to choose between them.

One option is the joint and several liability model. Thus the data subject could exercise all his or her rights vis-à-vis either of them and it is for the participants in the processing to ensure full compliance with the obligations incumbent on them.

On the other hand, the model of distribution of responsibilities implied in the rule, is equally reasonable, although for this to concern the data subjects they need to know clearly and precisely before whom to exercise each of the rights. This necessarily leads to a series of obligations on documentation and transparency of agreements.

Thus, we think this rule deals solely and exclusively with all matters concerning the data subject's exercising of rights, but not with the substantive and procedural system of financial liability for damage, which is governed by the principle of joint and several liability in accordance with Article 77.

We therefore propose the following amendments to this article:

Article 24

Joint controllers

Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them. ***For this agreement to be valid in relation to data subjects, it must be documented and must have been brought to their attention beforehand; otherwise, the aforementioned rights may be exercised in full before any of the controllers, and it shall be incumbent on them to ensure precise compliance with the legally established benefits.***

Article 25

On this article, we think that the Commission has made a laudable effort to find a compromise solution on a matter which by its nature is not straightforward.

We agree in principle with the approach taken, although we suggest including a risk criterion in point (b) of the second paragraph, so that the article would read as follows:

Article 25

Representatives of controllers not established in the Union

1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.

2. This obligation shall not apply to:

(a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or

(b) an enterprise employing fewer than 250 persons, ***unless the processing it carries out is considered high-risk by the supervisory authorities, taking account of its characteristics, the type of data or the number of persons it concerns;*** *or*

(c) a public authority or body; or

(d) a controller offering only occasionally goods or services to data subjects residing in the Union.

3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.

4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.

Article 26

We think this article correctly regulates the situation of the processor, although two refinements are needed:

- paragraph 3 seems to us too bureaucratic. A requirement that they simply compile in writing all the instructions may amount to a disproportionate burden, especially if it also includes the instructions that follow after the contract is concluded and in the framework of the contract. In some cases the instructions may arise daily and in very large numbers. Furthermore, operational instructions will normally be sent electronically and will be quite well recorded, and, lastly, this is a matter concerning essentially the relationship between controller and processor, but which need not directly concern security or privacy. Finally, it does seem reasonable that the contractual relationship between controller and processor should be documented in any medium that remains on record – which seems to us a more appropriate formulation than the written form *stricto sensu*, which is more restricted.

- Regarding paragraph 4, we think that in some cases there could be a combination of responsibilities, which should be mentioned. Without prejudice to the point that excesses by the processor could lead it to be personally obliged and liable for the processing (*ultra vires*), the possibility cannot be discounted of failure to fulfil a duty of supervision or control (*culpa in vigilando*) on the part of the principal.
- The powers granted the Commission in this article seem to us excessive. Their content, if considered essential, should be set out in the regulation itself.

Given the foregoing, we propose the following amendments:

Article 26

Processor

1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.

*2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller**, **which shall be documented on a medium which is kept on record,** and stipulating in particular that the processor shall:*

(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;

(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;

(c) take all required measures pursuant to Article 30;

(d) enlist another processor only with the prior permission of the controller;

(e) *insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;*

(f) *assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;*

(g) *hand over all results to the controller after the end of the processing and not process the personal data otherwise;*

(h) *make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.*

~~*3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.*~~

4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24, ***all without prejudice to any liability that may be incurred by the controller in fulfilling its obligations.***

~~*5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.*~~

Article 27

No objection to this article, although as drafted it adds almost nothing new.

From the Commission's explanations, it seems that what was attempted here was to define an obligation of confidentiality on all persons (such as employees of the controller or the processor) who have contact with the data processed, for any reason. If so, the present wording is not successful and should be revised.

3. Annex

3.1. Bases for a coherent certification policy

One of the cornerstones of our position is the promotion of policies to raise the awareness and capacities of the various stakeholders in the processing of personal data, not only in order to improve quality and levels of privacy protection but also with the aim of finding formulas to allow greater flexibility in administrative and bureaucratic requirements, in favour of solutions based on responsible accountability, on the basis of which formulas can be constructed that will increase options for self-organisation and reducing red tape.
Our proposal on a certification policy is thus intended to bring to the system valuable and quickly perceptible results.
To that end we will go on to suggest the foundation for the policy in question.

3.2 Institutional participants

From our point of view the policy we are proposing should be shaped in the context of the European Data Protection Board.
Thus we can ensure that the policy in question would follow a broad consensus of the supervisory authorities of the whole Union.
It should be for the Commission to officially approve the policy subsequently. In this way, the initiative would have official status, and would be equipped with the legal mechanisms to make it compulsory throughout the Union.
The implementation phase should be the responsibility of each country's supervisory authorities. Those authorities could either directly implement the policy using their own resources or assign training and technical monitoring of the life of certifications to third parties under their supervision. Similarly, the supervisory authorities would actively work together in monitoring and evaluation programmes and in planning policies.
Along these lines, we think it would also be very important to provide this new policy with a powerful analytical and monitoring apparatus, so as to be able to continue assessing its results and impacts over time. These tasks should be responsibilities of the European Council, with the help of national supervisory authorities, with reports being sent, lastly, to the Commission.

3.3 Certification models

Under the certification policy we are proposing, two major types of certificate would be issued: (a) institutional certificates; (b) personal or operator certificates.

The institutional certificates would be addressed to organisations, administrations and businesses, and would in a way endorse the capacities and commitment of the organisation as such.

This kind of certificate would be a necessary but not sufficient condition for obtaining a substantial part of the benefits which our position links to the obtention of certifications.

The most important certifications would in fact be personal/operator certifications.

The basic aim of this type of certification would be to accredit the capacities and level of personal commitment of the person, worker or official, and would be directly connected to that person. This means that they would be completely personal and non-transferable, and would "travel", so to speak, with each individual bearer to wherever he or she was providing services at any given time.

Personal certification seems to us of extraordinary importance, since it is the type of certification where the quality of work of each factor of production in a given organisation is definitely endorsed.

Personal certification should maintain an equilibrium between technical and legal competences, seeking a multidisciplinary profile in line with the new challenges. That balance could vary according to the type of certification, its aims and the level of cover.

It could be concluded in a way that institutional certification would be more focused on resources and organisation, while on the contrary personal certification would be focused on capacities, skills and awareness.

In any case, all certification would be subject to strict evaluation and analysis processes, both at the time when they are issued and in order to be maintained.

3.4 Characteristics of the certifications

In the framework of the proposed policy, certifications, in their various forms, would have the following characteristics:

(a) Strict issuing conditions. To obtain certification would require passing a series of objective tests, designed to accredit fulfilment of all parameters linked to the way those tests were defined. The content of the tests, and thus of the preparatory programmes or courses, would have to suitably combine legal and technical elements, weighted variably according to the type of certification and the personnel or institution to which they were geared.

(b) Time-limited character. All certifications would have limited periods of validity, varying depending on the type of certification. Before this time limit expired, it would have to be renewed, for which the necessary tests would be established for purposes of objectively accrediting the retention or upgrading of the personal or institutional capacities tied to the certification concerned.

(c) Revocability. All certifications may be revoked as a consequence of significant cases of non-compliance. The definition of non-compliance and the procedures for revocation would be defined in the regulation itself, in which powers of provisional revocation would also be established.

(d) Flexibility. In the general definition of the certifications policy, a wide enough range of certifications should be established to permit the various operational necessities to be covered. The starting point would be that only those capacities that were genuinely necessary for a given type of processing should be certified. Nobody should be obliged to be certified for activities not falling within the definition of his or her corporate or institutional duties. This should lead to a significant cost reduction for certifications.

(e) Quality. The certification policy should meet quality criteria. To that end, design and use quality control programmes would be developed.

(f) Planning. The certification policy should be in a position to give suitable responses to a constantly changing reality. To that end, a planning and development team should be organised, for the purpose of detecting new needs and proposing functional and efficient responses to them in policy terms.

FRANCE

I. General comments on the proposal for a Regulation

To begin with, the French delegation would point out that for all the articles in the Regulation, and particularly for those to which this note refers (Articles 11 to 27), at this stage we have considerable reservations on the use of delegated acts and implementing acts. This is a general remark which will not be systematically repeated in the article-by-article comments in the second part of this note.

In addition, we support the Presidency's desire to organise a thematic discussion and are therefore reserving our comments on reducing the administrative burden, delegated acts and implementing acts, and the areas in which Member States would like more flexibility for the public sector, and we will include them in our reply to the questionnaire from the Presidency in 12918/12.

We would also reiterate our desire to have the proposal for a Regulation take full account of the special features of the arrangements for archives, particularly public archives. While we support the Regulation's objective of ensuring uniform treatment throughout the Union with a high level of personal data protection, that objective should not result in disruption of the archives held by the Member States (which would be detrimental to the citizens of the Union) by making insufficient allowance for the constraints inherent in archiving. We therefore share the wishes expressed by other delegations and take the view that there should be a thorough process of consideration in order to ensure a proper fit between the rules on personal data protection and the rules on archiving.
The decision to use a regulation, for reasons of legal certainty, posits greater clarity at the European instrument stage.

II. Comments by the French delegation on the proposal for a Regulation, Article by Article

Article 11 - Transparent information and communication

In paragraph 2, we would like the obligation to adapt the information to the data subject to be moderated to take account of the resources available to the controller by inserting the words "*by all reasonable means*" after "*adapted to the data subject*".

We would also stress that targeting information in this way will, of necessity, involve specific data processing the relevance of which could be open to discussion, where it is likely to be particularly intrusive.

We also ask the Commission to state when this obligation would apply (only at the time of collection or at the time of each new processing operation?).

Moreover, we would like it to be possible to meet the obligation to inform the data subject, as set out in paragraph 2, by providing information on a digital portal.

In support of these requests, we would point out that forwarding information to the data subject at the time of each new processing operation is hardly compatible with the reduction in the administrative burden which the proposal for a Regulation seeks to achieve.

Article 12 - Procedures and mechanisms for exercising the rights of the data subject

In relation to paragraph 2, we would repeat our perplexity about the meaning of the word "*cooperation*" (between "*several data subjects*"); it is probably a translation error[1].

[1] [Translator's note: the English and French texts correspond.]

Article 13 - Rights in relation to recipients

The French delegation has no comments.

Article 14 - Information to the data subject

In line with our comments on Article 10, we would like a provision in Article 14 to the effect that the intermediary controllers whose data processing is for the same purposes as the processing by the initial controller who collected the data should be exempt from the obligation to provide information.

Likewise, in line with our comments on Article 11(2), we would stress that we need to know how the information is to be provided before we can express an opinion on the content of the right to information.

In paragraph 1(b), to be consistent with our comments on Article 12(2), we would like the phrase "*including the contract terms and general conditions*" to be replaced by "*including **access to** the contract terms and general conditions*" in order to make it clear that the controller must inform the data subject of the existence of the contract terms and general conditions and the means of access to them but does not need to supply those terms and conditions when implementing the right to information.

In point (c), we would reiterate our concerns regarding the arrangements applicable to archives and the need to lay down special arrangements for such data processing. We would like this provision to be amended to stipulate that archives are not affected by this obligation to inform data subjects of the period for which data will be stored.

In paragraph 1(g), we wish to have the word "*intends*" ("*that the controller intends to transfer to a third country or international organisation …*") replaced by "*wishes*", that being a more appropriate term.

In relation to point (h) we would stress that, as it is currently worded, we cannot support such a vague provision. Until such time as a clearer and more restricted draft is produced, the French delegation is therefore entering a scrutiny reservation on this point.

In paragraph 3, we wish an exception to be made where the processing relates to data from sources accessible to the public. We would suggest the following wording:

"*Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate****, except where such data originates from sources accessible to the public***."

We also wish to have an exception to the right to information in relation to the professional press. However, since the article specifically relating to the press has not yet been discussed, it is too early to make a proposal at this stage.

We are not in favour of the provision in paragraph 4(b) to the effect that information is to be provided at the time of the recording or *within a reasonable period* after the collection.
The controller should not be given the power to *decide on the period* within which the data subject must be informed of the use of personal data.

We also consider that the division of responsibilities between the controller disclosing the data and the controller receiving the data disclosed needs to be clarified. The fact is that the controller receiving the data may not necessarily be informed of the details of the data subject or of the origin of the personal data disclosed.

Also in connection with paragraph 4(b), we are still awaiting information about how this provision is to be aligned with Directive 2006/123/EC on services in the internal market.

With regard to paragraph 5(b), we support the proposed wording attached to the correspondence from the Chairman of the Working Party on Statistics, which also appears in Article 11(2) of Directive 95/46/EC and, subject to deletion of the word "research" (proposal accepted by the Presidency for Article 5(b) in 11326/12), we agree that it should be used in the proposal for a Regulation:

"*(b) the data are not collected from the data subject and the provision of such information, in particular when processing for historical, statistical, or scientific purposes, proves impossible or would involve a disproportionate effort; or"*

In line with our request regarding paragraph 3 (which relates only to data not collected from the data subject), we wish to add a new point (e) to ensure that the controller is not charged with forwarding data already available to the public:
"*(e) the data come from sources accessible to the public*".

We also support the second request from the Chairman of the Working Party on Statistics regarding the insertion of a new paragraph 5A creating an exception to the right accorded to the data subject in paragraph 1(d) where data are collected for historical, statistical, or scientific purposes.

Subject to the same condition that the word "research" be deleted, we also support the Presidency compromise and would like the following paragraph to be inserted:

"*5A. Paragraph 1(d) shall not apply where data are collected for historical, statistical, or scientific purposes and the conditions in Article 83(1A) are met."*

Article 15 - Right of access for the data subject

In relation to paragraph 1, we would ask to have it stipulated that the data subject provide the controller with proof of his/her identity. This request is all the more logical in that we supported the inversion of the definitions of "*personal data*" and "*data subject*", as they appear in Directive 95/46/EC.

In relation to point (d), we would reiterate our concerns regarding the arrangements applicable to archives and the need to lay down special arrangements for such data processing. We want it stipulated that archives are not affected by the obligation to inform data subjects of the period for which data will be stored.

In relation to paragraph 1(g), we would draw attention to what seems to be a translation error resulting in the use of the expression "*en cours de traitement*" for "*undergoing processing*". The current wording of the provision is open to interpretation and should be reviewed. It raises doubts, for example, as to whether or not historical data (which may have been archived) or future processing operations are included. Moreover, in the interests of clarity the words "*communication of the data*" should be replaced by "*the data*".

We also support the request from the Chairman of the Working Party on Statistics to add a new paragraph 5 to this Article creating an exemption from the data subject's right of access to data processed only for historical, statistical, or scientific purposes, worded as follows (i.e. without the term "research"):

"*5. The rights provided for in Article 15 do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1A) are met."*

Article 16 - Right to rectification

We also support the request from the Chairman of the Working Party on Statistics to add a new paragraph 2 to this Article creating an exemption from the data subject's right of rectification in relation to data processing carried out by the controller only for historical, statistical, or scientific purposes, worded as follows (i.e. without the term "research"):

"*2. The rights provided for in Article 16 do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1A) are met."*

Article 17 - Right to be forgotten and to erasure

We support this provision since it creates a useful reinforcement of the rights of data subjects whose data are collected on line.

We would nevertheless point out that several points in this article need further specification. We wonder, for instance, about the impact of this provision on companies' economic activities; perhaps a distinction should be made between access to data on the internet and access on other media.

We also consider that paragraph 1 is only a partial solution to the problem of social media. The proposal for a Regulation does not clearly enable data subjects to request the erasure of data put on line by a third party. Yet we attach great importance to recognition of the right to be forgotten being applicable, regardless of who put the data on line, and also to making sure that it does not represent a backward step regarding data subjects' rights outside the digital sphere.

In relation to paragraph 2, we also wonder about the apparent sharing of responsibility between the controller and third parties of which we would like further details, particularly as regards serial publication by different third parties. We have doubts as to whether this obligation is technically feasible.

In relation to paragraph 4, we would like further details of the option accorded to the controller to "restrict" data and the fact that that option means that he can block the data.

In relation to paragraph 4(a), which enables the controller to restrict the processing of personal data instead of erasing them "*for a period enabling the controller to verify the accuracy of the data*", we would point out that the inaccuracy of the data is not expressly listed as one of the grounds enabling the data subject to request erasure. This point should therefore specify the cases to which it refers.

In relation to paragraph 4(c), we would like to have examples of cases in which this provision would apply. As it now stands, it seems misplaced and should therefore be deleted.

More generally, we would like clarification of the relationship between the data subjects' "traditional" rights (right of access, right to rectification and right to object) and the "new" rights created by this Regulation (right to be forgotten).

In relation to paragraph 8, which prohibits the controller from processing data once they have been erased, we await clarification of what becomes of data to which the right of erasure applies: are they deleted or are they overwritten? Or is the access path to them simply invalidated or deleted?

Article 18 - Right to data portability

We are in favour of this new right which enables data subjects to move their personal data into another application.

However, insofar as portability is part of the service offered, we would stress that it could be problematic. We should like details of the relationship between this right and the right of competition and intellectual property rights. For example, we consider that this right appears above all to be intended to be implemented in the digital sphere and that it could therefore create discrimination between the obligations imposed on "traditional" traders (who might not have the obligations relating to the right to data portability imposed on them) and e-traders (who seem to be the main targets of Article 18). Such an administrative burden on those involved in electronic trading does not seem to be compatible with the priorities identified by the Commission, particularly completion of the digital single market.

We also wonder about the scope of this Article in relation to processing by persons having a public service mission. We would refer in particular to medical data. In that area, the portability of data should not create any obstacle to the implementation of the obligations devolving upon health professionals (e.g. continuity of care) nor should it interfere with ongoing research or with public health. Simply withdrawing data from the system would be prejudicial to the interests of health professionals who could face liability issues and not be able to retain the information relating to their activities.

In relation to paragraph 2, we would query the objective of the provision and the relationship between the right to data portability and intellectual property. We would stress that while we have no difficulty with the principle of portability of "raw" personal data, we do, however, have serious reservations about applying that right to data resulting from intermediate processing. In the case of such personal information, intellectual property rules act as a justifiable brake on the implementation of the right to data portability. And indeed the same applies to the exercise of the right of access.

Moreover, the last phrase in paragraph 2 raises questions about the scope of the obligation imposed on the controller from whom the data are withdrawn to cause no hindrance . The current wording is not sufficiently precise as regards the responsibility of this "initial" controller, particularly where the data being reused are inaccurate. We should therefore like this provision to include a proviso preventing disproportionate effort on the part of the controller from whom data are withdrawn.

We also wonder about what is covered by the term "*structured format which is commonly used*": does the right to data portability cover only personal data or does it extend to databases more generally? If the latter is the case, then the relationship between this provision and the Directive on the legal protection of databases needs to be specified.

In relation to paragraph 3, we would query the scope of the power given to the Commission to specify the electronic format for data transfer. In addition to the competition law questions imposing such an obligation raises, it would obviously involve expenditure which needs to be evaluated before the provision is adopted, in the light of the wide variety of formats available. We would therefore suggest that, instead of imposing a single format on all controllers, the Regulation specify criteria to be met by the formats used in order to ensure the highest possible level of portability.

We also support the request from the Chairman of the Working Party on Statistics to insert a new paragraph 4 in this Article creating an exemption from the right to data portability in the case of data processed only for historical, statistical, or scientific purposes, worded as follows (i.e. without the term "research"):

"*4. The rights provided for in Article 18 do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1A) are met."*

Article 19 - Right to object

In paragraph 1, the data subject "*shall have the right to object, **on grounds relating to their particular situation**, at any time to the processing of personal data (…)*". We wish to have the "*grounds relating to their particular situation*" defined.

The same paragraph provides that where the controller "*demonstrates **compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject***" the data subject's right to object is over-ruled. Leaving aside the specific features of "public" records, we find it difficult to see what compelling legitimate grounds a company or other private individual would invoke to counter the data subject's fundamental rights. We therefore consider that the only case in which the right to object may be over-ruled is when the controller is carrying out a public service mission or a mission in the public interest.

In paragraph 2, we want confirmation of the exact meaning of the term "*marketing direct*" (in English "direct marketing") and an assurance that it covers the concept of "*prospection commerciale*" (marketing carried out commercially) referred to in Directive 95/46/EC. In any event, we want the limitations on the right to object to cover all types of marketing, not just marketing for commercial purposes.

We also wish to be sure that the new Regulation retains the system in Directive 95/46/EC whereby the data subject has an opt-out from direct marketing. We are, in fact, worried about the risk of extending an opt-in system (which now exists only for electronic data processing) to all data processing.
We also support the request from the Chairman of the Working Party on Statistics to insert a new paragraph 4 in this Article creating an exemption from the right to object in the case of data processed by controllers only for historical, statistical, or scientific purposes, worded as follows (i.e. without the term "research"):

"4. The rights provided for in Article 19 do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1A) are met."

Article 20 - Measures based on profiling

We would reiterate that there needs to be consistency between this Article and the solutions already adopted in the Directive on privacy in the electronic communications sector (Directive 2009/136/EC), particularly the arrangements authorised for obtaining consent in automated communication systems.

We would also point out that it is simpler and more appropriate to insert a definition of profiling in Article 4 of the proposal for a Regulation and have Article 20 deal only with the arrangements for profiling. On this point, we support the request made by the Austrian delegation at the meeting of the Working Party on Information Exchange and Data Protection (DAPIX) on 3 and 4 September 2012 to use the definition of profiling adopted by the Council of Europe in Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling:

"*'Profiling' means an automatic data processing technique that consists of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.*"

In paragraph 3, we consider that the term "solely" has quite the opposite effect, enabling controllers to apply profiling to sensitive data where they are combined with "normal" data. If that is what the Commission intends, we feel that there should be stricter safeguards.

Article 21 - Restrictions

We wonder about the scope of the measures which may be introduced under national legislation to "*restrict (…) the scope of the obligations and rights*", and particularly about the data to which such measures might apply.

In relation to paragraph 1, which contains a list of restrictions to the rights and obligations provided for in the Regulation, we are not in favour of the reference to Article 5 in the introductory phrase since, in our view, the general principles on the protection of personal data (set out in Article 5) must apply, whatever the nature of the processing. For instance, it seems contrary to the principle of data subject privacy to collect personal data in a manner disproportionate to the purpose of the processing.

In relation to paragraph 1, we would also point out that points (a), (b), (c) and (d) do not include public health. That means that the obligation imposed by French law on doctors and public and private clinical biology services and laboratories to forward individual data to the health authority (Article L.3113-1 of the Public Health Code) would not be permitted under this Regulation. We therefore consider that that exception should be added to the list of areas in which Member States may provide for restrictions.

In relation to paragraph 1(a) and (b), which refer to "public security" and "the prevention, investigation, detection and prosecution of criminal offences", we would request clarification of how these two points relate to the proposal for a Directive since they fall within its scope rather than within the scope of the Regulation.

In paragraph 1(c), we request that the term "intérêts **publics**" be used in the French text instead of "intérêts **généraux**" in order to reflect the English term "*public interests*".

In the same point, we also want it made clearer that the processing of tax data is one of the areas in which it is possible to restrict the obligations and rights provided for in Article 5(a) to (e), Articles 11 to 20 and Article 32.

As a matter of substance, we also request that statistics be added to the list of areas for which derogations can be made.

In paragraph 2, we wish to have it specified that any legislative measure referred to in paragraph 1 should contain, in addition to the specific provisions as to the objectives to be pursued by the processing and the determination of the controller already stipulated, provisions on the period for which the data are stored and on the categories of personal data processed. This paragraph should also include the notion of "categories" of processing, making it possible to take account of the extent of the risk to privacy and to set specific limits for whole categories of processing (containing processing operations having the same purpose), particularly data processing for sovereign State purposes, e.g. tax records or data processing in the health sector. In practice, it does not seem conceivable for the legislator to intervene for every data processing operation.

We therefore propose that the following text should be substituted for this paragraph:
"*In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions as to the processing or categories of processing concerned which take account of the extent of the risk to privacy represented by those forms of processing and of the scope of the restrictions introduced.*"

We would reiterate what we said in our earlier comments on Chapters I and II of this proposal for a Regulation, i.e. that we are absolutely opposed to having this instrument impose the form of national measures to be adopted, whether a law or a regulation.

Chapter IV - Controller and processor

Article 22 - Responsibility of the controller

As a preliminary remark, we wonder about the implementation of this Article in relation to some activities, particularly those of members of the professions who collect sensitive data as part of their work (e.g. health professionals). In general, the obligations listed seem too general and ill-suited to the diversity of controllers and of data processed (sensitivity of data should be taken into account as a criterion). In any event, the obligations listed in Article 22 seem to be designed for large companies, i.e. those having the technical and financial resources to comply with these provisions. We would point out that recital 11 of the proposal for a Regulation refers to Commission Recommendation 2003/361/EC concerning the definition of micro, small and medium-sized enterprises. That Recommendation refers to three criteria: staff headcount, turnover and degree of autonomy (whether or not the enterprise belongs to a group), and not just to the number of employees.

Although European statisticians have classified enterprises on the basis of these criteria, that classification is generally subject to statistical confidentiality and is therefore not available to non-statisticians.

In any case, even if the classification were to be made public, it could not be invoked in law, nor could it be used for the application of a regulation. And it does not appear that there is any such classification in France which would have legal effect.

Hence, if the Regulation contains this kind of derogation, it will be difficult for anyone other than the controller to prove compliance with it (and he might even have difficulty in the event of indirect checking by an unknown party).

In conclusion, the use of this type of criterion is likely to give rise to considerable difficulties in application. We would also point out that the size of the enterprise is no guarantee that the processing of data does not represent a risk.

In paragraph 1, the term "*policies*" is vague and needs to be made more specific.

In paragraph 2, in the interests of parallelism, we would like to add a point (f) providing that the controller is required to keep the acts provided for in Article 24 (which defines the responsibilities of the controller and the processor respectively) and Article 26(2) (contract binding the processor to the controller).

In the same paragraph, the words "*in particular*", which indicate that the list is not exhaustive, should be deleted.
We are entering a scrutiny reservation on paragraph 2(c) since the article it refers to, Article 33, does not provide enterprises with sufficient legal certainty; it contains a non-exhaustive list ("*in particular"*) of processing operations presenting "*specific risks*" and that does not enable the controller carrying out his obligations under Article 22 to decide whether or not the processing presents a sufficient risk to require an impact assessment.

In relation to paragraph 3, we have a query about the "*independent internal auditor*". Will he be the subject of specific certification?

We would also emphasise that there is no justification for systematic auditing. As in the case of impact assessments, we wish to have the decision to audit taken on the basis of the nature of the processing or the risk it presents. The criterion of proportionality should also be specified in the Regulation and not in a delegated act.

In relation to paragraph 4, we would emphasise that the risks presented by data processing do not depend on the size of the enterprise and there is therefore no justification for empowering the Commission to adopt delegated acts containing specific measures for micro, small and medium-sized enterprises.

Article 23 - Data protection by design and by default

As the text now stands, we wish to **enter a scrutiny reservation** on this Article, pending further information on several points.

We would like further details of the meaning of the term "by default" in the title and in the body of Article, and of the mechanisms to be implemented to protect data from the time they are created, the real practical obligations of controllers and the penalty for failure to meet those obligations. We would also like to know why this Article applies only to the controller and not to the processor, since it may be the processor who defines the processing methods without any intervention by the controller.

As a general comment, we would stress that these provisions should be reworded in such a way as to recommend and encourage controllers and suppliers of software to adopt the approach it describes, in the same way as Article 39 encourages certification.

In paragraph 1, we wonder what exactly the term "*means of processing*" is intended to cover and would like clarification.

The provision in paragraph 2 on implementing mechanisms for ensuring that, by default, only those personal data are processed which are necessary for the purpose of the processing seems superfluous at first sight, in view of the minimisation obligation set out in Article 5. The relationship between this paragraph and Article 5 should therefore be clarified, particularly as regards data stored for historical or scientific purposes for longer than is necessary for the purposes for which the data were collected. We would query the meaning and scope of several expressions in this paragraph. We would thus like an explanation of the meaning of the following phrases: "*not collected or retained beyond the minimum necessary for those purposes*" (this should be amended to make provision for archives), "*both in terms of the amount of the data and the time of their storage*" and "*to an indefinite number of individuals*".

Article 24 - Joint controllers

An addition could be made to this Article obliging controllers to make data subjects aware of their respective obligations and the obligations of their processors so that they know who the competent controller is depending on the rights they wish to invoke.

The system of sharing responsibility between controllers and processors seems unclear and needs to be clarified. We also consider that it would be worth clarifying the arrangements for the processor and bringing them all together in one article.

Article 25 - Representatives of controllers not established in the Union

To begin with, we would reiterate our queries about the application of this Article to airlines; we consider that the specific features of that sector should be taken into account, particularly in relation to international flights involving transit, which may or may not be carried out under code sharing. We would repeat our example of flights between Paris and Manila on Air France and Cathay Pacific. For the second section of the flight, between Hong Kong and Manila, we wonder how and by whom the data relating to that section would be forwarded. [The heavy-handed arrangement proposed, particularly the provision in Article 25 requiring compulsory designation of a representative by the controller, could interfere with the development of international trade (sale of air tickets).][1] By the company in Manila which has no representation in France or by the French company which might well have difficulties to overcome in order to sell tickets? Moreover, making the designation of a representative compulsory would toughen the present procedure and could have an impact on international air travel. While the obligation to designate a representative does not apply where the third country ensures an adequate level of protection, is there not a risk that insufficient protection could make it impossible to operate flights to third countries, thus creating a barrier to the air transport business? Many companies do indeed fly to countries which do not have an adequate level of data protection. And airlines can be set up and dissolved so quickly as to be incompatible with the period required to obtain a decision on whether protection is adequate. If this system were to result in limiting the number of flights, the risk of reprisals would not be insignificant.

In relation to paragraph 1, we would like the arrangements for designating the controller's representative and the nature of his mandate to be set out in the proposal for a Regulation itself. We would also like the Regulation to impose an obligation to inform the national data protection supervisory authority of the contact details of the controller's representative. Unless that information is provided, control could not really be effective.

[1] [Translator's note: This sentence appears to be wrongly placed in this paragraph in the original French.]

The exception in paragraph 2(b) relating to the number of employees should either be deleted or amended since, as we have already pointed out, the criterion is not relevant because only statistical bodies have access to such data.

Moreover, in the light of paragraph 2(a) which exempts enterprises in third countries which the Commission has decided ensure an adequate level of protection, applying the criterion in point (b) would mean that enterprises employing fewer than 250 persons in third countries for which no decision had been taken would be able to process data relating to European nationals without any obligation to designate a representative in the EU, therefore potentially without any avenue of effective control of the processing.

In relation to the same paragraph, we also wonder which supervisory authority is responsible where there is no representative.

Article 26 - Processor

In paragraph 1, we want clarification of the "*sufficient guarantees*" to be provided by the processor. We should also like to delete the link between these guarantees and compliance with the Regulation.

In paragraph 2, we want clarification of the meaning of the term "*other legal act*".

In point (e), we also want clarification of the situations to which the phrase "*insofar as this is possible given the nature of the processing*" refers.

In relation to point (g), we would point out that the wording seems to be based on the idea that the processor has retained personal data after the purpose of the processing has been accomplished, although not authorised to do so. The wording should leave no doubt that after processing the processor must destroy the personal data received for processing. Such clarification would also make it easier to interpret the link between this point and paragraph 4 of the same Article in order to determine the scope of the data covered by that paragraph.

We propose the following draft:
"*hand over all results to the controller after the end of the processing and ~~not process the personal data otherwise~~ undertake to destroy all the data in its possession without delay;*"

In point (h), we think it would be desirable to remove the obligation on the processor to contact the supervisory authority directly and ensure that he can only do so through the controller.
Moreover, in our view that obligation duplicates the obligation in Article 29(1).

In Article 26(3), we would point to a difference between the French and English versions which needs to be corrected. The French version has "*conservent une trace documentaire*" ("shall keep a written record") while the English version has "*shall document in writing*".

In paragraph 4, the reference to Article 24 should be deleted. If a processor processes personal data other than as instructed by the controller, that controller cannot, by definition, be considered as joint controller. Moreover, this paragraph makes the processor who processes personal data other than as instructed by the controller a personal data controller without making any reference to the fact that such behaviour is in breach of the processor's contractual obligations. On the surface, such a provision appears to be favourable to the data subjects but in fact it encourages unlawful behaviour by processors. We therefore have reservations on this paragraph.

We would also point to the difficulty in relating the provisions in Article 26(4) to those in Article 27. Article 27 provides that "*the processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law*". Yet Article 26(4) opens the way for the processor to process "*personal data other than as instructed by the controller*".

In paragraph 5, the proposal for a Regulation empowers the Commission to adopt delegated acts for the purpose of further specifying the processor's responsibilities, duties and tasks. In addition to our general comments on delegated acts and implementing acts, we consider that this Article also raises the question of whether a subsidiary of an enterprise is to be considered as a processor.

Article 27 - Processing under the authority of the controller and processor

We would query the meaning and scope of this Article and particularly its role as a mechanism for resolving conflicts of national law.
We are also concerned about its relationship with the one-stop shop put in place by the Regulation. The last phrase in the Article, "*unless required to do so by Union or Member State law*", requires clarification since it raises, for instance, the question of how the legislator is to determine the processor and of whether the controller's consent would nevertheless be required. Such designation by law should perhaps be deleted. This provision would in fact enable the legislator to force the controller to work with a processor he had not chosen and over which he had no authority either; yet the Article does not stipulate whether the data security and confidentiality requirements would be maintained when this provision is applied. That could lead to conflict between the controller and a processor whose legitimacy came not from appointment by the controller but from the legislator. Moreover, it would be necessary, at the very least, to have the controller informed when a processor was processing data on the instructions of a Member State legislator instead of the controller's instructions.

IRELAND

Article 11 (Transparent information and communication)

1. The transparency principle is already set out in article 5(a).

2. While appropriate for data controllers operating on-line services, the practical implications of article 11(1) for other controllers are far from clear. What should “transparent” policies cover? Does “easily accessible” mean that the policies must be publicly displayed? Would it not be sufficient that the controller be required to be in a position to make the policies available if requested by a data subject?

3. In the case of SMEs, are controllers required to have detailed policies dealing with the personal data of staff (including family members), suppliers and customers? In the case of an individual, how is the requirement intended to apply to social networking activities?

4. Article 11.1 will impose excessive administrative burdens and unnecessary compliance costs in cases where the risk of data misuse is remote. It should be deleted. Article 38.1(d) already foresees the possibility of a code of conduct in relation to "requests of data subjects in exercise of their rights" and this is sufficient.

5. Article 11(2) is also far reaching. The requirement to supply information and any communications in clear and plain language is accepted but the requirement to *adapt* any information or communication to the data subject could be very onerous, possibly requiring translation into another language. The words “adapted to the data subject” should be deleted. Also, the obligation on the controller should be to take “appropriate measures” to respond to the data subject.

6. Finally, the relationship between articles 11 and 14 needs to be clarified.

Article 12 (Procedures and mechanisms for exercising the rights of data subjects)

7. The content of article 12.1 should be relocated to article 11.1. (i.e. the procedure should come before the requirement to provide responses in clear and plain language).

8. As regards article 12.2, the proposal to allow an additional month for the controller to respond in cases where "cooperation [of data subjects] is necessary to a reasonable extent" introduces uncertain elements. It would be preferable to avoid time limits and to continue to require the controller to inform the data subject "without excessive delay" (i.e. as in the current Directive).

9. While we support placing an obligation on the controller to inform the data subject of the possibility of lodging a complaint with a supervisory authority in article 12.3, we do not support the requirement to provide information on judicial remedies. The words "and seeking a judicial remedy" should be deleted.

10. We are unhappy with the "free of charge" proposal in article 12.4; the existing possibility to impose a modest charge should be retained in order to encourage 'bona fide' requests.

Article 13 (Rights in relation to recipients)

11. The title of this article should refer to the "obligations" rather than "rights". The term "third parties" which appears in the corresponding article 12(c) of the Directive should be used instead of "recipient".

Article 14 (Information to data subject)

12. This confusing article seeks to merge the content of article 10 (Information in cases of collection of data from the data subject) and article 11 (Information where the data have not been obtained from the data subject) of the Directive. It would be preferable to retain separate articles in the Regulation, even if this would require some repetition of text.

13. In article 14.1, the quantity of information to be provided to data subjects is excessive in the case of 'low risk' processing operations, e.g. reserving a table in a restaurant or making an appointment with the hairdresser. This applies in particular to paragraphs (d) and (e).

14. Paragraph 1(c) should be dropped. Moreover, paragraph (h) introduces an element of uncertainty and instability and should be dropped.

15. The obligations which are intended to apply under paragraphs 5(b) and 6 need to be clarified.

Article 15 (Right of access for the data subject)

16. In paragraph 1, the term “at any time” should be replaced by “at reasonable intervals”.

17. Paragraph 2 should state simply: “The information may be provided in electronic form unless otherwise requested by the data subject” (Duplication between this paragraph and the last sentence of article 12.2 needs to be addressed).

18. The data controller should have a right to verify the identity of a data subject, at least in cases of reasonable doubt.

Article 16 (Right to rectification)

19. The second sentence should read: “The data subject shall have the right to obtain completion of incomplete data, including by means of providing supplementary information.”

Article 17 (Right to be forgotten and to erasure)

20. In paragraph 1, the scope of what is meant by the data subject having a right to the erasure of personal data “relating to them” is unclear; does this refer to personal data provided by the data subject or include also personal data of a group of data subjects, including that of the data subject concerned, in a shared workspace? It would be preferable to drop the words “and the abstention from further dissemination of such data, especially in relation to personal data”.

21. In paragraph 2, an obligation is placed on a controller who has made the personal data public to take reasonable steps to inform any third parties processing the data concerned of the data subject’s request to erase the data. However, controllers are not in a position to supervise all internet users (as already recognised in the eCommerce Directive). There is a clear difference between making personal data available to an unspecified number of persons online and making it available to a limited number of identifiable third parties. It would be more realistic to oblige controllers to erase personal data which are under their control, or reasonably accessible to them in the ordinary course of business, i.e. within the control of those with whom they have contractual and business relations. This would require them to have adequate mechanisms in place to locate and erase data in response to data subject requests. The final sentence of paragraph 2 needs to be considered further.

22. It would be contrary to the data minimisation principle in article 5 if compliance with this article were to lead to increased data retention so that controllers could demonstrate compliance with 'right-to-be-forgotten' requests.

23. The right to freedom of expression – referred to in paragraph 3(a) and acknowledged in recital 121 – is welcome, especially important where data are stored in audiovisual and news archives.

24. It is essential that paragraph 3 be extended to allow controllers to retain data in order to comply with legal, regulatory and anti-fraud obligations and that this also be explicitly acknowledged in recital 53.

25. The second sentence of paragraph 3(d) should be deleted (as in article 6.3).

26. The contents of paragraph 4 to 7 should form the core of a new article entitled "Right to be forgotten and to restriction of processing". The existing concept of 'blocking' would be an acceptable alternative to 'restricting'.

Article 18 (Right to data portability)

27. It is not clear whether and, if so to what extent, this is intended to apply to public authorities. This should be clarified.

28. Intellectual property rights of data controllers, and any data which may be commercially sensitive for controllers, e.g. underwriting criteria in the case of insurance companies, must be protected under this article.

Article 19 (Right to object)

29. If this right is intended to apply to public authorities, it needs to be reconsidered. Also, does "compelling legitimate ground" represent a higher threshold than the grounds set out in article 6.1(d), (e) and (f). Clarification is required.

30. As regards restrictions on direct marketing activities, the campaigning actions of political parties and individuals seeking election to political office, which are essential features of democratic political systems, must be protected.

Article 20 (Measures based on profiling)

31. In paragraph 1, the reference to "measure" is unclear and should be replaced by "decision". It would be helpful to clarify further what is meant by a measure which "significantly affects" the data subject (this term is in the existing Directive but further clarification is necessary because of the enormous penalty referred to in article 79.6 (d)). Use of the term "in particular" in paragraph 1 is unacceptable in light of the level of penalty which applies to infringements.

32. Further consideration must be given to whether this article should generally to individuals or to data subjects.

33. This article does not appear to distinguish between profiling for potentially beneficial purposes (e.g. seeking to satisfy consumer demands for goods or services) and potentially detrimental purposes (e.g. discrimination in the provision of services such as insurance or financial products). An appropriate balance which protects individuals from harmful profiling while safeguarding innovation and promoting the digital economy is required.

34. In paragraph 2 (a) it is not clear what the words "has been satisfied" refers to. In paragraph 2 (c), it is not clear why suitable safeguards are required in addition to those in article 7.

35. It is essential that paragraph 3 continues to permit profiling by relevant public authorities for the purpose of promoting tax compliance or combating fraud. It should also remain possible to take criminal convictions into account when assessing risk (e.g. convictions for traffic offences in determining car insurance premiums) or in determining sanctions for repeat offences.

36. Article 8 of the Consumer Credit Directive (Directive 2008/48/EC) requires creditors to assess the consumer's creditworthiness on the basis of sufficient information "where appropriate obtained from the consumer and, where necessary, on the basis of a consultation of the relevant databases." Will article 20 impact on the operation of this Directive?

Article 21 (Restrictions)

37. Careful drafting is required to ensure that the overall objective of greater harmonisation of data protection standards is not undermined. Paragraph 2 needs to be clarified.

Article 22 (responsibility of the controller)

38. Paragraph 1 appears to repeat the content of article 5(f). The obligations foreseen in paragraph 2 are onerous, appear to apply to all controllers irrespective of level of risk of misuse and will be costly to implement.

Article 23 (Data protection by design and by default)

39. In addition to "the state of the art and the cost of implementation" referred to in paragraph 1, the "risk of misuse of the personal data" must be taken into account when determining what measures and procedures are appropriate.

40. The 'default' obligation in paragraph 2 would require controllers to process only data which are necessary for each specific purpose of the processing. It remains unclear what this new obligation requires in the case of social networking sites which are specifically intended to facilitate the sharing of personal data.

41. The proposal in paragraph 3 that the Commission be empowered to specify "appropriate measures and mechanisms" for data protection by design requirements across sectors, products and services <u>risks undermining the principle of technology neutrality and stifling product innovation</u>. Paragraph 3 should be deleted (see earlier comments in respect of Article 86).

Article 24 (Joint controllers)

42. While the principle seems appropriate, it is not clear how responsibility for compliance will operate in practice, especially if one of the controllers is established outside the Union.

Article 25 (Representatives of controllers not established in the Union)

43. The obligation to designate a representative in the Union applies in certain cases where article 3.2 applies. However, it raises the question of what exactly is meant by "the offering of goods and services" to data subjects in the Union. Is "offering" intended to refer to active marketing or targeting of goods and services at Union data subjects, or does it also cover cases where there is no such activity but there is a web site which, in theory, could be used by a data subject in the Union? This needs to be clarified.

Article 26 (Processor)

44. Paragraph 1 is long and confusing. The text after "… this Regulation" should be deleted.

45. In paragraph 2, the requirement that processing operations be governed by a contract or other binding legal act is welcome. However, the obligations are too specific and there is a risk of reducing the accountability of the controller.

46. Paragraph 2(c) requires the processor to take all the security measures required by article 30; there is no need, therefore, for paragraph (b) and it should be deleted. It is not clear why paragraph 2(d) specifies that the contract must provide that the processor shall obtain the prior permission of the controller before involving a sub-processor. Is this not a matter for the controller (who is ultimately accountable for compliance) and the processor?

47. The meaning of "hand over all results to the controller at the end of processing" in paragraph 2(g) is unclear and requires explanation or deletion. The same applies to the new obligation on the processor in paragraph 2(h) to provide information to the supervisory authority.

What is paragraph 3 intended to mean? Does it mean that the contract must be in writing? If so, paragraph 2 could specify that the contract must be in writing. If not, there is a risk of excessive documentation.

ITALY

Chapter III: rights of the data subject

The whole chapter appears to be lacking any systematic structure: before laying down provisions on the mechanism for exercising rights (currently contained in Article 12), it would be better if the provisions on information (currently in Article 14) were inserted after Article 11, followed by the articles on the rights of the data subject (currently Articles 15 to 19) and then the rights in relation to recipients (currently Article 13) and, lastly, in view of its purely procedural nature, the mechanism for the exercise of those rights.

Article 12(5) and (6)

As in the other cases in which provision is made for the Commission to act, the delegation believes that, although there is a need to ensure uniform legislation, it should be considered whether or not the Commission might adopt delegated acts in order to specify "*the criteria and conditions for the manifestly excessive requests and the fees referred to in paragraph 4*". This decision could be left to the data protection authorities or the European Data Protection Board. In paragraph 6 in particular, the Italian delegation suggests deleting the possibility for the Commission to take "*appropriate measures for micro, small and medium-sized enterprises*" in respect of the standard forms and procedures for replying to requests from the data subject. There should be no exceptions when it comes to exercising rights and, as in the other cases which will be mentioned later, any differences in burdens and safeguards should be subject to provisions which take into account not only the size of the enterprise but also the nature and scope of the data processing.

Article 14(1)(c)

It may be difficult or even impossible, when the data are collected, to supply accurate information on the period for which they will be stored. This information may be superfluous in any case given that, as a general rule, data must be stored only for the time needed to achieve the purposes for which they were collected. In the light of these considerations, it is therefore suggested that (c) be deleted.

Article 14(1)(f)

Although this clause reproduces to the letter the clause contained in Directive 95/46/EC, it would be useful to specify whether all recipients of the data should be listed (this would be an onerous and, possibly, unfeasible requirement to include among the information provisions, but could be envisaged as part of the exercise of rights) or only the categories of recipients.

Article 14(1)(g)

In the section that reads "*Given that there are still different grounds legitimising the transfer of data abroad",* it is suggested that the phrase "*and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission*" be replaced by "*, indicating the presumption of permissibility of such transfer*".

Article 14(1)(h)

The phrase "*any further information necessary to guarantee fair processing in respect of the data subject*" appears too general. We suggest that this information should include information on the existence of some processing operations for which a PIA has been necessary and which therefore present high risks for the data subject (Article 33), measures based on profiling (Article 20) and information on the consequences of the data processing for the data subjects.

Article 14(4)(b)

The phrase "*within a reasonable period*" is too vague and requires quantification. In the Italian version, the word "*divulgazione*" would be better replaced by "*comunicazione*", given that this provision seems to be referring to the disclosure of data to a particular recipient.

Article 14(5)(a)

This does not appear to be a matter that should be delegated to the Commission; instead, it should come under the criteria and general categories laid down in the regulation. The disproportionate effort needed to provide the information (which would constitute the grounds for an exemption) should be weighed against individual cases and different national situations.

Article 14(5)(d)

Whatever the arguments might be for an exemption from the requirement to provide information if data are not collected from the data subject, there would appear to be a case for introducing specific provisions in respect of data collected for the defence in court cases.

Article 14(7)

In addition to the doubts expressed concerning the Commission's role in adopting delegated acts in this field, the delegation also has reservations about the clause empowering the Commission to take "*the appropriate measures for micro, small and medium-sized enterprises*". It would seem preferable to impose a threshold that takes into account the nature and scope of the data processing and not just the size of the enterprise.

Article 15(1)(c)

It should be clarified whether or not the controller must keep records of and provide information on all third parties who are recipients of the data and for how long he must keep this information on the data (see the judgment of the Court of Justice of 7 May 2009 in Case C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*). It would therefore be better to use the phrase "*third party recipients of the data*" to ensure that the names of all those who have processed the data within the enterprise, on behalf of the controller, do not have to be disclosed to the data subjects.

Article 15(1)(e) and (f)

The right to request the rectification or erasure of personal data and to object to the processing of such data, as well as the right to lodge a complaint to the supervisory authority, should be included in the information to be provided to the data subject at the moment of collecting the data rather than in response to the exercise of rights (see Article 14(1)(d) and (e)). Both these subparagraphs should be deleted.

Article 15(3) and (4)

The delegation continues to have the same reservations as expressed earlier concerning the role of the Commission. As regards the coherence of Chapter III as a whole, as already mentioned, we would stress that empowering the Commission to specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1 is unnecessary in the light of the provisions laid down in Article 12(6). These two sets of provisions should be coordinated.

Article 17

While supporting the underlying purpose of this article, the delegation considers that it is worded in such a way that it will be difficult for the data subject to ensure that it is put into practice.

Article 17(1)(b)

The phrase "*when the storage period consented to has expired*" should be replaced by "*the data are no longer needed for the purposes for which they were collected*" (see the proposal to delete Article 14(1)(c)).

Article 17(1)(d)

The phrase "*does not comply with this Regulation for other reasons*" should be replaced by "*is illegal*" or "*is being carried out unlawfully*" so that it also covers cases where data processing may be considered unlawful because it is in breach of national sector-specific regulations that the Commission itself has recognised as being applicable.

Article 17(2)

The last sentence of this paragraph is unclear. The notion of "authorisation" is a broad one and requires further clarification.

The role of third parties which are processing the data should also be clarified so as to define the conditions under which, and in which capacity, they can carry out the data subject's request, as well as any consequences which may ensue in the event of a failure to comply with such request.

Furthermore, the regulation does not give any indication of how the data subject can exercise his rights if the controller no longer occupies that post, or has died, or cannot be identified or contacted.

Article 17(3)

With regard to the processing of data on the internet, there is no provision for a mechanism for cancelling links to data, or for cancelling copies or reproductions of the data which may still be published on other web pages. Such links, copies or reproductions may, however, facilitate access to the original content even though there may not necessarily be any justification for such access. Article 17(3)(d) should be coordinated with Article 21 to determine whether it is needed.

Article 17(4)

To make the substance of this provision clearer, the words "*to the storage of such data*" should be added after the phrase "*Instead of erasure, the controller shall restrict processing of personal data*".

Article 17(5)

The notion of "public interest" is too vague and should be clarified, or it may give rise to systematic recourse to exemptions, which could lead to inconsistencies in national legislation (here again there is a need for alignment with Article 21).

Article 17(8)

This phrase is rather illogical: if erasure is carried out, obviously the data can no longer be processed. We propose that Article 17(8) be deleted.

Article 18

The scope of the right to data portability should be specified in such a way as to ensure that it can actually be exercised.

Article 18(1) and (2)

The relationship between the right to obtain a copy of the data, as provided for in Article 18(1), and the right to take cognizance of the personal data being processed should be clarified. It should also be specified that the exercise of the right to data portability shall be without prejudice to the obligation on the holder to erase the data once they are no longer necessary for the purposes for which they were collected.

Article 19(1) - Right to object

The text should be modified, by adapting the phrase contained in Directive 95/46/EC: "*on legitimate grounds relating to his particular situation*".

Article 19(2)

The words "*and at any time*" should be added after the phrase "*the right to object free of charge*" where personal data are processed for direct marketing purposes.

Article 19(3)

If the data subject objects to certain types of processing (for example, dissemination of data), it would not be right to prohibit any type of further processing (such as cases of storage of data in compliance with a legal obligation). We therefore propose that Article 19(3) be deleted altogether.

Article 20(1) - Measures based on profiling

The expression "*significantly affects*" in Article 20(1) is imprecise; it should be specified that this expression covers, for example, the application of network analysis instruments, user behaviour tracking, the creation of movement profiles via portable applications and the creation of personal profiles through social networking sites.

Moreover, the rules should not be restricted to automated processing alone; they should also apply to methods involving partially automated processing. There is a need for an approach which clearly defines the purposes for which profiles may be created and used and which specifically requires controllers to inform the data subject, particularly in respect of the right to object to such creation and use.

Article 20(2)(a)

We propose that the right of the data subject to put his point of view - as already enshrined in Article 15 of Directive 95/46/EC - should be reintroduced.

Article 20(4)

We propose that the information to be provided by the controller should also include the processing logic.

Article 21

The "legislative measure" aimed at restricting the scope of the obligations and rights provided for in points (a) to (e) of Article 5 and Articles 11 to 20 and Article 32 should clearly indicate "*the purposes and methods of processing, the category of data processed, the controller and the authorised processors of the data and safeguards to prevent arbitrary interference by the public authorities*". The wording of this article therefore needs to be examined, as it seems to allow for broader exemptions than those laid down in Directive 95/46/EC, with the attendant risk that the rules may not be applied uniformly.

Article 21(1)(c)

The already broad category of "other public interests" is excessively widened by this clause.

Article 22

The application of the principle of responsibility should be contextualised, taking into account, notably, the size of the entity controlling the data processing, the nature of the data and the impact of the processing.

Article 22(3)

The rules specify that the data administrator must verify, if necessary by means of internal or external auditors, the effectiveness of the measures implemented to guarantee the lawfulness of the processing for which he is responsible and whether or not it is performed in compliance with the Regulation. The provisions need to be further modified, to ensure that no excessive burden is placed on the data administrator, who is required at all times to assess the suitability of the measures taken to comply with the general requirements, and bears legal liability for any non-compliance or non-fulfilment. The criteria relating to responsibility should, however, take into account the size of the controlling entity, the nature of the data and the impact of the processing.

Article 23 - Data protection by design and by default

The meaning of these provisions should be made clearer, for example in a recital stating that features of products and services designed to facilitate the protection of privacy should be activated automatically and that appropriate procedures should be set in motion during the design phase of the processing or the product. It must be up to the controller to demonstrate that his activities take account of the concepts of data protection by design and data protection by default, which in turn count as appropriate measures within the meaning of Article 22(1).

Article 23(3)

When laying down technical standards, the Commission should involve and, where appropriate, consult the European Data Protection Board and international standards organisations.

Article 25

Further clarification is needed with regard to the role and obligations of the representative referred to in Article 25. For example, there should be an explanation of the representative's role vis-à-vis the data subjects, the judicial authorities and the data protection authorities, given that Article 79(6)(f) provides for the maximum fine in the event of failure to designate a representative.

Article 25(2)(a)

Provision should also be made for the appointment of a representative even where the controller is established in a third country which ensures an adequate level of protection. The fact that a third country ensures an adequate level of protection has nothing to do with the need to have a point of contact in the European Union. We therefore propose that subparagraph (a) of Article 25(2) should be deleted.

Article 25(2)(b)

The exceptions to the obligation to designate a representative should be based on the nature and scope of the processing of the personal data, as well as on the number (if any) of interested parties affected within the EU. The current threshold expressed solely in terms of the number employed by the controller could result in the exclusion of small organisations which process enormous quantities of data and present specific risks to individuals.

Article 25(2)(d)

We suggest deleting this reference to merely occasional processing, since it is not sufficiently justified.

Article 25(3)

It should also be made clear that the reference to the representative's being established in the European Union ("*shall be established in one of those Member States*") will not result in the application of the main establishment provisions laid down in Article 4(13), i.e. that it does not constitute a decisive factor for the purposes of determining the competent data protection authority within the meaning of Article 51(2).

Article 26(2)(d)

This paragraph refers to the possibility of additionally introducing sub-processors. To avoid "blanket" authorisations, "*ad hoc*" or "*case by case*" could be added before "*prior permission*".

Article 26(4)

It should be clearly specified that this provision can only take effect if there is a prerequisite of lawful processing; otherwise the processing is unlawful and there will be consequences in terms of liability for both the processor and the controller.

Article 26(5)

Here, as elsewhere, we have misgivings as regards the power given to the Commission to adopt delegated acts under Article 86. The European Data Protection Board should at least be consulted when this power is exercised.

Article 27

The last part of the article ("*unless required to do so by Union or Member State law*") is unclear and seems to legitimise, without due reason, data processing by persons to whom the controller has not given the requisite indications for the processing of the data. We suggest that it be deleted, with reference also to the comments made on Article 26(4).

Article 28

The obligation to retain all documentation relating to processing carried out would impose a disproportionate burden if applied to all data administrators. On the other hand, the criteria laid down in paragraph 4 of this article do not seem sufficient to introduce nuances to this obligation, and it would therefore be preferable to introduce criteria similar to those suggested for Article 22.

Article 28(4)(a)

The exemption from the obligation to retain documentation for "*a natural person processing personal data without a commercial interest*" should be coordinated with the reference to the application of the system to natural persons (Article 2(2)(d)).

LITHUANIA

General Remarks

Stakeholders from public and private sectors exchanged by opinions regarding the General Regulation presented by the Commission and hereby presented comments and proposals of Lithuanian delegation for amendments regarding Chapter III and Chapter IV of the Draft of a General Data Protection Regulation.

Comments and proposals on the Regulation article by article

Article 12

The concept of "*manifestly excessive request*" laid down in *Article 12 Paragraph 4* raised some kind of concerns. If it is not defined more clearly, there could be possibilities for the controller not to exercise the rights of the data subjects or charge an unreasonable fee.

The requirement laid down in *Article 12 Paragraph 5* regarding fees is doubtful. Considering economical differences of member states, equal fees for all member states would be significant financial burden for data subjects. Lithuanian proposal is to determine that ***"once a calendar year the data controller shall disclose such data to the data subject free of charge. When such data are disclosed for a fee, the amount of the fee shall not exceed the cost of disclosure of the data".***

Article 14

It is not clear if data subject should be provided with all the information specified in the *Article 14 Paragraphs 1 and 2* in all cases not regarding what the coverage of data subject's request is. According to Lithuanian opinion, such regulation would cause significant administrative and partially financial burden because the scope of information is fairly broad.

Article 16

Uncertainty of definitions „inaccurate", "incomplete" determines difficulties in implementation of *Article 16*. According to proportionality principle the data controller may process as much data as it is necessary to achieve the objects of data processing. Thus the right of data subject to obtain completion of incomplete personal data is not clear. Also it is not clear if the controller must do it according to every data subject's request.

Article 17

Lithuania supports the choice of legal provision indicated in *Article 17* regarding very important data subjects' "right to be forgotten" but it raises some concerns due to practical implementation. Reasonable steps to inform third parties that a data subject requests them to erase his/her personal data should be defined more clearly. Practically any steps to inform all third parties would be costly and require additional time for that. In addition, the data controller may not even know all third parties which are processing such data using links, copies, replication of personal data and etc. Thus the right of data subject to be forgotten and to erasure of data would be realized incompletely. Also the liability of the third parties which refuse to take actions on requests of the controller should be discussed.

The wording of Article 17 Paragraph 2 "where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication" is not clear enough if the authorisation should be made officially by a contract or by other actions. For example, in case of implementing insufficient technical measures, therefore the third parties have the possibility to obtain the information that the controller has made public.

Article 18

According to the Lithuanian opinion, the right of the Commission to specify the electronic format for the transmission of personal data is doubtful. Member states should have the right to specify the electronic format for the transmission of personal data in the public sector by national law. Subjects of the private sector should have the right to rule this question by agreements themselves.

Article 19

According to the Lithuanian opinion, the concept of "compelling legitimate grounds" settled in *Article 19 Paragraph 1* should be detailed pointing out clearly defined conditions when the controller may refuse the objection of the data subject.

The provision of *Article 19 Paragraph 2* sets opt-out principle. According to the Lithuanian opinion, it does not adequately guarantee the right of the data subject to privacy while processing his personal data. Lithuanian suggestion is to set opt-in principle according to which Personal data may be processed for direct marketing purposes only after the data subject has given his consent.

Article 20

Lithuania agrees with the increased guarantees for data subjects regulated in the *Article 20*. Especially we support the provision that guarantees protection of the special categories of data referred to in *Article 9 Paragraph 3.*

Article 21

The concept of "other public interests of the Union or of a Member State <…>" indicated in *Article 21 Paragraph 1 Subparagraph c* raised some type of concerns. It does not guarantee that rights of data subjects would be reasonably restricted in all cases. Lithuania thinks that the bases when the rights of data subjects can be restricted should be defined more clearly.

The wording of *Article 21 Paragraph 1 Subparagraph e* gives wide opportunities to restrict rights of data subjects, thus concrete requirements concerning the restrictions of the rights of data subjects should be regulated in the Regulation.

Article 22

One of the main objectives of the Regulation is decreasing administrative obligations for business, but according the provision of the *Article 22 Paragraph 2 Subparagraphs c and e* there would be even more obligations for the controller that require additional human, technical and financial resources. Accordingly, ***Lithuanian proposal is to delete Subparagraphs c and e of the Paragraph 2 of the Article 22.***

Article 23

Lithuania supports the provision regulating data protection by design and by default, but it is not clear how these requirements would be implemented. The measures that the controller should implement at the time of the determination of the means for processing should be defined more clearly.

Article 24

Lithuania supports this new provision because it will help data subjects to exercise their rights easier, but it is not clear how the question of liability would be solved if there is not the arrangement between joint controllers.

Article 25

In the opinion of Lithuania, exceptions indicated in *Article 25 Paragraph 2 Subparagraphs b, c and d* would not ensure appropriate implementation of the rights of data subjects. For example, a lot of data controllers (legal persons) of the third countries would not be obliged to designate a representative in the Union. In the opinion of Lithuania, the exceptions regarding the obligation to designate a representative in the EU, should depend on character and quantity of processed personal data, but not on the number of employees of the data controller because a small enterprise can process a lot of personal data of special categories.

The concept of "occasionally" should be described more clearly (*Article 25 Paragraph 2 Subparagraph d).*

LUXEMBOURG

The general remarks made in earlier written comments remain valid.

Detailed comments/questions

Chapter III – Right of the data subject

- Art 14 – Information to the data subject: Luxembourg is not convinced that such a long list of information to be provided to the data subject is necessary in all circumstances. Indeed, the data subject may be "overwhelmed" with information, particularly in certain online (but also offline!) contexts, which does not result in better protection of his/her personal data. A contextual approach may be more relevant, in particular to maintain the technologically neutral character of the regulation.

- Art 14 (1) (c): Luxembourg does not support that information on the storage period should be provided on a mandatory basis by data controllers.

- Art 15 – Right of access for the data subject : Luxembourg wonders how the controller can effectively verify that the data subject and not another person is making the request for access. In this context, what is to be understood by "reasonable measures" in recital (52)?

- Art 17 – Right to be forgotten and to erasure: Luxembourg supports a clarification of the right to erasure and shares the objectives of a right to be forgotten in an online context. However, Luxembourg is not convinced about the practicability of the proposed right to be forgotten and wants to maintain a technologically neutral regulation. The following concerns are raised:

    - How can controllers comply with the obligation to ensure that third parties erase any links to, copies or replication of the data? There is a risk of obliging controllers, in an online context, to monitor all data traffic which is contrary to the principle of data minimization and in breach with the prohibition in the e-commerce directive to monitor transmitted information (Article 15 of Directive 2000/31/EC)

- To what extent is the right to be forgotten different or new compared to the right to erasure? What is the articulation of the right to be forgotten with the right of rectification?
- The right to be forgotten may create false expectations among data subjects, and may even be counter-productive by encouraging data subjects to share all their information in the knowledge that they can "un-share" it at any time. This does not encourage a responsible and enlightened handling of personal data by individuals.
- What is the articulation of the right to be forgotten with fundamental rights such as freedom of expression? What is the articulation of the right to be forgotten with other legitimate reasons – or even legal obligations arising from other sectoral legislation - of the controller to retain data (for purposes of fraud prevention e.g.)?
- Luxembourg underlines the necessity of this provision to be without prejudice and consistent with Directive 2001/31/EC (e-commerce directive), more precisely the provisions on intermediary liability.

- Art 18 – Right to data portability: Luxembourg wonders about the compatibility of this right with the obligation for controllers to retain certain data for compliance reasons. Luxembourg is not sure to what extent this right is workable in the offline environment.

- Art 20 – Measures based on profiling: Luxembourg wonders why paragraph 1 concerns "natural persons" and not the "data subject", and is not sure about the technologically neutral character of these provisions.

- Art 21 – Restrictions: Luxembourg considers this article as very important in the overall Regulation. It is crucial to get the balance right and to avoid jeopardizing the objective of the Regulation which is to create harmonised and uniform rules across the internal market. The derogations should therefore not be laid out too vaguely but strictly limited and precise. Luxembourg suggests to add in paragraph (1) that restrictions constitute "a necessary, non-discriminatory and proportionate measure" which is the third criterion consecrated by EUCJ case law necessary to justify any restriction to the free movement in the internal market.

Chapter IV – Controller and processor

General remark: Luxembourg welcomes that the Regulation maintains the traditional controller-processor concepts. However, it is crucial to clarify as much as possible the respective allocation of obligations and responsibilities between both. According to Luxembourg, there is an inherent risk of overlap or confusion of responsibility between both at the expense of legal certainty and protection for data subjects. This is particularly the case where the processor's responsibilities have been extended, blurring the roles between controllers and processors. Such a potential grey zone is unhelpful particularly in a cloud computing context, where different contractual obligations may be interfered with. For Luxembourg, the addition "and processor" should therefore be deleted in several of the subsequent articles to clarify which entity is ultimately responsible.
Furthermore, certain obligations conflict with other obligations imposed upon businesses to be in conformity with other EU legislation. There is a need for clarifying the relationship of this Regulation with other sector-specific legal texts.
Finally, Luxembourg supports an overall reduction of administrative burden on controllers and processors, which does not have to come at the expense of less protection of personal data.

- Art 23 – Data protection by design and by default: Luxembourg supports both principles which should be developed and continuously improved by the market forces. Delegated acts defining such measures may put a damper on innovation.

- Art 26 – Processor: As laid out in the general remarks above, Luxembourg is not convinced by the extension of the responsibilities of the processor which blurs the two concepts of controller and processor. Particularly in a cloud computing context, there is a need for flexibility as different entities and sub-contractors may be involved in the processing of personal data with different responsibilities and different means of access or control over personal data. Some of these may not have any meaningful access and may be considered neutral intermediaries (and not be considered controllers or processors as defined under this Regulation).

HUNGARY

Chapter III

Procedures and mechanisms for exercising the rights of the data subject

Article 12 (2)

According to the second sentence of Article 12 (2) the controller may prolong the period within which the data subject's request of information shall be responded to if "*several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller*".

Hungary fears that the cited provision is too vague; it is not entirely clear whether the phrase "*their cooperation"* refers to the cooperation between the "*several data subjects"* or to the cooperation between the data subjects and the data controller.

Hungary therefore recommends to clarify the provision accordingly.

Right to rectification

Article 16

Hungary strongly supports the inclusion of the right to rectification into the proposal as it is a basic guarantee of the protection of personal data. However, further clarification seems necessary with regard to the phrase "*including by way of supplementing a corrective statement*" because the text in its present form neither defines the notion of a "*corrective statement*" nor regulates the obligations of the controller regarding the "*supplementing*" of such statement.

Right to be forgotten and to erasure

Article 17 (8)

Hungary welcomes the introduction of the right to be forgotten and recognises the need for a very exact and careful regulation of the rights and obligations of the controllers and processors in connection with this right.

Article 17 (8) stipulates that if personal data were erased the controller shall not otherwise process the erased data.

In this respect Hungary would like to draw the attention to the fact that "erasure" by its very nature is and should always be immediate and final, any potential option for further processing seems illogical. Hence the aim of the provision in Article 17 (8) is ambiguous and the provision itself seems unnecessary.

Right to data portability

Article 18 (2)

While the right to data portability in the view of Hungary does not represent a fundamental guarantee for the individuals, it might be a useful tool for the data subjects in the online environment.

Hungary is of the opinion that the phrase "*without hindrance from the controller from whom the personal data are withdrawn*" in Article 18 (2) lacks the sufficient clarity, the precise limits of the exercise of the right of data portability are hardly identifiable.

Hungary therefore suggests redrafting the phrase in order to ensure legal certainty.

Right to object

Article 19 (1)

Article 19 (1) allows the data subject to exercise the right to object in connection with the processing of personal data based on point (e) of Article 6 (1). According to Article 6 (3) the basis of the processing referred to in point (e) must be provided for either in Union law or in the law of the Member State to which the controller is subject.

Consequently data controllers in these situations are acting as sheer executors of the legal provisions obliging them to process personal data. Hence it is obviously not the data controller who would be able to „*demonstrate compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject*" but the legislator. That makes the application of Article 19 (1) irrational in cases falling under point (e) of Article 6 (1).

Hungary therefore advises to delete the reference to point (e) of Article 6 (1) in Article 19 (1).

Restrictions

Article 21 (1)

Hungary has reservations about the current wording of Article 21 (1). This provision allows for the Union or Member State legislator to restrict the scope of the obligations and rights provided for *inter alia* in points (a) to (e) of Article 5. This means that according to this provision in certain situations fundamental principles of the protection of personal data are not to be met such as the obligation of lawful and fair processing and the processing for legitimate purposes.

Hungary strongly believes that these principles are meant to be the very core of the fundamental right of the protection of personal data, hence there should be no such interest, be it defined in Union or Member State law, that could override their application.

On the other hand Hungary recognises that there might be situations where restrictions with regard to certain principles drafted in Article 5 should be acceptable and justifiable (e.g. the obligation to keep the data up to date). These exceptions however should be as carefully and narrowly defined as possible.

In the light of the above mentioned reasons Hungary proposes to review Article 21 (1) and redraft the provision in a way that derogations are limited to the minimum necessary.

THE NETHERLANDS

(46) The principle of transparency requires that any information addressed to the public or to the data subject should be easily accessible, *where appropriate in electronic form*[1], and easy to understand, and that clear and plain language is used. This is in particular relevant where in situations, such as online advertising, the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand if personal data relating to them are being collected, by whom and for what purpose. Given that children deserve specific protection, any information and communication, where processing is addressed specifically to a child, should be in such a clear and plain language that the child can easily understand.

(48) The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes, how long the data will be stored, on the existence of the right of access, rectification or erasure and on the right to lodge a complaint. *Furthermore the data subject should be informed on the existence of certain processing operations which have a particular impact on individuals, such as those for which a personal data impact assessment indicates a high risk and measures based on profiling, as well as the consequences of such operations and measures on individuals*[2]. Where the data are collected from the data subject, the data subject should also be informed on the consequences, in cases they do not provide such data.

(55) To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are processed by electronic means and in a structured (...)[3] format, to obtain a copy of the data concerning them also in (...) electronic format. The data subject should also be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one. This should apply where the data subject provided the data to the automated processing system, based on their consent or in the performance of a contract.

---

1 To accommodate data subjects.

2 Without prejudice to future amendments to Article 20, it should be made clear that transparency is a key value in accepting and accommodating profiling operations, while at the same time strengthening data subjects' rights.

3 In conformity with proposals on Article 18.

CHAPTER III

RIGHTS OF THE DATA SUBJECT

SECTION 1
TRANSPARENCY AND MODALITIES

Article 11
Transparent information and communication

1. The controller shall […] provide in a transparent and easily accessible manner […] the information referred to in Article 14 […] and information on […] the exercise of data subjects' rights.[1]

2. The controller shall, having regard to the state of the art, the cost of the implementation, the risks of the processing and the nature of the data to be protected, provide […] appropriate information and […] communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child.[2]

Article 12
Procedures and mechanisms for exercising the rights of the data subject

1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.

2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.

3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority. […] [3]

---

1 This is to clarify the relation between Articles 11 and 14.

2 A proportionality test should be introduced.

3 Data controllers should not be burdened with providing legal advice to data subjects. This does not preclude any specific Member State law for public sector data controllers to inform citizens on remedies against administrative acts.

4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are a manifest […] abuse of right[1], in particular because of their repetitive or manifestly unfounded [alternative: vexatious] character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive or unfounded character of the request.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the manifestly excessive requests and the fees referred to in paragraph 4.

6. The Commission may lay down standard forms and specifying standard procedures for the communication referred to in paragraph 2, including the electronic format. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 13
Rights in relation to recipients

The controller shall communicate any rectification or erasure carried out in accordance with Articles 16 and 17 to each recipient to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort.

SECTION 2
INFORMATION AND ACCESS TO DATA

Article 14
Information to the data subject

1. Where personal data relating to a data subject are collected, the controller shall provide the data subject, where applicable[2], with at least the following information:

   (a) the identity and the contact details of the controller and, if any, of the controller's representative […] [3];

[1] Abuse of right is a broader term in order to imply substantially manifestly unfounded [or vexatious] requests.
[2] Para 1, a- h, do not seem applicable in all cases.
[3] It should be left to the discretion of the data controller whether contact details of a DPO should be revealed.

(b) the purposes of the processing for which the personal data are intended, including the […] [1]and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);

(c) the period for which the personal data will be stored;

(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;

(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;

(f) the recipients or categories of recipients[2] of the personal data;

(g) that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;

(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.

2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract […] [3], as well as the possible consequences of failure to provide such data.

3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate.

4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:

(a) at the time when the personal data are obtained from the data subject; or

(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.

---

[1] An overload of information should be avoided in order to reduce administrative burdens and to protect the data subject interests.

[2] The definition of recipient should be clarified. NL supports the express inclusion of third parties.

[3] Informing the data subject on the consequences of his refusal to provide data only makes sense if there is a statutory or contractual duty to provide the data. Voluntary data collection is not in accordance with Article 5(c).

5. Paragraphs 1 to 4 shall not apply, where:

(a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or

(b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or

(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by Union or Member State [1]law; or

(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21;

(e) the data are processed for statistical purposes or for the purposes of historical or scientific research, and the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by Union or Member State law[2].

6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises.

8. The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

---

[1] Clarification.

[2] The existing exemption in Directive 95/46/EC for statistical, historical and scientific purposes is still justified.

Article 15

Right of access for the data subject

1. The data subject shall have the right to obtain from the controller at […] reasonable intervals[1], on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information:

   (a) the purposes of the processing;

   (b) the categories of personal data concerned;

   (c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries;

   (d) the period for which the personal data will be stored;

   (e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;

   (f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;

   (g) communication of the personal data undergoing processing and of any available information as to their source;

   (h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.

2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.

2a. Paragraph 1 shall not apply where the data are processed for statistical purposes or for the purposes of historical or scientific research, and the exercise of the right of access proves impossible or would involve a disproportionate effort[2].

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.

---

[1] This is to avoid excessive administrative burdens for data controllers.

[2] The existing exemption in Directive 95/46/EC for statistical, historical and scientific purposes is still justified.

4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

SECTION 3

RECTIFICATION AND ERASURE

Article 16
Right to rectification

1. The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement.

2. Paragraph 1 shall not apply where the data are processed for statistical purposes or for the purposes of historical or scientific research, and the exercise of the right of rectification proves impossible or would involve a disproportionate effort[1].

Article 17
Right to be forgotten and to erasure

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:

   (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

   (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;

   (c) the data subject successfully objects to the […] collection or retention of personal data pursuant to Article 19[2];

---

[1] The existing exemption in Directive 95/46/EC for statistical, historical and scientific purposes is still justified.

[2] Clarification. The right to object has no absolute character.

(d) the processing of the data does not comply with Articles 5, 6, 8 and 9 […] [1].

2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.

3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:

(a) for exercising the right of freedom of expression in accordance with Article 80;

(b) for reasons of public interest in the area of public health in accordance with Article 81;

(c) for historical, statistical and scientific research purposes in accordance with Article 83;

(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;

(e) in the cases referred to in paragraph 4.

4. Instead of erasure, the controller shall block or otherwise [2] restrict[3] processing of personal data where:

(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data[4];

---

1 Clarification. Other articles can be added.

2 A clarification in order to retain the possibility of blocking data.

3 The definition of "restriction of processing" in Article 3(4) 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, should be inserted in Article 4 of the Regulation.

4 It should be considered to regulate the blocking or restrictions on processing contested data in Article 16.

(b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof or the settlement of disputes[1];

(c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;

(d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2).

5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof or the settlement of disputes, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.

6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.

7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.

8[2]. Where the erasure is carried out, the controller shall not otherwise process such personal data.

9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:

(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;

(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;

(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.

---

[1] Retention of data for purposes of proof usually implies other purposes such as the settlement of disputes in or out of court.

[2] Striking this paragraph should be considered, since erasure should imply definite destruction of the data concerned.

Article 18
Right to data portability[1]

1. The data subject shall have the right, where personal data are processed by electronic means and in a structured […] format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used or based on open standards[2] and allows for further use by the data subject.

2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.

3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

SECTION 4

RIGHT TO OBJECT AND PROFILING

Article 19
Right to object

1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f)[3] of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.

---

1 It could be considered limiting the right of data portability to user-generated content published through information society services only, in order to target social media directly and to clarify the relation with Article 15.

2 To avoid unnecessary restrictions on the use of formats.

3 The relation of the weighing of interests by the controller pursuant to Article 6 (f) and the weighing of interests pursuant to Article 19, paras 1 and 3 should be clarified. Is it meant that when the controller concludes that the processing of personal data is justified under Article 6(f), he will have to make a second weighing of interest after having received an objection from the data subject in which he now has to demonstrate *compelling* grounds for processing?

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object free of charge to the processing of their personal data for such marketing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information.

3. Where an objection is upheld pursuant to paragraphs 1 and 2, the controller shall no longer use or otherwise process the personal data concerned.

4. Paragraph 1 shall not apply where:

(a) the data are processed in public records or other registrations established by Member State law[1];

(b) the data are processed for statistical purposes or for the purposes of historical or scientific research, and the exercise of the right to object proves impossible or would involve a disproportionate effort[2].

Article 20
Measures based on profiling

1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict […] such as[3] the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.

2. Subject to the other provisions of this Regulation, a person, not being a child[4], may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:

(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention and arrangements allowing him to put his point of view[5]; or

(b) is expressly authorised by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or

---

1 The right to object is incompatible with the statutory duty of governments to provide for public registers such as vehicle registrations, land registers etc.

2 The existing exemption in Directive 95/46/EC for statistical, historical and scientific purposes is still justified.

3 Clarification on the status of the enumeration.

4 This is to align article 20, para 2, with recital 58.

5 This addition stems form Article 15 of Directive 95/46/EC which still seems to be adequate.

(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.

3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.

4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.

SECTION 5
RESTRICTIONS

Article 21
Restrictions

1. Union or Member State law[1] may restrict by way of a legislative measure the scope of the obligations and rights provided for in points (a) to (e) of Article 5 and Articles 11 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:

(a) public security

(b) national security[2];

(c) the prevention, investigation, detection and prosecution of criminal offences;

(d) other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters and the protection of market stability and integrity;

---

[1] It could be considered addressing the data controller directly as an alternative to Union or Member State law regulating restrictions.

[2] The present exemption on national security of Article 13 of Directive 95/46/EC should be retained.

(e) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (a), (b), (c) and (d);

(g) the protection of the data subject or the rights and freedoms of others.

2. […] Any[1] legislative measure referred to in paragraph 1 shall contain specific provisions at least as to the objectives to be pursued by the processing and the determination of the controller.

CHAPTER IV
CONTROLLER AND PROCESSOR

SECTION 1
GENERAL OBLIGATIONS

Article 22
Responsibility of the controller

1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.

2. The measures provided for in paragraph 1 shall in particular include:

(a) keeping the documentation pursuant to Article 28;

(b)implementing the data security requirements laid down in Article 30;

(c)performing a data protection impact assessment pursuant to Article 33;

(d)complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);

(e)designating a data protection officer pursuant to Article 35(1).

3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.

[1] Clarification of the text.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises[1].

Article 23
Data protection by design and by default

1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, […] in terms of the amount of the data, […] the time of their storage <u>and their accessibility</u>.[2] In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.

4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

---

[1] There is a need to assess the relation between the principle of accountability and existing Union law on regulated professions or sectors, such as the financial sector, in order to accommodate existing limitations on adoption of measures or duties to inform the general public of the processing of data.

[2] A clarification to ensure a better connection between the second and third sentence as well as an additional encouragement to data controllers to restrict access to data as much as possible.

Article 24
Joint controllers

Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject and their respective duties to provide the information referred to in Article 14[1], by means of an arrangement between them, or on the basis of a specific legal basis in Union or Member State law[2].

Article 25
Representatives of controllers not established in the Union

1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.

2. This obligation shall not apply to:

   (a)[3] a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or

   (b) an enterprise employing fewer than 250 persons; or

   (c) a public authority or body; or

   (d) a controller offering only occasionally goods or services to data subjects residing in the Union.

3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside[4].

4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.

---

1 Clarification in order to express that joint controllers should also determine their respective duties under Article 14.

2 Relations between joint controllers should also be established by a specific Union or Member State law.

3 Striking of this exception should be considered, since the level of data protection in any given third country does not necessarily assist in enforcement of the Regulation by the DPA in the EU Member State concerned.

4 The Member State in which a representative is established is not necessarily decisive in designating a DPA under Article 51, para 2.

Article 26
Processor

1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation […] [1] in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.

2. The carrying out of processing by a processor shall, where appropriate,[2] be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:

   (a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;

   (b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;

   (c) take all required measures pursuant to Article 30;

   (d) enlist another processor only with the prior permission of the controller;

   (e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

   (f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;

   (g) hand over all data[3] […] to the controller after the end of the processing and not process the personal data otherwise;

   (h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.

---

1 Protection the interests of the data subject is the prime responsibility of the controller, not the processor.

2 Controller - processor relations can also be found within a group of undertakings. Those relations are usually not determined by contracts or legally binding instruments, but based on internal instructions only.

3 Clarification. It is not clear to which results Para 2(g) refers.

3. The controller and the processor shall <u>be able to demonstrate the existence and execution</u>[1] […] of the controller's instructions and the processor's obligations referred to in paragraph 2.

4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.

Article 27

Processing under the authority of the controller and processor

The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.

[1] Reduction of an administrative burden in conformity with the principle of accountability.

POLAND

Article 11

Transparent information and communication

- The terms "*transparent and easily accessible policies*" (par.1) and "*intelligible form, using clear and plain language, adapted to the data subject*" (par. 2) are not clear and raise many doubts among the controllers. PL sees the need to reformulate the wording of this article so that the general meaning of this article as a general rule applying to the following paragraphs is more visible.
- The sanctions relating to this article and their practical examination should be further examined and verified.

Article 12

Procedures and mechanisms for exercising the rights of the data subject

- PL welcomes the model according to which, in principle, realization of the right of the data subject to request information is free of charge. However, it is necessary to balance the interests and to introduce the mechanisms to protect controllers from potential abuse.
- PL sees the need to clarify the criteria and conditions of "*manifestly excessive character of the requests*" at the level of the regulation. PL suggests including the criterion of the limit of requests in specific time (once every 6 months).
- Par. 5 (delegated act) needs to be erased.

Article 14

Information to the data subject

- PL has concerns about applying all the obligations listed in art. 14(1) to the controllers of the large-scale public registers. PL asks for clarification if the large-scale public registers are also covered by the provisions of art. 14(1) or are there any exemptions for public registers. In that case including the proportional and justifiable limitations for these registers should be considered.

Otherwise PL has concerns that applying of the obligations listed in art. 14 to large-scale public registers (for example register PESEL – Polish Universal Electronic System for Registration of the Population comprising the identification numbers of all citizens) would impose disproportionate and costly burden.

- If these obligations apply to the controllers of the public registers, PL asks for clarification if the information listed in art. 14(1) can be provided to the data subject by giving the reference to the specific provisions of law.
- Par. 6 - PL sees the need for clarification and developing the par. 6: "*In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests"*. It is not clear, what the meaning of "*appropriate means*" and "*data subject's legitimate interests*" is.
- Par. 1 (b) PL asks for clarification of the intention of imposing on data controller the obligation to provide the data subject with "*contract terms and general conditions*". PL asks to explain the relation of this provision with consumer protection law.
- Par. 1 (h) – in order to avoid legal uncertainty to controllers, the criteria for any further information necessary to guarantee fair processing in respect of the data subject should be specified in the wording of the regulation itself and not in the delegated acts.
- PL supports the proposition of the Council Working Party on Statistics to complement par. 5(b):
  (b) the data are not collected from the data subject and the provision of such information, ***in particular when processing for historical, statistical, or scientific research purposes****, proves impossible or would involve a disproportionate effort*;
- PL does not support the proposition of the Council Working Party on Statistics to insert new par. 5A: "Paragraph 1(d) shall not apply where data are collected for historical, statistical or scientific research purposes and the conditions in Article 83(1A) are met."

Article 15

Right of access for the data subject

- PL proposes to put the wording from recital (52): "*The controller should use all reasonable measures to verify the identity of a data subject that requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the unique purpose of being able to react to potential requests*" into the proper text of regulation.
- The wording of Art.15 par. 1(g) is not clear. PL demands reformulation and clarification.
- PL suggests to insert new paragraph in Art. 15 allowing exemptions when data is processed for the purposes of official statistics and it proves impossible or involves a disproportionate effort to guarantee the right of access to the data subject.

Article 16

Right to rectification

- PL suggests to insert new paragraph in Art. 16 allowing exemptions when data is processed for the purposes of official statistics and it proves impossible or involves a disproportionate effort to guarantee the right to the data subject.

Article 17

Right to be forgotten and to erasure

- PL points that, due to technical limitations to the Internet, execution of the right to be forgotten would be impossible.
- It is unclear why– taking into account the lack of mechanism of enforcement as regards third parties – it is considered that data subject rights will be fulfilled effectively. Requiring data controllers to be responsible for the data that is not under their control seems to be disproportionate measure.

- It is also unclear how – taking into account the lack of mechanism of enforcement as regards third parties – application of Art. 13, which obliges data controller to communication of any rectification or erasure carried out in accordance with Articles 16 and 17 to each recipient to whom the data have been disclosed unless this proves impossible or involves a disproportionate effort, will be applied.
- In Art. 17 (3) b) the term "*public health*" should be precise. Simultaneously, PL would like to ask what is the relation between aforementioned provision and provision of Art. 21.
- It is still unclear for PL, whether Art. 17 is a general clause or is it of procedural character.
- PL asks for clarification if the provisions listed in Art. 17 (right of the data subject to erasure) apply to filing systems carried out by public authorities under the law or are the filing systems carried out by public authorities under the law exempted from obligation to erasure the data requested by data subject. PL expresses concerns that applying of the provisions listed in Art. 17 to filing systems carried out by public authorities would cause many problems.
- To summarize – the proposed writing of the Article 17 can pose a lot of problems with practical feasibility and scope of responsibility for processing of the data by third parties.

Article 18
Right to data portability

- PL have concerns that the proposed provisions would have negative implications for competition and intellectual property. PL suggests including provision that would enable to protect confidential and intellectually protected information.
- It is necessary to clarify the categories of the recipients of the provisions foreseen in this article. If this article also covers national statistical offices, it is recommended to include the restrictions of the rights of the data subject when the data are processed for the purpose of official statistics and the exercise of rights of the data subject would be impossible or would involve a disproportionate effort.
- In par. (3) PL points the translation inaccuracy. The term "*specify*" should be translated rather as "*określić*" in Polish and not – "*opracować*."

Article 19
Right to object

- PL sees the need to precise in a recital the term "*compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.*".
- PL proposes to insert the term "*free of charge*" in par. 1:
  1. *The data subject shall have the right to object* ***free of charge****, on grounds relating to their particular situation,* (…)"
- Par. (3) needs clarification, what are the practical consequences when the objection of the data subject is upheld and there is no agreement between controller and data subject.
- PL does not support the proposition of the Council Working Party on Statistics to insert new par. 4 "*The rights provided for in Article 19 do not apply when data are processed only for historical, statistical, or scientific research purposes and the conditions in Article 83(1A) are met.*"
  The right to process the data for historical, statistical, or scientific research purposes is provided in art. 6(2) and no right of the data subject to object is foreseen.

Article 20
Measures based on profiling

- PL expresses concern about the term "*significantly affect*" which seems to be too vague and may lead to abuses by entities using profiling techniques. It is questionable whether in case of such vaguely worded criterion – suggesting broad possibilities of various interpretations – the scope of the regulation will cover significant cases of using profiling mechanism, important in colloquial understanding (as for example choosing specific advertising messages).

Article 21
Restrictions

- PL expresses concerns about restricting in this article the rights provided in Art. 5 points (a) to (e). PL finds the rights provided in Art. 5 as fundamental and they should not be subject to general exemption provided in Art. 21.
- In the opinion of PL Art. 21 (2) should be complemented by additional safeguards for data subject.

Article 25
Representatives of controllers not established in the Union

- PL sees the need to describe more in detail the obligations of the representative of the controller.
- 2(a) - PL finds an exemption from the obligation to have a representative for controllers established in third countries with an adequate level of data protection unjustified.
- 2 (b) – PL expresses doubts if the size of the entity limited to 250 would be an appropriate criterion for the application of data protection rules in this case.

As a general comment **concerning the exemptions for the data processed for the purposes of historical, statistical and scientific research purposes** it is of vital importance to define the statistical purposes and make a distinction between the data processed for these purposes only by national statistical offices on the one hand and by other private entities – on the other. Different provisions should apply to these two different cases of data processing.
It's also not clear why the terms "statistical research" and "statistical purposes" are applied alternately in the proposal.
Also historical and scientific research purposes need to be further explained and detailed.
It should be also noticed that delegation of rights in the scope of statistics (Art. 83) raises doubts as to hierarchy of legal acts of the EU. Statistical issues are regulated by the regulation 223/2009, which is framework document resulting from Article 338 of the Treaty on Functioning of the European Union.

ROMANIA

Art. 12 (1) last thesis, in relation with ***Art. 12(2),*** last thesis:
Par. (1): (…) Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.
Par. (2): (…) Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.

Romania would like to express its concerns regarding the applicability, in practice, of the paragraphs mentioned, which provide for the possibility to answer to a request from a data subject, electronically. **Identity frauds may occur** in case of providing personal data in electronic format. In practice, the authorities will have to establish (from the computer terminal), that the one whom the information is sent to, **is the real data subject**, even in cases when the request was sent in an electronic way. In this respect, Romania would welcome some solutions and additional information for best practices regarding **the means of identification of the data subject, when the request is sent electronically.**

Art. 14 (1) g) Romania supports the necessity of clarifying the wording *"by reference to an adequacy decision by the Commission"*.

Art. 22 point 2(c) in relation with **Art. 33(5)** - Romania would welcome clarifications regarding the **necessity** for the controllers to carry out impact assessments regarding data protection, as it is stipulated in art. 22 point 2(c), as well as the reasoning for which public authorities are exempted from the rules above mentioned regarding impact assessments obligation, as stipulated in **Art. 33(5).**

Art. 23(4) shall be completed in order to confer the Commission guidance on establish the minimum technical standards in order to ensure the protection of data subject personal data.

SLOVENIA

In accordance with the document of the Cyprus Presidency of the Council of the European Union, submitted by the General Secretariat (CM 3942/1/12 REV 1, as of 5 September 2012) to delegations of Member States at DAPIX, the Republic of Slovenia states its positions on Articles 11-27 of the Draft of the General Data Protection Regulation, in order that they may be included in appropriate footnotes or taken into account while provisionally changing the text of this draft legal act.

Accordingly, the Republic of Slovenia states as a summary its preliminary comments and concerns or proposals, which are understood to be additional to those already expressed at the DAPIX Working Party, and only exceptionally, the same positions are re-stated.

Preliminary comments and some proposed amendments:

1. concerning Article 11:

We propose to delete paragraph 2 of Article 11. The provision does not guarantee legal certainty and it seems that it is an additional obligation for data controllers, which might prove to be as such in practice - contrary or different to general data protection (information) policies.

2. concerning Article 12:

With respect to Article 12, paragraph 3, we are of the opinion that paragraph 3 should be deleted. Data controllers cannot be presumed to be responsible for providing legal advice to data subjects - usually, they are not administrative bodies and especially those from the private sector cannot be transformed into them by virtue of this draft legal act.

3. concerning Article 14:

We are of the opinion with respect to Article 14, paragraph 1, that the deadline for storing of personal data (data retention) should be communicated to data subject at least in a general (framework) manner, we deem this to be an important information right of the data subject. We are also of the opinion that the relationship of employer/employee should be taken into account, since employees can be considered to be data recipients in some case, not just data subjects.

4. concerning Article 16:

Specifics of public books or public registers that are established by detailed rules of national legislation should be regulated favourably in this Article. A general exception, referring to national (procedural) law would be preferred.

5. concerning Article 17:

We are highly sceptical with respect to the feasibility of enforcing the proposed right to be forgotten, especially to relation of the freedom of expression or works of history. Concerning Web 1.0 or Web 2.0 it is advisable to state explicitly that this provision has no influence on the public access to public judgments. This is needed not just because of national procedural rules, but also in respect of published judgments of international (criminal, human rights and other) courts or tribunals.

And paragraph 8 should be deleted, it designates a so called "false erasure".

At the end: due to the possible dangers of encroachment(s) on freedom of expression and possible dangers of "blocking/restricting access to information", Slovenia requests that it is explicitly mentioned in a footnote with respect to the entire Article that Slovenia expresses the reservation.

6. concerning Article 19:

With respect to Article 19, paragraph 2 it has to be made clear when does the moment arise that the data subject can opt out from the direct marketing. And the provision is too wide - all personal data, including sensitive ones, can be processed for direct marketing purposes.

Concerning paragraph 3 it should be made clear that prohibition only applies to direct marketing purposes.

It is also unclear whether these rules do apply also for political marketing purposes, purposes of cooperation with non-governmental organisations, humanitarian organisations etc.

Slovenia requests that it is to be explicitly mentioned in a footnote with respect to the entire Article as expressing the reservation.

7. concerning Article 20:

Any mentioning of "measures" should be deleted from Article 20, only "decisions" or "decision-making" are proper terms, in our opinion, that can be used. The term "measures" might be mis-interpreted, it could be related to other legal areas.

8. concerning Article 21:

In Article 21, paragraph 2, the entire paragraph should be deleted. It is understood that it is already included in the introductory part of paragraph 1 and general provisions of this draft legal act. As an "legislative advice" it does not bring any additional value, but it might unnecessarily cause some interpretative problems.

9. concerning Article 22:

The entire Article presents high and hardly completely assessable administrative burdens for data controllers, irrespective of their size, but is especially problematic for small and medium enterprises. Therefore, Slovenia requests that it is to be explicitly mentioned in a footnote with respect to the entire Article as expressing the reservation.

10. concerning Article 24:

The relationship between two (or several) data controllers, that are called "joint controllers" in Article 24 is unclear. It is necessary to have a written agreement. Also, if data controllers are a part of public sector, their competences and duties are prescribed by detailed rules of national legislation, certain interconnections are also prescribed by national legislation, and certain activities of theirs are also proscribed by national legislation. Therefore, Slovenia requests that it is to be explicitly mentioned in a footnote with respect to the entire Article as expressing the reservation.

11. concerning Article 25:

Concerning Article 25, paragraph 1, we opine that there is a problem with its connection with Article 3, paragraph 2, and its possible "extraterritorial component". Therefore, Slovenia requests that it is to be explicitly mentioned in a footnote with respect to the paragraph 1 of this Article as expressing the reservation.

12. concerning Article 26:

We opine that in Article 26, paragraph 4 should be deleted. It designates data controller as a joint controller that is co-responsible with data processor (who becomes a new data controller) who violated data controllers` instructions or contract. This type of possible result is illogical and unreasonable.

13. concerning Article 27:

It is questionable whether the entire Article 27 is really needed. It is understood that its provisions are already to be understood from the whole draft legal act. And if it is meant to be a sort of self-standing provision, then at least orders of independent judiciary are missing (such as in cases of data retention of electronic communications data).

Slovenia reserves for the future process of dialogue at the DAPIX the possibility to add additional comments or reservations.

FINLAND

The FI delegation notes that the wording of Article 10 of Directive 95/46/EC slightly differs from that of Article 14 of the proposed Regulation. The proposed Directive (Article 11) contains a similar wording, which has raised some questions. In order to remove doubts as to the exact meaning of the introductory phrase, it is worth considering whether it should be made more flexible e.g. as follows:

Article 14
Information to the data subject

1. Where personal data relating to a data subject are collected, the controller shall ~~provide~~ ***make available to*** the data subject ~~with~~ at least the following information:

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

   (b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);

   (c) the period for which the personal data will be stored; (d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;

   (e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;

   (f) the recipients or categories of recipients of the personal data;

   (g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;

   (h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.

[…]

Article 19

FI delegation supports the comments presented by some delegations on the wording of Article 19, paragraph 1 and raises some doubts as to the shift of the burden of proof as suggested by the Commission (the expression “compelling legitimate grounds” appears somewhat unclear as it is in the existing Directive used for the data subject). The use of public powers in Finland is provided for by law and it would seem strange if the authorities had to specifically demonstrate the existence of compelling legitimate grounds for the processing of data. The suggested provision should perhaps be clarified.

Article 20

FI supports the protection of the data subject against profiling in cases such as unwanted marketing. Moreover, the exact meaning of the expression “a measure which produces legal effects concerning this natural person or significantly affects” is some what unclear. There may be cases where profiling is necessary for the management of risk assessments, particularly for credit and insurance institutions. Such risk assessments should not be made too difficult. Article 9 of the proposed directive includes the word “adverse” (legal effects). Should it perhaps be added to Article 20(1) as well?

Article 21

FI proposes the addition of “State security and defence” as a ground for derogation into Article 21(1), as already proposed at the working party meeting. A reference to defence and State security has already been added to Article 2(2)(a). Furthermore, the FI delegation is of the opinion, that also processing for historical, statistical and scientific purposes should be mentioned as a ground of derogation in Article 21 (1) unless it is sufficiently taken into account in Article 83.
In addition, the reference to Article 5(a) in paragraph 1 seems misplaced. That reference appears to allow unlawful processing of data, which is most likely not the intended purpose of the provision.

Article 22

The question of implementing acts will be addressed separately. However, the reference in Article 22(3) to “independent internal or external auditors” raises doubts particularly as the criteria for proportionality is left to be decided in implementing acts.

Article 24

FI does not find this provision problematic. However, the FI delegation supports the SE and DE views, according to which the respective responsibilities of joint controllers may, particularly as regards public authorities, be based directly on legislation. Furthermore, in such cases each authority is under an obligation to advise the data subject on which authority to contact. That obligation is based on Finnish public law and does not require any provision to that effect in the data protection legislation.

Article 25

As some other delegations, FI wishes to draw attention to the number of employees as a criterion for the appointment of a representative. Due to the increasing number of services offered on the internet, it should perhaps not be the only criterion. However, the nature of internet-based services may also make it difficult to control compliance with this obligation.

Article 26

In the light of the discussions on the wording of Article 26(4), FI delegation wonders whether there has been a misunderstanding of the intended meaning. Some delegations have referred to unlawful data processing. Given the Commission's explanation, however, the provision should perhaps be slightly corrected e.g. as follows:

"If a processor processes personal data other than ~~as instructed~~ ***that designated*** by the controller, the processor shall be considered to be a controller ~~in respect of that~~ ***to the extent the*** processing ***concerns that data***. ***In such a case, the processor*** shall be subject to the rules on joint controllers laid down in Article 24."

SWEDEN

Introduction

The Presidency has invited delegations to send in proposals for amendments or comments regarding Articles 11-27 of the General Data Protection Regulation. Sweden welcomes the Presidency's initiative and presents in this paper some comments and preliminary proposals for amendments, in addition to those already put forward at the meetings of the working party. After some general comments, relevant articles are reproduced with our proposed amendments (***bold italics*** indicating proposed new text, ~~**bold strikethrough**~~ indicating proposed deletions and **[bold in brackets]** indicating points that need further consideration). We would like to underline that both the comments and proposals for amendments are preliminary and that we maintain a general scrutiny reservation and a reservation regarding the legal form of the instrument. We may provide new comments and suggestions when the working party revisits these articles.

Further, as we have already stated in earlier written comments, we are not convinced that the Commission should be empowered to adopt delegated acts in the extent proposed in the Regulation. In this document, we will however not provide comments regarding the issue of empowerments for the Commission, since that issue will be dealt with separately. Consequently, we have omitted the paragraphs containing empowerments for the Commission in this memorandum.

Administrative burdens

We are concerned about the new administrative burdens and requirements in the proposed Regulation. New administrative burdens should only be introduced if they are proportionate in relation to the benefit for the protection of individuals' privacy. It is important to bear in mind that the Regulation has an extremely wide field of application covering everything from natural persons acting on the Internet to taxation databases and bio banks. Requirements considered appropriate for a large company or a public authority handling sensitive information may be unreasonable for a natural person or a small company, e.g. a family restaurant. We therefore believe that there is a need for greater differentiation of the rules, based on the risks entailed by the processing. This is needed, on the one hand, to provide adequate protection for high-risk processing and, on the other, to avoid unnecessary bureaucracy for low-risk processing. These issues require a horizontal approach rather than an article-by-article discussion. We therefore welcome the Presidency's initiative to discuss these issues at separate meetings, and we wish to underline that the suggestions for amendments put forth in this memorandum is without prejudice to any future suggestions to adjust the proposal in a more comprehensive manner.

Article 11 Transparent information and communication

1. The controller shall***, where appropriate,*** have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights.

2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, **adapted to the data subject [delete/move to recital]**, in particular for any information addressed specifically to a child.

Comment

Although Sweden supports in principle the introducing of transparent and easily accessible policies it seems too far-reaching and bureaucratic to impose such an obligation on all controllers, regardless of the nature and extent of their processing. As stated above, we believe that new administrative burdens should only be introduced if they are proportionate in relation to the benefit for the protection of individuals' privacy. Therefore, we suggest introducing the qualification "where appropriate" as cited above. This change should be accompanied by an added recital in which the typical cases where a policy is needed is stated, e.g. when the processing implies some level of risk to data subject´s privacy.

We also suggest deleting or moving "adapted to the data subject" to a recital, as this obligation in its current drafting will often require disproportionate efforts by controllers. In fact, it will often be impossible to adhere to, for instance when the controller only knows the name and address of the data subjects. Considering the administrative sanctions connected to this provision according to Article 79.5, clarity as to the scope of the obligations is required.

Article 12 Procedures and mechanisms for exercising the rights of the data subject

1. The controller shall***, where appropriate,*** establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.

2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if ~~**several data subjects exercise their rights and their cooperation is**~~ necessary to ~~**a reasonable extent to**~~ prevent a ~~**n unnecessary and**~~ disproportionate effort on the part of the controller. The information shall be given in writing. ~~**Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.**~~

3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.

4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are ~~**manifestly**~~ excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the ~~**manifestly**~~ excessive character of the request.

[…]

Comment

In our view the requirement in Article 12.1 to establish procedures and mechanisms for providing the information and for the exercise of the rights of data subjects may certainly be appropriate for certain categories of processing – e.g. processing carried out by the provider of a social network – but not for others, e.g. processing carried out by users of social networks. It hardly seems reasonable that failure to establish such procedures and mechanisms in the latter types of processing should be punishable by administrative fines according to Article 79.4. We therefore believe that the provision needs to be redrafted for added flexibility or possibly exempted from the provisions on administrative sanctions. Pending a more horizontal solution to this and similar issues in the draft Regulation we suggest to insert the qualification "where appropriate" as cited above.

Even though we support the introduction of a fixed deadline in Article 12.2 we have doubts whether it is appropriate to set this deadline at a maximum of only two months. In any case, it does not seem justified to limit the possible exemption from the general rule of one-month to situations where several data subjects exercise their rights and their cooperation is necessary. It should be enough to establish that a further month is needed to prevent an disproportionate effort on the part of the controller, regardless of the cause. We would therefore propose a redraft to widen the scope and to move the deleted text to a recital, to serve as an example of when a disproportionate effort on the part of the controller could occur.

Further, we suggest deleting the obligation to provide information in electronic form since this, as was brought up by several delegations at the DAPIX meeting of June 2012, could prove very problematic in practice. For instance, this requirement raises serious security issues when dealing with sensitive data. To fulfil the obligation the controller will have to, inter alia, be able to positively identify the data subject and be able to arrange for a secure (encrypted) method of electronically providing the requested information. This is most likely not feasible for controllers in general.

As regards Article 12.4, we believe that the requirement that requests must be *manifestly* excessive before controllers may refuse to take action etc. could induce a burden that is not proportionate to the benefits it brings for data subjects privacy. It should be enough to find that requests are excessive.

Article 13 Rights in relation to recipients

The controller shall communicate any rectification or erasure carried out in accordance with Articles 16 and 17 to each recipient to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort.

Comment

Sweden has no comments regarding this article at this time.

Article 14 Information to the data subject

1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:

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

   (b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);

   (c) the period, ***when known,*** for which the personal data will be stored;

   (d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;

   (e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;

   (f) the recipients or categories of recipients of the personal data;

(g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;

(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.

2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.

3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate.

4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:

(a) at the time when the personal data are obtained from the data subject; or

(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.

5. Paragraphs 1 to 4 shall not apply, where:

(a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or

(b) ~~**the data are not collected from the data subject and**~~ the provision of such information proves impossible or would involve a disproportionate effort***,*** ***considering the risks represented by the processing and the nature of the personal data***; or

(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or

(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.

6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.

[…]

Comment

Making sure that data subjects are well-informed is of paramount importance for the practical implementation of data protection rules. Therefore Sweden supports a clear provision on the right to information. At the same time, we do not believe in upholding the same rules in this regard to all types of processing. In fact, upholding such a provision in all circumstances would add very little value for the privacy of data subjects. As was discussed at DAPIX, it hardly seems reasonable that the local restaurant should be obliged to inform you, inter alia, of the contact details of the supervisory authority when you call to make a reservation. This could however be required according to the current wording of this article. We therefore suggest to redraft paragraph 5 (b) to add flexibility and to make it possible to take due account of the risks of the processing and the nature of the personal data.

Further, it is clear that it will often not be possible to inform data subjects of the period for which their personal data will be stored already at the time of the collection of that data. We therefore support the suggestion put forth at DAPIX to add “where known” to Article 14.1 (c).

Article 15 Right of access for the data subject

1. The data subject shall have the right to obtain from the controller -**at any time [consider deleting]**, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information:

   (a) the purposes of the processing;

   (b) the categories of personal data concerned;

   (c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries;

   (d) the period***, where known,*** for which the personal data will be stored;

   (e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;

   (f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;

   (g) communication of the personal data undergoing processing and of any available information as to their source;

   (h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.

2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. ~~**Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.**~~

[…]

Comment

We suggest making the same adjustments to Article 15 as was suggested above concerning Article 12 and 14, i.e. to delete the obligation to provide information in electronic form and to add "where known" as regards information concerning the period that data will be stored. Further, we are not convinced that data subjects should have the right to access "at any time", considering that the exercise of this right shall be free of charge according to Article 12. According to Article 12(a) of Directive 95/46 data subjects have the right to access "at reasonable intervals". Even though we can support that data subjects should, in principle, have the right of access at any time, it seems that the current drafting of Articles 15 and 12 might entail an administrative burden that is not proportionate to the possible benefits to data subject´s privacy.

Article 16 Right to rectification

The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement.

Comment

Sweden has no comments regarding Article 16 at this time.

Article 17 Right to be forgotten and to erasure

4. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:

   (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;

(c) the data subject objects to the processing of personal data pursuant to Article 19;

(d) the processing of the data does not comply with this Regulation for other reasons.

[This paragraph needs further consideration and redrafting]

2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.
[This paragraph needs further consideration and redrafting]

3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:

(f) for exercising the right of freedom of expression in accordance with Article 80;

(g) for reasons of public interest in the area of public health in accordance with Article 81;

(h) for historical, statistical and scientific ~~**research**~~ purposes in accordance with Article 83;

(i) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;

(j) in the cases referred to in paragraph 4.

4. Instead of erasure, the controller shall restrict processing of personal data where:

(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;

(b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;

(c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;

(d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2).

5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.

6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.
[Move paragraphs 4-6 to separate Article]

7. The controller shall implement mechanisms to ensure that the time limits, ***if any,*** established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed. **[Move to recital or Article 23]**

8. Where the erasure is carried out, the controller shall not otherwise process such personal data. [**Consider deleting**]

[…]

Comment

The right to erasure is undeniably an essential part of data protection. However, we are uncertain how the current drafting of this article will work in practice. This is especially true of Article 17.2. For example, if personal data has been made public on the internet, it is hardly possible for controllers to even identify what third parties might be further processing that data. Further, Article 17.1 (d) is in our view too vague a criterion to be used in a provision that can lead to heavy administrative sanctions. We believe that Article 17.1-2 needs to be redrafted for the sake of legal certainty.

As we understand the explanations given by the Commission, the added word “research” in Article 17.3 (among others), in comparison to the wording of Directive 95/46, is not meant to impose any restrictions on processing for historical, statistical and scientific purposes. To eliminate uncertainty on this point we suggest deleting the word “research”.

As regards Article 17.4-6, we support the delegations that suggested that the rules governing restriction of processing should be moved to a separate article for the sake of clarity. It should also be considered whether restricting the processing of personal data should be an alternative to rectification in accordance with Article 16.

It is unclear why the article regarding erasure includes a paragraph containing an obligation to implement certain mechanisms regarding time limits. We believe that this provision should be moved to Article 23 or alternatively to a recital connected to that article. In any case, it should be clarified that this provision does not in itself constitute an obligation to determine the actual time limit. This could be achieved by adding “if any” as indicated above. Finally, we have not been convinced of the necessity of Article 17.8. The significance of this paragraph needs to be considered and if it is superfluous, it should be deleted.

Article 18 Right to data portability

1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.

2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.
[Article 18 needs further consideration]

[…]

Comment

In our view it is questionable if the right to obtain personal data in a format that allows further use and the right to transmit personal data into different processing systems can be derived from the right to protection of personal data. This is especially true of Article 18.2. Hence, we believe that the introduction of the right to data portability needs to be closely considered, not the least in view of the administrative burden that it entails. In any case, it should be considered amending Article 18.1 so that the right to obtain a copy of the personal data only applies to data that was supplied by the data subject. This would minimize the potential conflict between the provision and intellectual property rights etc.

Article 19 Right to object

1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object **free of charge** [**Consider deleting**] to the processing of their personal data for such marketing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information.

3. Where an objection is upheld pursuant to paragraphs 1 and 2, the controller shall no longer **use or otherwise** [**Consider deleting**] process the personal data concerned.

Comment

If the data subject believes that processing is not lawful under Article 6.1 (d), (e) or (f), he or she may require the controller to end the processing already pursuant to Article 6. The controller will then, most likely, have the burden of proving that the processing is lawful. Thus, the right to object comes into play when the data subject has objections, based on his or her particular situation, to *otherwise lawful processing*. Therefore, it may appear logical that Article 14 of Directive 95/46 requires the data subject to present compelling and legitimate arguments in order to exercise the right to object. In the proposed Regulation the burden of proof is shifted to the controller. However, there is no requirement as regards the quality of the arguments presented by the data subject.

The right of objection is especially problematic with regard to processing with a legal basis in Article 6.1 (e), as complete information often is of paramount importance, e.g. in real property and company registers. If there is a legal obligation to carry out the processing, pursuant to Article 6.1 (c), the right to object is not applicable. However, it may be essential to have complete information also in cases where the processing is carried out on the basis of explicit permission provided by law. One example is credit information databases handled by specially licensed private companies. Such databases are of fundamental importance for the functioning of the financial system and should not be subject to the right to object.

Processing with a legal basis in Article 6.1 (e) must, pursuant to Article 6.3, be governed by specific provisions in Union or Member State law. When adopting such legislation a balance must be struck between the interests involved. It may be argued that, in such cases, the EU or national legislator should, as in the current Directive, be able to decide whether the right to object should be applicable.

Against this backdrop we have doubts whether the proposed changes compared to Article 14 in the Directive are justified, especially as regards processing governed by Article 6.1 (e).

According to Article 19.2, an objection regarding processing for direct marketing purposes is free of charge (as in Article 14 (b) of Directive 95/46). However, already in Article 12.4 it has been established that objections under article 19 shall be free of charge. It therefore appears unnecessary to repeat this in art. 19.2. Further, it may be confusing to clarify this in Article 19.2 and not in Article 19.1. There is also a need to further analyse the consequences with regard to direct marketing of the changes made in Article 19.2 compared to Directive 95/46.

As regards Article 19.3 it would appear that “use or otherwise” is unnecessary.

Article 20 Measures based on profiling

1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.

5. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:

   (a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or

   (b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or

   (c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.

6. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.

4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject. **[Consider moving to Article 14 in order to make that article as exhaustive as possible.]**

[…]

Comment

In Article 20.1, it is proposed that the scope of the provision on automated individual decisions in Article 15 of Directive 95/46 shall be widened, inter alia through the use of "measure" instead of "decision". It is difficult to foresee the consequences of the proposal e.g. for risk assessments by insurance companies, selections of addressees for direct marketing and scoring in relation to credit applications. It is also difficult to foresee the consequences of Article 20.3, e.g. for the health sector.

It is, thus, necessary to clarify the scope of these provisions and the types of processing that they intend to target.

Article 21 Restrictions

1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in points (a) to (e) of Article 5 and Articles 11 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:

   (a) ***national security, defence and*** public security;

(b) the prevention, investigation, detection and prosecution of criminal offences;

(c) ~~**other public interests of the Union or of a Member State in particular**~~ an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters and the protection of market stability and integrity;

(d) ***other public interests of the Union or of a Member State*** [moved from c];

(e) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (a), (b), (c) and (d);

(g) the protection of the data subject or the rights and freedoms of others.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least as to the objectives to be pursued by the processing and the determination of the controller.

Comment

According to Article 13 of Directive 95/46, it is possible to make restrictions on grounds of "public security" and "defence". At the DAPIX meeting on 3–4 September 2012, the Commission clarified that Article 21.1 (c) ("other public interests") covers such restrictions. Since no change is intended, we believe that "public security" and "defence" should be explicitly mentioned also in the Regulation in order to avoid the impression that a change has been made.

We welcome the inclusion of "other public interests" in Article 21.1 (c) as it is difficult to enumerate exhaustively the public interests that may justify restrictions. This approach is in line with the Charter of Fundamental Rights of the European Union (Article 52). For the sake of clarity, we would suggest to move "other public interests" to a separate subparagraph.

Some delegations have proposed to eliminate the possibility to make restrictions regarding Article 5. This would constitute a change compared to Article 13 of Directive 95/46. On the one hand, we agree that it should not be possible to make exemptions from certain principles in Article 5; the principle of lawfulness being an obvious example. However, there are other principles to which restrictions may be necessary, e.g. the principle of transparency in Article 5 (a) and the restriction on processing for incompatible purposes in Article 5 (b). As regards the latter provision, it is true that processing for new incompatible purposes is allowed pursuant to Article 6.4 if the new processing has a legal basis in at least one of the grounds in Article 6.1 (a) to (e). However, as regards processing with a legal basis in Article 6.1 (f) there may be a need for restrictions of Article 5 (b). Therefore, in our view it is not possible to exclude Article 5 in its entirety from the scope of Article 21.

Article 22 Responsibility of the controller

1. The controller shall ~~**adopt policies and**~~ implement appropriate measures ***and, where appropriate, adopt policies*** to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.

2. The measures provided for in paragraph 1 shall in particular include:

   (k) keeping the documentation pursuant to Article 28;

   (l) implementing the data security requirements laid down in Article 30;

   (m) performing a data protection impact assessment pursuant to Article 33;

   (n) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);

   (o) designating a data protection officer pursuant to Article 35(1).

3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.

[…]

Comment

Sweden welcomes the abolition of the general notification requirement and the move towards an accountability-based approach. However, we are concerned about the new administrative burdens and requirements in the proposal. The requirement in Article 22.1 to adopt a data protection policy to ensure compliance may be appropriate for certain categories of processing – e.g. processing carried out by the provider of a social network – but not for others, e.g. processing carried out by users of social networks. For small and medium-sized companies – e.g. small shops and restaurants – the adoption of policies may constitute a mere paper exercise not providing any real benefit for the data subjects. We believe that a policy requirement should only apply where this is appropriate with regard to the risks involved for individuals.

As other delegations have pointed out, the non-exhaustive list in Article 22.2 raises issues of legal certainty, since breaches of this provision are sanctioned by heavy fines according to Article 79.6. Therefore, Article 22 should either be re-drafted or exempted from the provisions on administrative sanctions.

We have not been convinced of the need to introduce a specific requirement in *Article 22.3* for verification mechanisms in addition to the general requirement to adopt measures to ensure compliance. In any event, the requirement to introduce verification mechanism should only apply where appropriate.

Article 23 Data protection by design and by default

1. Having regard to the state of the art, ~~**and**~~ the cost of implementation***, the risks represented by the processing and the nature of the personal data***, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. ~~**In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.**~~

[…]

Comment

Sweden welcomes the intention behind Article 23 and the attempt to introduce the principle of privacy-by-design in the proposal. However, at this point it is still difficult to overview the consequences of the proposal.

An initial observation regarding Article 23.1 is that it must be possible to take into account the risks involved and the nature of the personal data (see Article 30.1). An important question is to what extent the provision will require the reconstruction of existing IT systems, which may be very costly.

Article 23.2 seems to require the implementation of mechanisms that – by default – ensure compliance with Article 5 (c). It is necessary to clarify what "by default" means in this context; does it e.g. mean that IT systems must have built-in mechanisms that automatically erase data not fulfilling the requirement "minimum necessary"? This may in some cases prove very costly. It is therefore problematic that Article 23.2 seems to lay down an absolute requirement, which does not allow for costs and appropriateness to be taken into account, which is possible under Article 23.1.

The last sentence in Article 23.2 seems to focus on privacy settings in social networks. However, Article 23.2 has a much larger field of application. The sentence in question may be construed as a requirement for all systems to – by default – hinder publication on the internet. However, this may be the principal purpose of certain categories of processing, e.g. certain public registers published on the internet. We would, therefore, propose to redraft this sentence to make it less general and move it to a recital.

Article 24 Joint controllers

Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them***, unless the respective responsibilities of the controllers are determined in Union law or national law to which the controllers are subject***.

Comment

A possible interpretation of the phrase "Where a controller determines the purposes…" is that Article 24 is not applicable where the purpose etc. of the processing is determined by Union or national law. In such cases, it will not be possible for the controller to determine the purposes. However, as we understood the Commission's explanations during DAPIX 3-4 September 2012, this is not the intention behind the provision. Therefore, it may be necessary re-draft the article in order to avoid misinterpretations.

Further, we have understood that the intention behind Article 24 is not to exclude the possibility to regulate the responsibilities of joint controllers in Union or Member State law. For public authorities this may in some cases be the most appropriate solution. Therefore, it should be clarified that the possibility for controllers to make arrangements pursuant to Article 24 only applies when the matter is not regulated in Union or national legislation.

Article 25 Representatives of controllers not established in the Union

1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.

2. This obligation shall not apply to:

   (a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or

(b) an enterprise employing fewer than 250 persons; or

(c) a public authority or body; or

(d) a controller offering only occasionally goods or services to data subjects residing in the Union.

3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.

4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.

Comment

At this point we have no other comments than the ones delivered at DAPIX 3–4 September 2012.

Article 26 Processor

1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and-**ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and [Consider deleting]** shall ensure compliance with those measures.

1bis. ***The processor shall not process personal data except on instructions from the controller, unless required to do so by Union or Member State law.*** [Moved from Article 27] ***The controller and the processor shall document the instructions in writing.***[Moved from Article 26.4]

2. The carrying out of processing by a processor shall be governed by a contract or other legal act, ***in particular a legislative measure in Union or Member State law*** [This clarification could instead be inserted in a recital]**,** binding the processor to the controller and stipulating in particular that the processor shall:

(a) act only on instructions from the controller ***pursuant to paragraph 1bis*****~~, in particular, where the transfer of the personal data used is prohibited~~**;

(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;

(c) take all required measures pursuant to Article 30;

(d) enlist another processor only with the prior permission of the controller;

(e) **~~insofar as this is possible given the nature of the processing~~** ***where appropriate***, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;

(g) ***delete or*** hand over ***the personal data*** **~~all results~~** to the controller after the end of the processing, **and not process the personal data otherwise [Consider deleting]**;

(h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.

3. **~~The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.~~** [Moved to Article 26.1bis]

4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing **~~and shall be subject to the rules on joint controllers laid down in Article 24~~**.

[…]

Comment

On a general note, we support the delegations asking for an in-depth study of the implications of this article for cloud computing.

As regards Article 26.1 we believe that simplifications are possible without changing the content. Since the rights of the data subjects are guaranteed in the Regulation, it would appear that it is sufficient to require the controller to ensure compliance with the Regulation. It should therefore be possible to alleviate the text by deleting "ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and".

For reasons of clarity we would propose to move the requirement for the processor to process personal data only on instructions from the controller from Article 27 to Article 26.1bis. It would then be logical to move the documentation requirement in 26.3 to the same paragraph. As the obligations of the processor in Article 26.2 are documented in the agreement, it is difficult to see the need for an additional documentation requirement. The requirement to document should therefore only regard the instructions from the controller.

During the DAPIX meeting on 3–4 September 2012, the Commission confirmed that "legal act" in Article 26.2 is to be understood as including Union or Member State legislation. We believe that this should be clarified either in Article 26 or in a recital.

It should be clarified that the obligation in Article 26.2 (a*)* is a reflection of the obligation set out in Article 26.1bis.

In Article 26.2 (c) it should be clarified that it is left to the parties to decide whether the processor should hand over or delete the personal data when the processing ends. "Personal data" should replace the rather vague expression "all results". Further, it is unclear in what way it would be possible to process data that has been deleted or handed over to the controller. It should therefore be considered to delete "and not process the personal data otherwise".

As regards *Article 26.4*, we have doubts whether it is appropriate to define a processor as a controller when he or she acts without instructions from the controller. Such processing is unlawful pursuant to art. 27 (moved to art. 26.1bis above) and can lead to administrative sanctions pursuant art. 79.6 (g). The data subject would further have a right to compensation from the processor under article 77. Thus, it is clear that the processor will bear the responsibility for the unlawful processing, even if the processor is not considered as controller. In any event, the reference to Article 24 should be deleted. It is inappropriate to establish a joint controllership between the controller and the processor for the processor's unlawful processing and require an arrangement regarding this processing.

Article 27 Processing under the authority of the controller and processor

~~**The processor and**~~[Moved to Article 26] ***A***ny person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.

Comment

We believe that the obligation for the *processor* to process only on instructions from the controller should be moved to Article 26.

In practice, it may be difficult, or even impossible, for persons acting under the authority of the processor (e.g. an employee) to verify whether the processor's (e.g. an employer's) instructions correspond to instructions from the controller (e.g. a customer of the employer). However, according to Article 79.6 (g) the employee shall be imposed a fine in case he or she follows instructions of the employer (processor) going beyond the instructions from the employer's customer (controller). Against this backdrop, Article 27 may need to be re-thought for reasons of legal certainty for persons acting under the authority of the processor.

UNITED KINGDOM

General Comments:

We welcome the opportunity, provided by the Presidency of the Council, to make general comments and suggested textual amendments on Articles 11-27 of the proposed Regulation. At this stage, we would want to place a general scrutiny reserve on these Articles as there are a number of cross-cutting provisions that interact with later Articles and we would want to consider the package as a whole before reaching a definitive view on all the issues contained within these Articles.

There are a number of issues that we have previously raised as part of the UK submission on draft amendments to Chapter I & II of the proposed Regulation. Given the Presidency has decided that these issues – delegated and implementing acts, administrative burdens, and public-private sector split – will be looked at horizontally, we do not intend to comment further on these areas at this stage.

Choice of Instrument – Arguments for a Directive:

We would, however, reiterate our view that the proposed general Regulation should be a Directive. The UK would recommend a Directive as a better choice of instrument for the following reasons:

1. It allows a more nuanced instrument, with detail where it is needed, and flexibility where it is needed.

- A Regulation must necessarily have a level of detail that allows all of its provisions to be directly binding on data controllers. But in data protection, a "one size fits all" approach does not work for every provision.

2. The subject matter is not well-suited to a Regulation.

- Data protection is an EU fundamental right. The concepts within this area are quite different to the technical areas we are used to seeing regulated under Regulations. Fundamental rights, like human rights, are best legislated for via high level principles set out in instruments that allow users of the legislation to strike a balance, subject to the supervision of courts.

- A Regulation needs subject matter that lends itself to technical prescriptive regulation – data protection is not such an area. The choice of a Regulation means that while some areas are too prescriptive, others by their very nature are not capable of being sufficiently prescriptive for purposes of a Regulation that is directly effective. This point was picked up recently by the Council Legal Service, who noted that some of the provisions pushed at the boundaries of what could properly be included in a directly effective Regulation.

- This points to data protection being an area that is best regulated by way of a Directive. Some flexibility at national level is beneficial and need not make the playing field too uneven.

- A Directive would allow Member States to go further where they wish to impose higher standards. It is a very odd thing to place a cap on the level of fundamental rights that can be afforded to citizens.

3. A Directive would be easier to implement and more user-friendly.

- This is particularly so for individuals, small businesses and charities trying to understand their rights and obligations.

- Looking at the package as a whole – a package consisting of two Directives could be implemented in one piece of national legislation so everything is in the one place for users.

Historical, Statistical and Scientific Research Purposes

We request a scrutiny reservation in respect of the application of the Regulation and exemptions in relation to processing for historical, statistical and scientific research purposes. In particular we would seek clarity on whether exceptions should apply to Articles 14-19 (apart from Article 17 where a reference has already been made).

Request for written CLS opinion

The UK would ask the Presidency to request that the Council Legal Service provide a written opinion based on the comments they raised orally at a recent JHA meeting on the choice instrument and the implications of having a Regulation governing legislation in this area.

Article	Relevant Recitals	Proposed Text/Suggested Amendments	Commentary
CHAPTER III – RIGHTS OF THE DATA SUBJECT			
11 – Transparent information and communication	Recital 46	11 - Recommend deleting the entire article	The UK considers that Article 11 is unnecessary. It overlaps with the obligation in Article 5(a) that data should be processed in a transparent manner in relation to the data subject. Furthermore, it risks presenting a disproportionate burden on SMEs.
11(2)		11 (2) - recommend removal of **"adapted to the data subject, in particular for any information addressed specifically to a child."**	If this provision is retained, the UK considers that the wording of paragraph 2 should be limited to providing information in an intelligible form, using clear and plain language. We believe the reference to "adapted to the data subject" is a step too far and will impose disproportionate burdens on the controller
12 – Procedures and mechanisms for exercising the rights of the data subject	Recital 47		
12(1)		Recommend deletion of 12(1)	The UK considers that this paragraph should be deleted. The relevant articles already set out the data subject's rights. The requirement that the controller should "establish procedures" and "provide mechanisms" is over-regulation: as long as controllers ensure that the rights of data subjects are respected, there is no need to also set out the manner in which those rights are given effect to. Further, the requirement that the controller should provide means for requests to be made electronically runs the risk of not being technology-neutral. It will also become out of date very quickly, in a world where information is already sent by automated means far more often than on paper.

12 (2)		12 (2) – Recommend removal of **"within one month of receipt of the request"** and replaced with **"without excessive delay"** (as per Article 12(a) of the 1995 Directive) Delete from "this period" to "controller" and from "where the data subject" to the end of the paragraph.	The UK considers the timeframe of 1 month for the data controller to inform the data subject to be too prescriptive. It is not clear what "any action" means. It could refer to delivering on the rights in Articles 13 and Articles 15 to 19 or it could refer to action short of delivering on those rights. The terminology "and shall provide the requested information" is problematic because some of the rights do not concern the provision of information to the data subject. The ability to extend the period during which "action" must be taken if "several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller" is vague and unhelpful. "Several" means more than two but, at least as far as the English language version is concerned, does not connote a large number. It is not clear why the need for the cooperation of the data subjects is the only ground on which the relevant period may be extended. If a request from one data subject is complex and requires significant resource to give effect to their rights this would surely also be a good reason to extend the period at the end of which the relevant "action" must be taken. Data controllers with little resource or which hold complex data or data in large quantities are likely to find this timeframe very difficult to work with and may face multiple sanctions under Article 79 (4)(a) for failing to take the requisite action in the relevant timeframe. At a time of scarce resources this may put an intolerable strain on public and private sector organisations alike. As for Article 12(1), the reference to electronic form is not technology-neutral and should be removed. Furthermore, using automated means to request information or in order to exercise the relevant rights is already so commonplace that this wording seems unnecessary.

12(2)		Suggest delete the last sentence of para 2: "~~Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.~~"	The last sentence of paragraph 2 requires information to be provided electronically where requested in this form. However this is often not appropriate in terms of data security, and may not be the data subject's preferred means of receiving the information. There seems no justification in using a potentially less secure form of communication as the default.
12(3)		Delete "refuses to take action" and substitute "does not take action". It would also be helpful to make it clear which of these articles this obligation refers to. Delete "and on the possibilities" to the end of the paragraph.	The drafting is problematic. It might be better to link this paragraph to a situation where the relevant action is not taken, because a data controller may not actively refuse to take the relevant action, but may simply ignore the request or may be unable to deal with it for some other reason. The mentioning of complaints/judicial remedies may have the effect of increasing the number of complaints/cases.
12 (4)		12 (4) – Recommend the removal of this paragraph	The UK supports consumer protection and individuals' rights. Access to your personal information is important because it is from those access rights that other rights can be asserted. But in a time of scarce resources burdens on data controllers must be proportionate. In the United Kingdom data controllers are able to charge a fee (if they want to) to the data subject for exercising the right of access to the data the controller holds about them (this is the right under Article 12 of the 1995 Directive and Article 15 of the proposed instrument). Charging a fee is permitted under Article 12(a) of the 1995 Directive, provided that the fee is not excessive. Under our data protection act, which implements the 1995 Directive, the maximum fee which the data controller can charge is currently £10 – roughly 15 Euro. The fee was never intended to allow the data controller to recoup the cost of responding to the request, which is inevitably more than 15 Euro. Instead, the fee acts as a filter mechanism to deter speculative requests for personal data.

			We consider that the mechanism of charging a small fee works because it will not deter someone who genuinely wants to see their data, and it helps data controllers because it stems the tide of speculative requests. These are likely to rise as the ease with which data subjects can make requests for their information increases (for example the requirement at Article 12(2) that data subjects who make the request in electronic form should be provided with a response in electronic form unless otherwise requested by the data subject). Sending an e-mail requesting your data will take a couple of minutes. Whilst other member states may not have a mechanism for charging a small fee to put off speculative requests in this context, we are aware that it exists for requests under freedom of information legislation in other member states. Again, the mechanism acts as a filter in these examples to ensure that those who access public services do actually need them, and charging a small fee deters casual use. We therefore consider that our ability under the '95 Directive to allow data controllers to charge a small fee for giving data subjects access to their information should be retained to stem the volume of requests. This volume is already high. For instance the United Kingdom Border agency currently deals with 450 requests per week – that is 22 000 a year. Our Department for food and rural affairs has also argued for the retention of the fee, stating that it has experienced a significant number of cases where the small charge of £10 has deterred speculative requests. We think that in a time of scarce resources the abolition of the ability to charge a fee must be rethought. We also wonder whether the increase in volume of requests has been taken into account in the Commission's impact assessment.

			The UK is of the view that the ability to charge a small fee for subject deters speculative requests. For certain sectors the volume of requests is already very high and the removal of the fee is likely to increase these figures further. e.g. The United Kingdom Border Agency currently deals with 450 requests per week – which amounts to 22 000 a year. Furthermore, the UK considers that charging a fee is compatible with fundamental rights. Article 8 of the ECHR as re-stated in Article 7 of the Charter guarantees the right to respect for private and family life. Article 8 of the Charter re-states the specific right to the protection of personal data. Article 8 of the Charter, like Article 8 of the ECHR is in any event a qualified right. Interference with qualified rights is permissible where the interference is prescribed by law, in pursuit of a legitimate aim, necessary in a democratic society and proportionate. Insofar as charging a small fee could be seen as an interference with a qualified right, such an interference would be lawful, provided it conformed with those principles[1]. In this context, the legitimate aim behind charging the fee is to dissuade abuse of the system which would put a disproportionate burden on data controllers. The fee which data controllers may presently charge under UK law is proportionate. It is nominal, and there is no obligation on the data controller to charge the fee.

[1] In other contexts which engage Article 8 of the ECHR, courts been mindful of the fair balance which must be struck between the competing interests of the individual and of the community as a whole, and to the wide margin of appreciation enjoyed by States in determining the steps to be taken to ensure compliance with the Convention. The courts have been slow to find an implied positive obligation which would involve imposing on the State significant additional expenditure, which will necessarily involve a diversion of resources from other activities of the State in the public interest (see for example *Sentges v. The Netherlands*, ECtHR, decision of 8 July 2003 no. 27677/02). In the context of Article 10, the system of levying fees from subscribers to ensure that public service broadcasting could fulfil its function informing public opinion has been held to be justified under Article 10(2), on the basis that the relevant rules pursued the aim of protecting the rights of others (see *Kretzchmar v. Germany* – app. No. 26907/95 (admissibility decision of 12.4.96)).

13 – Rights in relation to recipients			The UK supports this provision in principle. We do not believe that communication of rectification or erasure to all to whom the data has been disclosed will be possible in an online environment
14 – Information to the data subject	Recitals 48-50		
14(1) –(5)		14 1 (a) Recommend amending as follows "the identity and the contact details of the controller or **alternative"** Create two provisions, one dealing with the situation where information is obtained from the data subject and one where it has not.	14 (1) (a) In some cases the details of the data protection officer are not allowed to be disclosed. In general, we prefer the structure of Articles 10 and 11 of the Data Protection Directive 95/46/EC which set out separately the requirements where information was or was not collected from the data subject. We do not think proposed Article 14 very clear as it sets out general provisions relating to both, followed by a complicated set of exceptions and qualifications, some of which do not work together (see below).
14(1)-(5)		Replace references to "collect" with "obtain"	The terms "obtain" and "collect" are used interchangeably throughout the provision, as are "data" and "information". It is good drafting practice to use consistent language if these are intended to mean the same.
14			

14(1)-(5)		14(4)(b) - suggest delete the words “at the time of the recording, or”	Query whether “recorded” is the same as collected/obtained? In paragraph (4)(a), does this mean when initially written down or entered into a processing system? Does it only apply the first time information is recorded? The words “at the time of the recording” in para 4(b) are confusing and do not add to the separate alternative time limit of “within a reasonable period after the collection”.
14(1)		14(1) – Full stop at end of para 1(b). The remaining paras (c)-(g) go into a separate sub-paragraph, to be qualified by similar words at the end of Article 10 DPD 95/46/EC, i.e.: “In so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.” Para 9(h) can then be deleted. It should clearly only be a qualification on the preceding paragraphs, rather than a freestanding paragraph suggesting even more information might be supplied than the substantial amount specified in preceding paragraphs.	The equivalent provision in the existing Data Protection Directive 95/46/EC requires identity and purposes to be provided each time, whereas further information such as recipients, whether questions are obligatory, consequences of failure to reply and rights of access and rectification were required only “insofar as information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.” We think that is a more proportionate approach, rather than requiring controllers to provide all this information in each case to every data subject whether required for fair processing or not. Alternatively, we think there is merit in the suggestion that controllers should only be required at first instance to give the information in para 1(a) and (b), and to give contact details where the data subject can be given the remainder if interested. This would target the burden on controllers to those data subjects who actually want the additional information.

14(1)(f)			Disclosing the sources of information to a data subject can have implications for company secrets and commercial confidentiality. The text now exposes these sorts of areas because there is a blanket requirement to provide the information which is not subject to the "fair processing" qualification at the end of Article 10 DPD 95/46/EC This should be addressed by reinstating the qualification that information in para1(c)-(g) only has to be provided where necessary for fair processing – that will import a balancing mechanism that can address issues such as commercial confidentiality.
14(4)(a) and 14(5)(a) 14(2) and 14(5)(a)		No neat fix for these provisions – the Article as a whole needs to be re-drafted and re-structured so it works together coherently.	These two provisions do not seem to work together. On the one hand, the controller has to provide all the information in paras 1-3 to the data subject at the time of collection, but then para 5(a) disapplies this where the data subject already has the information in paras 1-3. These seem to cancel each other out completely. If the information is collected from the data subject, this means he/she will already have it and paras 1-3 will never apply to information that has come from the data subject. Similarly, paras 1-4 are disapplied when the data subject already has the information in paras 1-3 – which means that the obligation in 14(2) to tell the data subject whether provision of information is voluntary or obligatory will be cancelled out automatically in every case.

14(2)		Recital 48 – add a final sentence "Provision of personal data is obligatory if it is necessary for a particular transaction or form of processing."	Recital 48 should make clear what is meant by "obligatory" and "voluntary" data.
14(5)(a)		5a – amend as follows: "the data subject already has access to the information referred to…." OR add a new sub-para (e) so that paras 1-4 shall not apply where:" the data is publicly available".	It is unclear whether data the data subject "already has" means has in their possession, or extends to has access to. We agree with other Member States that information that controllers should not be expected to give all this information to data subjects where the information is publically accessible in any event.
		14 (1)(c) – Recommend inserting the words **"where known"** to qualify the provision for notifying the data subject of the period for which personal data will be stored.	It will not always be known at the point of collection how long the data will need to be stored for.
14(5)(b)		14(5)(b) – delete "the data are not collected from the data subject and the" add the words "in particular for processing for statistical purposes or for the purposes of historical or scientific research"	This disapplies 1-4 where data is not collected from the data subject and the provision of information is impossible or involves a disproportionate effort. The implication is that where data is collected from the data subject, the controller is expected to provide the information – including where it is impossible or disproportionate. This is obviously absurd. The final sentence of Article 11 DPD 95/46/EC highlighted the application to processing for statistical, historical or scientific research principles and we think that should also be included here.

14(5)(c)		14(5)(c) – delete "the data are not collected from the data subject and "	This disapplies paras 1-4 where data are not collected from the data subject and recording or disclosure is expressly laid down by law – we cannot see any logical reason why data controllers should give all this information to data subjects where the need to collect information from data subjects themselves is expressly laid down by law.
14(5)(d)		14(5)(d) – delete "the data are not collected from the data subject and"	Similarly to the above two points, the drafting suggests that the controller is expected to give information to the data subject that is collected from elsewhere even when it will impair the rights and freedoms of others.
15 – Right of access for the data subject	Recitals 51-52		
15(1)			As a general point, much of the information required to be given to data subjects under Article 14 is repeated as information that they have access to under Article 15. The intention is apparently that Article 14 only requires a high level of generality where Article 15 requires greater specificity. But we do not see the need to duplicate in this way.
15 (1)		15(1) – delete "at any time" and replace with "at reasonable intervals provided for in Member State law".	Para 1(d) gives data subjects access to information about the period of storage, which is not always obvious to a controller. We do no think it is proportionate for the right of access to be exercised "at any time". This needs to be more circumscribed, otherwise controllers may be overwhelmed by frequent requests. Member States should be able to determine what constitute "reasonable intervals" in national legislation.

15(1)(b)		Clarify or delete Article 15(1)(b)	It is unclear what is meant by "categories of personal data concerned" – although used in DPD 95/46/EC, neither instrument makes this clear. If this cannot be clarified, consideration should be given to deleting it.
15(1)(h)			It is quite unclear what is meant by "significance and envisaged consequences of processing". It also appears to go beyond the general understanding of access rights, which should be to the actual personal data rather than the results of processing it. This provision seems to be particularly aimed at profiling, and yet Article 20(4) uses different language to describe what must be provided under Article 14 (i.e. "the envisaged effects of such processing on the data subject"). Articles 14,15(1)(h) and 20(4) should all use consistent language and Article 20(4) should cross-refer to Article 15. Does the information provided under Article 15(1)(h) add to that provided under 14? If not, this should be something reserved for access rights under Article 15 rather than given as a matter of course under Article 14.
15(2)		Delete all of Article 15(2)	Article 15(2) simply repeats the first sentence of Article 15(1)(g) and should be deleted. As with Article 12(2), the default mode of communication in the second sentence should not be electronic as data security may favour a more secure means of communication. This should also be deleted.

16 – Right to rectification	Recital 53	16 – Recommend clarification of what and who defines **"incomplete personal data"** Add the words in italics to Article 16: "The data subject shall have the right, *where necessary and reasonably practicable*, to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, *as appropriate and having regard to the purposes for which they were collected or for which they are further processed*."	The UK would want clarification on who determines if data is complete or incomplete. Completion should be tied to the purposes of processing, otherwise it becomes a subjective matter. Article 12(b) of the DPD 95/46/EC qualified the right to rectification with "as appropriate" – we think Article 16 should retain qualifications for both the right to rectification and completion and have suggested text opposite.
17 – Right to be forgotten	Recital 53-54		The UK has concerns that the "right to be forgotten" may raise unrealistic expectations among data subjects that any data placed on the internet might later be deleted, leading young people in particular to be more reckless with their personal data. Compliance with this provision is likely to place disproportionate burdens on organisations, and in particular SMEs. Although Article 21 allows Member States are able to restrict the right to be forgotten where it interferes with freedom of expression, it is unlikely that controllers will be able to make complex determinations about the balance between the right to be forgotten against rights such as free expression and will err on the side of caution, particularly in view of the large mandatory fines proposed elsewhere in the Regulation. This may produce unintended consequences such as adversely impacting on the historical record and imposing a chilling effect, particularly on the internet.

			We think the proposal also misses its target as individuals posting "late-night" photos on social networking sites will be acting in a purely private capacity so will not be covered by the Regulation at any rate.
17(1)		17(1) – Amend the opening sentence by deleting the words indicating with a strike-through mark - as follows: **The data subject shall have the right to obtain from the controller the erasure of personal data relating to them ~~and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child~~, where one of the following grounds applies**: "	Once data has been erased, there will surely be no data in existence that could be further disseminated, so the opening sentence should only refer to erasure. The phrase "especially in relation to personal data which are made available by the data subject while he or she was a child.." is not needed and should be deleted. The right either exists for all data subjects, or it does not – to add that it especially applies to a certain category causes confusion and casts doubt on its application to others.
17(1)(a)-(d)		Either add the words "as appropriate" to the opening words of Article 17(1) … **"The data subject shall have the right, as appropriate, to obtain**…." OR Limiting the grounds giving rise to a right to erasure, for example as follows:	Article 12(b) DPD 95/46/EC qualifies the right to erasure with "as appropriate", however proposed Article 17 gives data subject an absolute right as long as grounds (a) – (d) (which are very wide) are met. This is problematic as almost any transgression of the Regulation, including those wholly unrelated to data quality, might give rise to a right to erasure. In particular, the fact that the data subject exercises his or her right to object should not automatically trigger a right to erasure. This needs to be addressed by either limiting the grounds that can give rise to the right to erasure to those relating to data quality, or introducing a similar qualification to "as appropriate" as in the current Directive.

		Delete paragraph 1 and replace with: "**1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them where it is incomplete or inaccurate or, where appropriate, it does not comply with this Regulation for other reasons.** "	
17(2)		Article 17(2) should be deleted	Article 17(2) should be deleted for the reasons given above regarding the potentially serious adverse implications of this new mechanism, which we think creates more problems than it solves. It also seems to go beyond the scope of data protection law. If retained, it should be made clear what concrete steps data controllers are expected to take in respect of third parties. The concept of proportionality needs to be added to the steps expected to be taken. It should not apply to paper copies of personal data. The final sentence of para 2 says that a controller who "has authorised a third party publication" should be considered responsible for that publication. It is most unclear what consequences would follow from that attribution of responsibility – but it does not seem to add to the controller's responsibility under this Regulation and should therefore be deleted.
17(3)			The edict that the controller shall carry out the erasure "without delay" is confusing when read with the alternative time limit of one month in "without delay" in Article 12.

17(3)(d)		17(3)(d) – Recommend this paragraph reads: "for compliance with **or to avoid a breach of** a legal obligation to retain the personal data by Union or Member State law to which the controller is subject.." Delete the words indicated with a strike-through in para 3(d): "(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject. Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued"	Not every instance of processing carried out for legal or regulatory compliance reasons will be specifically required by law. In certain cases such processing will be undertaken as part of a prudent risk-management programme designed to avoid a breach of law The requirements that Member State laws should meet a public interest objective etc are inappropriate and should be deleted. In particular, it is most unclear what the "essence of the right to the protection of personal data" means.
17(3)(e)			It is confusing to say that the alternative procedure of restricting data is an exception to erasure. We suggest this is deleted. If necessary, para 3 could be made subject to para 4.
17(3)			There should be an exception for creditworthiness and credit scoring, which is needed to facilitate responsible lending, as well as for judicial proceedings.
17(4)(a)		Remove sub para (a) and re-letter the remaining sub-paras.	The restriction of processing while accuracy is contested belongs in Article 16 on the right to rectification.

17(4)(b)		17(4)(b) should be amended as follows: "the controller no longer needs the personal data for the purposes of processing for which they were collected or further processed, but the data has to be maintained for ~~purposes of proof~~ the purpose of defending legal claims" It should be clarified in recitals that defence of legal claims may include those which may be made as well as those already initiated.	The opening words should refer to the controller's purposes for processing rather than particular tasks this may be related to. "maintained for the purposes of proof" is too narrow – this should include retention of information for the purpose of defending potential legal claims.
17(4)(d)		Delete Article 17(4)(d)	The data subject will have a right to data portability separately under Article 18(2) – there is no need to introduce a mechanism where data can be restricted prior to that separate right being exercised. .
17(6)			The Regulation is silent on why a restriction on processing would or could be lifted, but it seems to imply that it could be. How?
17(7)		Delete the words indicated by the strike-through: "The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data ~~and or for a periodic review of the need for the storage of the data~~ are observed"	The requirement that controllers set up mechanisms for periodic review of the need for storage does not fit in an Article primarily about erasure and the right to be forgotten. This needs to be moved to Chapter IV on controller's general obligations. A further example of a double meta-requirement; not only must data controllers erase the data, they are also required to have time limits in place for this and mechanisms to ensure these are observed.

17(8)		Delete Article 17(8)	This sub-para is superfluous – if data has been deleted it cannot be otherwise processed. This seems simply to be saying that once you have deleted personal data it should stay deleted. It would appear to be unnecessary.
18 – Right to data portability	Recital 55	We consider that Article 18 should be deleted. If retained, there should be an exemption for data held for historical, scientific research or statistical purposes.	The UK supports the concept of data portability in principle but considers it not within scope of data protection, as it seems to address consumer empowerment so belongs in a consumer law or competition measure. It is certainly not appropriate for this to apply to the public sector, but also raises serious issues about intellectual property and commercial confidentiality for all controllers. Data portability would also potentially increase the risk of fraud as it may be used to fraudulently obtain the data of innocent data subjects. If retained we would want an exemption for data held for historical, scientific research and statistical purposes The UK Call for Evidence indicated that this provision could cost businesses between £100,000 - £5,000,000 with the likelihood that costs would be passed onto consumer through higher prices for services.

19 – Right to object	Recital 56-57	We support Article 19, but with the qualification that the exemptions in Article 21 remain.	The UK needs to consider this article in further detail to ensure that it is workable and that there are minimal impacts upon controllers and that legitimate and vital processing is not prevented
19(1)		Paragraph 19(1): delete "compelling". Article 19(1) is engaged when the processing is based on points (d), (e) and (f) of Article 6(1) –	This is more restrictive than what was found in Article 14(a) of the '95 Directive , which was worded "at least in the cases referred to in Article 7 (e) and (f) (these more or less replicate Article 6(1) (e) and (f) of this instrument). It is unclear what happens when there is more than one possible ground in Article 6 on which the controller could rely. If the particular form of processing could fall within "processing necessary for the performance of a contract" under Article 6(1)(b) and Article 6(1)(f) – legitimate interests, what is the position then as regards the right to object? Could the controller circumvent the application of the right by asserting that the controller only relied on Article 6(1)(b) and not 6(1)(f), even though 6(1)(f) was potentially available? Under the directive Member States could if they so wished ensure that this did not happen by implementing the right to object more widely, so that it covered a broader range of processing. Of course this is not possible under a Regulation, but it would be in a Directive, going back to the wording of the '95 Directive "at least in cases referred in Article 7(e) and (f)". It is not clear why the ground to object does not extend to processing which takes place on the basis of Article 6(1)(c), because the difference between 6(1)(c) and 6(1)(e) is marginal. We do not consider that "compelling legitimate grounds" is sufficiently clear, and question what the relationship is between "compelling legitimate grounds" here and the processing of data for "legitimate purposes" under article 6(1)(f).

19(2)			In relation to Article 19(2) it would be helpful to have a definition of direct marketing.
19(3)		At Article 19(3) add the words "save for demonstrating compliance with the obligations imposed under this instrument".	In relation to Article 19(3) it is not clear how the obligation not to use or otherwise process the personal data concerned fits in with the obligation in Article 22(1) to be able demonstrate that the processing of personal data is performed in compliance with the Regulation and Article 28(1) to maintain documentation of all processing operations under the responsibility of the controller and processor. If the objection to the processing is upheld, the controller would need to demonstrate that they had abided by the requirement not to contact an individual for direct marketing purposes, for example? Should 3 say "save for demonstrating compliance with the obligations imposed under this instrument"?
20 – Measures based on profiling	Recital 58	We are placing a general scrutiny reserve on this Article	Given the possibility of a fine of up to €1m or 2% of global annual turnover for breaching this Article, businesses and other organisations will need greater clarity over the scope of Article 20. The UK considers there is a lack of clarity in 20(4) as to whether profiling carried out to deliver content to an individual, for example, through behavioural advertising falls within the scope of this Article. seek clarification on whether the Commission consider profiling for behavioural advertising and related activities to "produce legal effects or significantly affects" the data subject.
20(1)		Article 20(1): replace "natural person" with "data subject".	

20(2)			The UK needs to consider further whether the current exemptions in 20 (2) are sufficient, and whether there are any unintended consequences arising out of the details of this Article – especially on sectors such as the Credit Referencing Industry that rely on profiling to conduct due diligence, e.g. credit checks for the purposes of responsible lending that it is not clear what a "measure which produces legal effects concerning [a] natural person or significantly affects [a] natural person" might be. For example, the UK considers there is a lack of clarity as to whether profiling carried out to deliver content to an individual, for example, through behavioural advertising falls within the scope of this Article. The title "profiling" is not defined in the instrument and may cause confusion. (DN: do we want to go back to the previous title - Automated individual decisions which was in Article 15 of the 1995 Directive?] "natural subject" should be replaced with "data subject" in order to be consistent with this important definition, which delineates the scope of the instrument. We could query whether "personal preferences" is too wide. On the other hand, the list of performance at work etc. is vaguely drafted using the words "in particular" which means it is not a closed list. Would the list be better in recitals? The main point is that people should not be subject to the "computer says no" culture in important decisions in their lives, without some ability to challenge that automated analysis. But that does not mean that the automated decision is necessarily wrong per se, provided these safeguards are available. Several member states mentioned a Council of Europe paper on profiling. I think we should study that carefully, to ensure that we have not missed any important issues here.

			Arguably whilst the intentions in 20(3) are good, there might be a risk that useful processing was not allowed – for example processing by a computer in relation to health, which might be of benefit to an individual. We need to make sure this is not the case
20(4)			
21 - Restrictions	Recital 59	**We believe that Article 21 should continue to apply to Articles 5, 11 to 20 and 32 (as now).** **We do <u>not</u> support a proposal that this article should not apply to Article 5.** **We would like to place a general scrutiny reserve on the whole of Article 21**	The UK supports the scope for the Union and Member States to restrict the application of certain rights set out in the instrument where such restrictions are necessary and proportionate The UK welcomes the intention of this article, which is to provide exemptions for circumstances where it is necessary to do so. The UK supports the purpose of this Article, which is to restrict the application of certain rights set out in the instrument where such restrictions are necessary and proportionate. As currently drafted, the UK is of the view that it is not possible to foresee every circumstance in legislation where a restriction is necessary and proportionate. We do not believe an absolute detailed and prescriptive list of where restrictions should apply is practical or achievable. Whilst we recognise that the current wording of Article 21 is taken from Article 13 of the 1995 Directive, we are also conscious that significant changes are proposed elsewhere in the new proposal. We, therefore, believe it is important, at the same time, to reassess the restrictions and, having done so, believe that increased flexibility is necessary.

			So we think a better approach would be to create a little more flexibility in the drafting of Article 21(c). We think this can be done by replacing the wording "in particular" with the words "including, but not limited to". Additionally, it seems odd to us that Articles 6-10 are not explicitly covered by the exemption. We would be grateful for the Commission's explanation of this and believe that these articles should also be covered. The need for flexibility underlines that a one size fits all approach which a Regulation by its very nature seeks to achieve may not be the right approach when it comes to data protection. The need for derogations provided for by national law emphasises that a more tightly worded Directive, giving flexibility where appropriate, but also providing a level playing field by tightening up key provisions is the right solution for data protection.
21(1)(a)			Defence/national security and public security appear to have been incorporated into public security in this provision. The UK would like to understand why and ensure that the existing exemptions are still protected.

21 (1)(c)		In 21(1)(c) replace the wording "in particular" with the words "including, but not limited to" **We believe Article 21(c) should be amended as follows (new text underlined):** ***Other public interests of the Union or of a Member State, ~~in particular~~ <u>including, but not limited to</u>, international relations, professional legal privilege or an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters and protection of market stability and integrity. [We would request a specific scrutiny reserve on 21(1)(c)]***	The UK questions whether the provision at Article 21(1)(c) captures due diligence processing by organisations such as credit reference agencies. The exemption as currently drafted does not make clear that the intention is to cover both economic and non-economic public interests. We presume similar amendments will also be needed to Article 9 of Council of Europe Convention 108 to ensure there is no dispute in future over of the draft Regulation) and Member States' obligations under the Convention. The UK questions whether the restrictions set out at Article 21 are too prescriptive and limited and whether Member States should have greater discretion to decide instances where restrictions have legitimate grounds. Under the current Directive the UK has provided for a number of common-sense exemptions, such as parliamentary privilege and legal professional privilege and we would to continue to retain these important derogations. Given the instrument is a Regulation we would be concerned that the provisions in this Article will be read in a very limited way.

CHAPTER IV - CONTROLLER AND PROCESSOR			
22 – Responsibility of the controller	Recital 60	22 - Delete Article 22	The UK questions whether this Article is necessary in that it appears to simply restate the obligations on controllers in other Articles in the Regulation. In particular, Article 5(f) states that personal data shall be "processed under the responsibility and liability of the controller, **who shall ensure and demonstrate** (my emphasis) for each processing operation the compliance with the provisions of this Regulation". Article 22(1) covers the same territory as Article 5(f). This is a good example of one of the main problems with this instrument, as the UK sees it. It focuses too much on procedures rather than outcomes. Provided the outcome is clear, the manner in which the controller achieves that outcome is irrelevant and merely bloats the instrument and makes it excessively burdensome and bureaucratic. The UK believes the prescriptive approach set out in Article 22 is the wrong approach and focuses too much on process rather than outcomes, making the instrument excessively burdensome and bureaucratic.
22(2)(d)			The wording here is imprecise. This looks like a closed list, but the insertion of the words "in particular" suggests that it is not. This leaves controllers in a state of uncertainty as to what measures are actually required. We would like to see this paragraph deleted in its entirety, for the reasons set out above. Further, the fact that sanctions can be imposed both for breaches of Article 22 and each of the Articles listed in 22(2) would appear to create a "double liability" for data controllers in terms of the sanctions which could be imposed.

23 – Data protection by design and default	Recital 61	23 – Recommend deletion of this Article as the requirements do not need to be set out in legislation. Data protection by design and default should be instead best practice ways of achieving compliance with the provisions of Article 5.	The UK supports the principle of data protection by design and default but believes that the design of processes does not need to be included in legislation – data controllers should have the flexibility in deciding how their processes meet the requirements of the regulation The UK believes that the high level principles set out in Article 5 offer a sufficient framework for the protection of personal data. The UK believes the level of prescription risks imposing disproportionate burdens and financial costs on organisations who would likely have to overhaul and redesign existing systems to comply with this provision.
24 – Joint controllers	Recital 62	Delete article 24 - Recommend that this provision is included in the recitals rather than the main body of the regulation. Delete "conditions" in first line.	The UK considers that the provision is sensible in terms of ensuring there are agreements in place between joint controllers, but consider this does not need to be set out in legislation and would be better set out in the recitals It is difficult to see how this will work in practice, in particular in a cloud computing environment. The UK would like to consider the practical implications of this Article in more detail. As per the UK's comments on the definition of "controller", the core definition should be the person who determines the "purposes and means" not the conditions of processing, which is something conventionally done by the processor, The inclusion of "conditions" will create a loophole for those who do not meet all three criteria of purposes, means and conditions. These will also not be processors as very often they will not be processing on behalf of anyone, so will escape regulation entirely.

25 – Representatives of controllers not established in the European Union	Recital 63-64	25 – Recommend reviewing this Article along with the extraterritorial reach of the instrument and the steps that Member States are expected to take to enforce something that is unenforceable.	The UK has concerns about how this provision would be enforceable outside the EU, and the extent to which EU law can apply in 3rd countries. This provision needs to be considered alongside Article 3(2) on scope and Article 78(1) which says that Member States shall take all measures necessary to ensure that this provision in particular is implemented by controllers. We note that the failure to appoint a representative attracts the highest level of mandatory fine under Article 79(6)(f) – up to 2% of AWWTO or 1 million Euros – and yet the provision does not clearly set out the scope of a representative's mission, his/her role or liability.
26 - Processor	Recital 62		The UK believes that the responsibilities of data controllers should be clear and transparent, but question the level of prescription , which is far greater than under Article 17 DPD 95/46/EC Further, it is questionable whether the current draft reflects the realities of the relationship between controllers and processors, in particular in the context of cloud computing.
26(2)(a)		26(4) – Recommend clarification of the interaction between 26(2)(a) and 26(4) as the 2 provisions seem contradictory	The UK would question the wording of Article 26(4) and its interaction with 26(2)(a). Article 26(2)(a) stipulates that processors shall only act on the instructions from the controller, but 26(4) sets out that a processor who processes data beyond the controller's instructions is to be considered a joint controller – the 2 paragraphs appear contradictory and need clarification.
26(2)(b)		Recommend deleting this paragraph	The UK considers this to be overly prescriptive and should surely be left to the contract

26(2)(c)		Recommend deleting this paragraph	This is already covered at Article 30 There is also potentially a "double liability" here in terms of penalties – a processor could end up being liable to a penalty under both Article 79(6)(e) and (g) if they did not comply with "security of processing" (Article 30) and "taking measures pursuant to Article 30" under Article 26(2)(c).
26(2)(d)		Recommend deleting this paragraph	This overlaps with the requirement under 26(2)(a) – if you only act on instructions from the controller then you cannot enlist another processor without telling them.
26(2)(e)		Recommend deleting this paragraph	If the data subject has an obligation to respond to requests for exercising the data subject's rights under Chapter II surely it follows that they cannot escape those obligations by using a processor, so the contract with the processor will already contain this
26(2)(f)		26(2)(f) – Recommend amending this Article to read: **"the processor shall, as far as they are able, assist the controller in ensuring compliance with the obligations pursuant to Articles 30-34"**	The UK believes the role and liability of the processor should be limited to the scope of processing obligations within their direct control

26(4)		See comments at 26(2)(a)	Article 26(4) creates a mechanism by which a processor stepping outside the bounds of authority him/herself becomes a controller. We do not think this is workable – once a processor exceeds controller 1's authority, s/he will be deemed a controller (controller 2) and will then have to comply with the plethora of obligations on controllers in the Regulation, many of which are inappropriate to someone who is in reality a processor, albeit one that has overstepped the limits of his/her authority, Controller 2 may not appreciate the shift in status, and will likely become subject to hefty mandatory fines for failing to carry out all the obligations on controllers such as appointing a DPO. This seems a disproportionate way to deal with the real issue of a processor exceeding his or her authority. It is also a very odd situation as there will be two controllers, controller 1 determining the purposes and means of processing that controller 2 (who may not realise they are now also a controller) is doing on controller 1's behalf (controller 2 having no influence over the purpose or means), albeit in a way that exceeded the bounds of controller 1's authority at some point.
27 – Processing under the authority of the controller and processor	Recital 62	27 - Recommend deleting Article 27 and the moving of its provisions into articles on the responsibilities of controller and processor to avoid the scope for confusion and contradictory provisions.	The UK supports the intention in this Article but question how it works with Article 26(4), which appears to envisage processing without instruction from the data controller

SWITZERLAND

Switzerland thanks the Presidency for this opportunity to put forward comments on chapter III and Articles 22 to 27 of Chapter IV of the proposal for a General Data Protection Regulation. Switzerland welcomes the general idea behind the proposal and in particular the intention to adjust the data protection provisions to the new social and technological realities. At the same time, Switzerland shares many of the concerns voiced by other States during the debates in the DAPIX Working Party. In particular, we would like to highlight the following points which are important for us in Chapter III and IV of the proposal:

1. We would welcome a differentiation between provisions for the public sector and provisions for the private sector. In particular, there should be enough room for specific national solutions with respect to the public sector. This concerns for instance Articles 11, 17, 18, 19 and 21.

2. With respect to several provisions (such as Article 23), we are of the opinion that more emphasis should be put on the risks that arise from data processing for the data subject. The higher such risks, the more requirements should the data controller and processor be bound to respect.

3. In the interest of legal certainty, we would welcome a precision (at least in the recitals) on the following questions:

    - What type of data is referred to in the first sentence of Article 15 para. 2, that is not yet mentioned in Article 15 para. 1 let. g?

    - What actual situations could fall under Article 20?

4. The requirements for any data processing as spelled out in Chapter IV should be measured according to their usefulness for the data subject. Additional administrative burden is in our opinion only justifiable if there is a clear benefit for the data subject. In this respect, a credible estimate of the costs of the various measures is in our view indispensable to assess their proportionality.

NORWAY

1. GENERAL COMMENTS

With reference document 3942/1/12, where the Presidency invites delegations to send proposals for amendments or comments on Chapter III and Articles 20-27 of Chapter IV by 20 September 2012, we will in the following comment on the said articles.

Provided that the provisions on delegated acts and implementing acts will be discussed as a separate issue in DAPIX, our comments on this subject will be presented at a later stage.

We would like to point out that we have a general scrutiny reservation on the regulation, and the comments presented in the following are hence preliminary.

2. ARTICLE 11 TRANSPARENT INFORMATION AD COMMUNICATION

In principle, we support the idea that the controller shall have an easily accessible policy with regard to the processing of personal data and for the exercise of data subject's rights. However, we question whether such a requirement is suitable for small companies, particularly where processing of personal data is not the main activity of the company. We are worried that a requirement of developing such a policy will constitute an unreasonable administrative burden on smaller companies or private persons processing personal data.

3. ARTICLE 12 PROCEDURES AND MECHANISMS FOR EXERCISING THE RIGHTS OF THE DATA SUBJECT

Norway supports the idea that it should be possible to file a request with the controller electronically, where personal data are processed by automated means. We do, however, believe that the controller should be entitled to decide whether the information in question should also be sent to the data subject by electronic means, taking the required security level when transferring information into consideration.

Norway supports the principle that it, at least as the main rule, should be free of charge to access personal data about oneself and information about the processing of such data.

4. ARTICLE 14 INFORMATION TO THE DATA SUBJECT

We believe that it is crucial that the data subject is given information about the processing of personal data about him or her. It is however of great importance that the right to information is not drafted in such a manner that it lays unreasonable administrative burdens on small companies. Consequently, we believe the provision in Article 14 nr. 1 c should be redrafted, since it may be difficult to know at the time of collection how long the data will be stored. We also think that the provision in Article 14 nr. 1 g should be redrafted, so that it only applies under certain circumstances, for example when significant amounts of data or sensitive data are transferred, and not when for instance a hotel reservation is made over the Internet.

5. ARTICLE 15 RIGHT OF ACCESS FOR THE DATA SUBJECT

Norway supports the provision, and we believe it is important that the regulation ensures the data subject's right to access their own personal data and information related to the data. We do, however, find that Article 15 nr. 1 should be given a more flexible wording, in line with the comments made with regard to Article 14 nr. 1 c.

We also think that the data subject should be entitled to request information on relevant security measures related to the processing. This will both enhance the data subject's confidence that the personal data is processed in a fair manner and will increase the controllers' awareness of maintaining relevant security measures.

6. ARTICLE 17 RIGHT TO BE FORGOTTEN AND TO ERASURE

Norway supports the right to have personal data deleted and welcomes the provision in Article 17. We do, however, believe that the provision could be redrafted, in order to simplify the text and make it more applicable in practice.

A possible way to simplify the article would be to separate the rules on deletion and restricted processing into two separate articles. We also believe that Article 17 nr. 7 could be implemented into a different article, for example in Chapter IV. Furthermore, we question if Article 17 nr. 8 is superfluous, since it is not possible to process data which has been erased.

We believe that it should be clarified, in the legal text or in a preamble, how the provision can be applied to social networks and search engines on the Internet. We fully support the intention of a technologically neutral legal instrument, but we still believe that the legislator's intention should be clarified on this point. We also think that it should be clarified how the article will apply in cases where the personal data relates to more than one data subject, for instance a photograph of several people, and not all agree that it should be deleted.

Norway would also like the link between Article 17 and 19 to be clarified. A possible solution is to incorporate article 19 into Article 17, to make it clear that in cases where you have the right to a lawful objection to the processing of personal data, you may also ask for the data to be deleted. Furthermore, it should be clarified in Article 17 that an objection under Article 19 has to meet several criteria in order to be lawful.

7. ARTICLE 18 RIGHT TO DATA PORTABILITY

Norway supports a right to data portability, but we believe that the scope of the provision should be narrowed and that the conditions for, and consequences of, data portability should be clarified in the legal text.

We are worried that data portability is not appropriate when personal data are processed by public authorities. Furthermore the meaning of the phrase "electronic and structured format which is commonly used" is unclear to us. We are worried that the provision will not be suitable for data processed with day-to-day computer programs, such as Microsoft Word and different e-mail accounts. We are therefore wondering if the conditions for applying the provision should be specified, so as to clarify what processing the article is meant to apply to. It is also unclear to us if obtaining a copy under nr. 1 and transmitting the data under nr. 2 implies that the data are deleted by the controller, and this could be clarified in the legal text.

8. ARTICLE 19 RIGHT TO OBJECT

Norway supports the article, but as stated in relation to Article 17, it should be considered whether Article 19 could be incorporated into Article 17.

9. ARTICLE 21 RESTRICTIONS

We would like a clarification as to what public interests will be covered under Article 21 nr. 1 c. We believe the wording could be more flexible, to make it clear that also other public interests than economic or financial interests may provide a ground for derogation from the regulation. We also think that the provision in Directive 95/46 Article 13 nr. 2 regarding restrictions from the data subject's right to access in cases where data is processed for statistical and research purposes should be maintained. Alternatively, it should be clarified if this restriction is now meant to be covered by the scope of Article 21 nr. 1 c.

10. ARTICLE 27 PROCESSING UNDER THE AUTHORITY OF THE CONTROLLER AND PROCESSOR

Norway supports the article, but we believe that nr. 3 should be deleted in order to avoid an increase of administrative burden, since the instructions and obligations will already be written in the contract.

Furthermore, nr. 4 should be deleted in order to make it clear that the data processor cannot act outside of the instructions given by the controller. If a data processor acts outside the instructions given, we believe that it is sufficiently clear from the regulation as a whole that he can be held responsible for the processing.