EUROPEAN COMMISSION
Information Society and Media Directorate-General

The Director General

Brussels, 22/12/2011
INFSO B1/RB Ares(2011) 1488963

ANNEX TO REPLY FROM

INFORMATION SOCIETY AND MEDIA DIRECTORATE GENERAL (INFSO) ON CIS-NET

***Interservice consultation launched by*:** DG JUST

***Reference*:** DG JUST.C3 (2011) 1350739 bis

Deadline for reply: 20/12/2011

***Titles*:**

- Proposal (draft) 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 (**DP Regulation**).

- Proposal (draft) for a Directive 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 (**Police and Criminal Justice Data Protection Directive** or **Directive**).

The draft versions of the above mentioned legal acts are accompanied among others by the following documents:

- Impact assessment on the reform of personal data protection in the EU (**Impact Assessment**).

- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions "*Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century*" (referred to as the "**Chapeau communication**").

Contact person in INFSO DG: R. Barcelo, INFSO B.1 *(Tel. 88182)*

☐ **Agreement**

☐ **Favourable opinion subject to comments being taken into account**

☒ **Unfavourable opinion**

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111
Office: BU 7/23 - Tel. direct line +32 229-56165 - Fax +32 229-68391

Rosa.barcelo@ec.europa.eu

Thank you for consulting INFSO on the Data Protection Reform Package. INFSO recognises that the draft DP Regulation is very complex legislation and appreciates the helpful exchanges before and during the ISC. INFSO agrees with the potential of privacy and data protection to contribute to the aim of "building digital confidence" under a "vibrant digital single market" as mentioned in the Chapeau Communication. In this regard, the legal instrument of the draft DP Regulation is welcome.

INFSO also appreciates a number of proposals reducing the administrative burden on business, in particular on cloud computing, and thereby on growth and innovation. Such measures include the cutting of red tape for international data transfers (Articles 37-40) and, as a principle, the competence of a single Data Protection Authority.

INFSO further welcomes that, in the bilateral exchanges during ISC, JUST has accommodated some of INFSO's fundamental concerns such as the definition of consent, as well as other practically important issues, for instance the definition of "main establishment" or the facilitation of the enlistment of sub-processors (Article 23 (2)) and health issues.

1. Issues of outstanding disagreement

INFSO believes that JUST recognises the need to address a number of issues of concern. However, INFSO regrets that JUST has not proposed significant changes on several crucial issues where INFSO insists on avoiding unnecessary obstacles to ICT and new business, including the development of the Internet.

These issues are, first, the definition of personal data which is too broad. The wording proposed by JUST considers location data and online identifiers per se as personal data, thereby imposing automatically considerable obligations on service providers.

Second, INFSO considers that the provisions of Articles 28 and 29 on data breach notifications are not practicable: on the one hand, they impose a compulsory 24-hour notification period sanctioned by a minimum fine of EUR 100.000 which appears disproportionate. On the other hand, these provisions introduce the concept of "establishment of a breach by the controller" as triggering event, thereby creating legal uncertainty. INFSO is further highly concerned that the proposed Articles 28 and 29 would result in an unlevel playing field for communications providers who are bound by the ePrivacy Directive, and other companies. So far, while JUST has shown openness to some limiting language as regards the timing of notification to data subjects, it has not positively responded to INFSO's request to adapt the draft DP Regulation to the wording of Article 4 of the ePrivacy Directive which applies clear ("as soon as becomes aware") and well-known ("without undue delay") legal terms.

Third, INFSO considers that the draft DP Regulation is not the appropriate place for a definition of "child". INFSO therefore strongly suggests removing it. However, if this is unavoidable for some specific provision, for example parental consent to open an account on a social network, then the weight of evidence available today suggests that the threshold is 12-13 years and not 18.

Fourth, JUST has not shown much openness regarding INFSO's objective to ensure that the draft DP Regulation facilitates a dialogue on the evolving notion of data protection

and social behaviour so that this will ultimately permeate into future policies. INFSO considers this essential, particularly as the draft DP Regulation will ultimately contain potentially burdensome requirements. Therefore, the existence of a review mechanism such as the one suggested by INFSO (point VI) would help bring future policy regulations on the right track. Such mechanisms would also be highly valuable for the development of policy under the regulation itself, for example via the EDPB. Indeed, INFSO's purpose in inserting such a feed back loop is to make the application of the DP Regulation actually future proof which is a key characteristic of legislation in the 21st Century.

2. Issues of disagreement where JUST has moved insufficiently

With respect to some of INFSO's concerns JUST has shown a certain degree of flexibility which is appreciated. However, JUST's new proposals do not sufficiently accommodate INFSO's concerns. This relates mainly to the right to be forgotten (Article 15) where the obligations imposed on data controllers would still be too burdensome. Another area necessitating further improvements relates to processor requirements.

In addition, regarding data transfers, JUST's reaction in the course of the ISC to INFSO's comments on limiting language relative to massive, frequent or structural transfers would actually generalise the limiting language in question, and thus probably increase overall burdens (Article 41).

3. Key principles and other issues

Finally, INFSO emphasises the importance of some key principles. First, it should be made sure that the draft DP Regulation does not interfere in areas that are currently covered by the ePrivacy Directive. In particular, it is important that the draft DP Regulation does not contradict, the ePrivacy Directive's security breach and direct marketing provisions nor create needless confusion regarding their application (see point IV.2). Furthermore, irrespective of any future amendments to the ePrivacy Directive that may be proposed in the near future, it is important for the draft DP Regulation to delimit clearly the relationship of the draft DP Regulation vis-à-vis the ePrivacy Directive (point V).

Second, INFSO is concerned about the compulsory imposition of fines (without any discretion) and the maximum level of these fines.

Third, some key concepts need to be further clarified (e.g. point VII.1).

On balance, INFSO considers that, in spite of some improvements during the ISC, the draft DP Regulation still sets forth an overly cumbersome legal framework which places new burdens and costs upon data controllers and processors, thereby acting as a deterrent for the development of new business models. INFSO is concerned that the proposal does not sufficiently take account of the economic climate and is at odds with the vision of Europe 2020.

In particular, INFSO considers that the draft DP Regulation does not deliver a sufficiently balanced framework accommodating the interests of data subjects while at the same time enabling ICT companies to operate and explore new business models at a

reasonable cost. A number of provisions in the draft DP Regulation will place a heavy and at times unreasonable burden upon data controllers and processors, without bringing corresponding advantages in terms of protection of the interests of data subjects. Some of them are likely to hinder the deployment of on-line services and products. For example, the cumulative effect of new requirements imposed upon data controllers and particularly upon processors, such as providing for a broad range of processing operations subject to private impact assessment and corresponding prior authorization as well as requiring to maintain appropriate documentation and to demonstrate compliance, may deter the development and use of cloud computing services, particularly by SMEs. The right to be forgotten requiring controllers to erase all Internet links to and copies or replications of data is another eloquent example of excessive burden.

In sum, INFSO is of the view that taken as a whole the draft DP Regulation would have significant negative effects on the development of the digital economy and jeopardise the Commission's Digital Agenda. Furthermore, INFSO believes that the very nature of data and personal data is in the midst of a fundamental transformation, and is conscious that no legislative initiative can adequately capture this process. The risks of empty regulation and of unintended negative consequences are both correspondingly high.

However, as indicated, INFSO looks forward to further inter-service contact after the ISC consistent with the fact that the review was launched last year by Vice-President Reding in agreement with Vice-President Kroes.

For your convienence we are providing a version of the draft DP Regulation in track changes. The points made are also reflected in the track changes version of the Chapeau Communication.[1]

Regarding the Directive, INFSO suggests that for reasons of consistency, the text of the provisions should be aligned as much as possible with that of the draft DP Regulation whenever the two texts includes similar provisions.

I. Definitions

I.1. Personal data and data subject

Articles 3 Nr.1 and 3 Nr.2 of the draft DP Regulation incorporate respectively the definions of "*data subject"* and that of "*personal data*". Under Directive 95/46 these concepts were covered by a single definition. The draft DP Regulation deems personal data as any information relating to a data subject. Article 3 Nr.1 defines a data subject as "*an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier*..." (the underlined parts reflect what the draft DP Regulation has added).

However, INFSO is concerned that under the draft DP Regulation factors such as location data and "online identifiers" are deemed "*per se*" as relating to a data subject and

[1] Regarding the Impact Assessment, INFSO notes that the actual budget of ENISA for 2011 is 8.1 million euros which should be corrected in the IA.

thus qualify automatically as personal data. Yet, in some cases online identifiers may not identify an individual and in such cases they should not be considered personal data. In order to address this concern, INFSO proposes amending Article 3 Nr.1 and adding a new recital, as follows:

Article 3 Nr.1: *'data subject' means an identified natural person or a natural person who can be identified directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.*

Recital 23 new: "When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. Therefore, the question whether, in a given context, location data, online identifiers, identification numbers or other specific factors on their own are deemed to be personal data should depend on whether they are reasonably likely to be used to identify a natural person by the controller or another natural or legal person who may obtain this information from the controller in case the latter did not treat it as personal data."

In addition, we understand that JUST and INFSO share the view that, in cases where a data controller has not identified a data subject on the basis of data at his disposal, he should not be required to gather additional information simply in order to permit the data subject to exercise certain rights foreseen in the draft regulation (e.g. to receive a copy of data held on that person, to review its accuracy, to seek its deletion, etc.). This provision would be particularly helpful for data controllers which process on-line identifiers (such as IP addresses) but ignore the identity of the natural person related to the identifier. To reflect this, we propose adding the following provision (e.g. as a new Article 4(3)):

"*A data controller shall not be obliged to acquire additional information in order to identify a data subject for the sole purpose of complying with any provision of this Regulation*."

I.2. Definition of consent

Article 3 Nr.8 defines consent at a higher threshold than the current Directive 95/46, namely as a *"freely given specific, informed and explicit indication"* of the individual's wishes. Explicit consent could be construed as requesting a "yes" response to having one's personal data processed (for instance, signing at the bottom of a paper under a paragraph saying "*yes, I accept my data to be processed for such purposes*"). It is very doubtful whether explicit consent would encompass also consent implied from individuals' actions or behaviour, for example downloading an application or playing a game. However, INFSO notes that, in terms of current behavioural psychology, consent can in fact be inferred or implied from such actions - which are crucial for new technologies. Yet, even if such action or behaviour is clear, it may not meet the threshold of "explicit" consent insofar as consent which is implied from behaviour is by definition "implicit" (not "explicit").

To avoid jeopardising the development of ICT and new business models which frequently rely on innovative ways of providing consent, DG INFSO suggest changing

the definition of consent as follows (the underlined part reflects INFSO's suggested changes):

'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, by a statement or a clear action, signifies agreement to personal data relating to them being processed. We understand that JUST agrees with this proposal.

INFSO further suggests amending Recital 24 to clarify that the data subject's statement or action should be interpreted in their context. A sentence should be added: "any interpretation as to whether consent is given should take due account of the context of the data subject's statement or action".

INFSO understands that JUST agrees with this proposal.

I.3. Main establishment

Under Article 3 Nr.13 of the draft DP Regulation the "main establishment" is defined as the central administration as far as data processors and controllers are concerned. However, Article 3 Nr.13 contains a second criterion to determine "main establishment" as far as controllers are concerned (i.e., the place where the purposes, conditions and means of the processing are determined). This is very confusing. INFSO fails to understand the logic of setting forth two different criteria for controllers.

This key concept which has an impact on the competent DPAs, should be clear in the text to dispel any doubt about jurisdiction. INFSO therefore proposed the following wording of Article 3 Nr.13:

'Main establishment' means where the controller's or the processor's central administration in the Union is located. For the purposes of this Regulation the central administration of a controller is deemed to be located where the purposes, conditions and means of the processing of personal data are determined.

In turn, JUST proposed the following wording: 'Main establishment' means, as regards the processor where the central administration in the Union is located. As regards the controller, the main establishment is deemed to be located where the purposes, conditions and means of the processing of personal data are determined.

INFSO can agree with this language.

II. Lawfulness of the processing

II.1 Consent for direct marketing

Article 5(2) and the corresponding recital 50 of the draft DP Regulation require consent to *process* personal data "*for direct marketing for commercial purposes"*. Since processing is defined as covering all kinds of data operations, including collection and use, consent would be required both for the initial collection of data and also for the sending of direct marketing. It applies both to traditional paper based direct marketing and to marketing delivered by electronic means (cf. Recital 23). This constitutes a radical change as compared to the current legal framework. Direct marketing (by non-electronic

means) for commercial purposes is traditionally based on Article 7(f) of Directive 95/46/EC, which provides for the legitimate interests of the data controller as a legal ground. Article 14(b) of Directive 95/46/EC enables the data subject to object *"to the processing of personal data relating to him which the controller anticipates being processed for the purpose of direct marketing ..."*. These rules apply to mail marketing while the ePrivacy Directive applies to the **collection** of information for on-line behavioural advertising (Article5(3)) and to the **sending** of direct marketing communications by any electronic means (Article 13).

INFSO considers that the blunt statement in Article 5(2) of the draft DP Regulation pursuant to which "processing of personal data for commercial purposes shall be lawful only if the data subject has given consent…" should be more differentiated.

Regarding the sending aspect, INFSO is concerned that Article 5(2) of the draft DP Regulation may jeopardise legitimate business practices such as the contacting of existing customers. To address this problem, INFSO suggests that this article is further developed to provide more clarity. In particular, INFSO suggests that this article explicitly refers to the sending of commercial communications and integrates, in any event, the exception foreseen in Article 13(2) of the ePrivacy Directive. Pursuant to this exception, data controllers may engage in direct marketing to existing customers to advertise similar products and services provided that customers are given the opportunity to object to such use of their contact details.

Regarding the collection aspect, INFSO questions whether the consent requirement is justified as a general rule. It is true that Article 5(3) of the ePrivacy Directive requires consent, subject to some significant exemptions. Such a consent requirement appears appropriate because the collection of information stored on a user's equipment may give a deep insight into his or her privacy. By contrast, the collection of data for the purpose of direct marketing is generally much less invasive and frequently confined to address data. It is therefore highly questionable whether requiring consent for the collection, and also for other processing steps such as organisation or adaptation, is really appropriate.
Furthermore, INFSO questions whether the explicit consent requirement would be practical in the on-line environment. For example, the serving of on-line ads personalised on the basis of IP addresses previously collected – rather than cookies - would require prior explicit consent under the proposed draft Article 5 (2). INFSO doubts whether in practice this would be feasible without impacting negatively upon Internet users' experience.

In addition to the substantive points outlined above, from a legal point of view, INFSO has concerns about the interplay of this requirement with Articles 5(3) and 13 of the ePrivacy Directive, which apply respectively to the gaining or accessing of information (i.e. to the collection of information) for on-line behavioural advertising and to the sending of direct marketing communications. For example, it is uncertain whether the current exception to consent for direct marketing to existing clients ex Article 13(2) of the ePrivacy Directive would continue to apply. The draft Article 5(2) also puts into question the "acquis" for direct marketing, including the codes of conduct of the private sector (FEDMA) which have been approved by the Article 29 Working Party.

In sum, INFSO is not convinced of the reasonableness of this new rule and is concerned about creating risks of confusion as to the applicable rules on processing (the ePrivacy Directive or the draft Data DP Regulation).

INFSO does therefore not agree with Article 5(2) in its current form and the relevant recitals and urges JUST to amend it as described above, or to delete it.

II.2 Consent "in imbalanced situations"

Article 7(4) establishes that "*Consent shall not provide a legal basis for the processing, where there is a significant imbalance in the form of dependence between the position of the data subject and the controller"*. This is explained in Recital 30. DG INFSO agrees that in many situations of imbalance (such as in an employer/employee relation), individuals' consent will not be freely given (individuals may feel coerced to accept). However, there may be occasions where - despite the imbalance - individuals freely give their consent. This may be the case when a refusal to accept does not trigger any negative consequence (e.g., acceptance/refusal to have a picture loaded in the intranet). Therefore, it seems inappropriate for the draft DP Regulation to completely exclude the use of consent in these situations. Thus, the problem is adequately addressed on a case-by-case basis through the words "freely given" in the definition of consent and there should be no outright prohibition.

DG INFSO suggests deleting Article 7(4) and introducing a Recital clarifying that the existence of imbalanced situations should be taken into account in determining whether consent is "freely given, explicit and informed". This should be sufficient, in particular given the burden on the party relying on consent to demonstrate compliance with these requirements.

JUST has proposed alternative language, merging Article 7 (4) and (5) as follows:

"4. Consent shall not provide a legal basis for the processing, where <u>in the specific case</u> there is a significant imbalance in the form of dependence between the position of the data subject and the controller, <u>in particular for the processing</u>
<u>(a) by public authorities in the performance of their tasks; or</u>
<u>(b) for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law.</u>"

<u>INFSO considers that this language does not address the problem outlined above. This is because the new proposal still excludes as a general rule the possibility to rely on consent as legal basis for the processing of data when there is an imbalance situation. For the reasons set out above, INFSO considers that this proposal is not satisfactory.</u>

<u>III. Rights of the data subject</u>

III.1 Modalities

The Digital Agenda for Europe aims to maximise the social and economic potential of ICT, most notably the internet. Against this background, DG INFSO suggests adding some elements to maximise the use of electronic means to exercise individuals' rights. More particularly, in Article 10 (2), last sentence, the wording should be adapted from

"may" into "shall" as follows:

"Where the data subject makes the request in electronic form, the information ~~may~~ shall be provided in electronic form unless otherwise requested by the data subject."

In Article 13(2) which refers to the individuals' right to access their data and the corresponding recitals 44 and 104 concerning health data, we suggest adding:

"Where personal data are processed by automated means, the controller shall provide the information in electronic form unless otherwise requested by the data subject."

INFSO understands that JUST agrees with the above proposal.

III.2 Right to be forgotten

INFSO has identified multiple layers of problems regarding the right to be forgotten:

First, as a general comment, DG INFSO seriously doubts that the right to be forgotten as presented in the draft DP Regulation will meet expectations created or be workable in practice. INFSO is further concerned about the proportionality of the sanctions (up to 600,000 EUR) under Article 79(3)(c) in case of failure to grant this right or to "*erase any public Internet link to, copy of, or replication of the personal data relating to the data subject contained in a publicly available communications service*". INFSO also notes a misalignment of language between Article 15 in its current version and Article 79(3)(c) on sanctions.

Second, INFSO does not understand the reference to the application of the right to be forgotten "*in relation to personal data which are made available by the data subject while he or she was a child*". In particular, if the right applies to everyone, the proposed wording results in a lack of clarity. In other words, does this right differ if it is applied to information posted by an adult as opposed to information posted by a child and do the data controller's obligations differ? Unless JUST can formulate clearly the set of different responsibilities that may apply in these two hypothesis (information posted as a child versus information posted as an adult), INFSO suggests deleting the reference altogether. On the other hand, INFSO would not object to mentioning in the relevant recital that the enduring effects on individuals of information released at a young age is a significant motivating factor for this provision of general application.

Third, DG INFSO is particularly concerned about Article 15(2), which requires data controllers, beyond the removal from the original source, to erase Internet links to and copies or replications of data. This is further explained in Recital 47 pursuant to which "the right to erasure should also be extended in such a way that any publicly available copies or replications in websites and search engines should also be deleted by the controller who has made the information public". This means that, for example, if an employee withdrew his consent to have his picture uploaded on the company's Internet site, the employer would be required to go around the Internet, websites and other online services (e.g. P2P networks, search engines) and delete (on which legal grounds?) "links, copies and replications" of the picture. The draft DP Regulation foresees heavy sanctions in case the data controller fails to do so (up to 600,000 EUR).

The above example illustrates that it would be very difficult, and virtually impossible, for a data controller to comply with this obligation, and even more so for private individuals uploading information on the Internet. Many controllers will simply lack the technical capability to do this search and to follow the data. This is particularly true for SMEs and individuals. Good legislation should not impose obligations which cannot be complied with ("impossibilium nulla est obligatio"). INFSO therefore suggests to remove Article 15 (2) altogether, including the relevant parts of Recital 47.

As a second-best option, INFSO suggests turning this obligation into a "reasonable efforts" obligation. The controller could be expected to bear the burden to proof that he has taken all the reasonable steps and appropriate technical measures to ensure the execution of this right. Article 15(2) could thus read as follows:

"Where the controller referred to in paragraph 1 has made the data public, it shall take all reasonable steps, to the extent consistent with paragraph 1, including technical measures, 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 data".

INFSO understands that JUST would agree with similar wording, although with some changes (basically, rather than an obligation to "take all reasonable steps" JUST suggests an obligation to "take all necessary steps […] in relation to data for the publication of which the controller is responsible". In addition, JUST proposes adding an additional Article 15(2 bis) which would read as follows: "In relation to the subparagraph above a controller shall be considered responsible for the publication by a third party publication of data where it has authorised the third party to publish it."

Regarding the standard "take all reasonable steps"" *versus* " take all necessary steps", INFSO has a strong preference for the wording that it proposed (i.e., make reasonable efforts"). Legally "reasonable efforts" is a standard type of legal or contractual obligation with well defined meaning. Notably, it requires applying the efforts that are reasonable in the circumstances all things considered. By contrast, "take all necessary steps" is less precise legally speaking and, *a priori*, it appears to require extra efforts compared to what would be required under "reasonable efforts". Therefore, INFSO confirms its wish to use the language it proposed and suggests adding guiding language, through a recital, on what would constitute reasonable efforts, by reference to the current state and cost of technology, the sensitivity of the data, and perhaps other parameters. This could be done as follows:

"To strengthen the 'right to be forgotten' in the online environment, the controller should undertake all reasonable efforts to inform third parties that the subject has requested the information to be deleted. In determining what constitute reasonable efforts, account should be taken of all relevant factors, including the nature of the information in the individual case, the sensitivity of the data, whether the information is otherwise publicly available, the status and the conduct of the controller, and the availability and cost of technology".

In addition to the above, INFSO fails to understand the *rationale* of the suggested new Article 15(2 bis) and questions its workability. In particular, it is unclear how the term "authorised" is to be construed, e.g. would the same requirements as for consent apply? Unless JUST can provide a convincing rationale for its approach on the "responsibility

concept", INFSO suggests to remove Article 15 (2 bis) and the corresponding references in the new Article 15 (2) proposed by JUST.

As a separate matter, DG INFSO is of the view that mere intermediaries such as conduits, storage providers and search engines etc, when they are not controllers themselves, should not be covered by the obligation. If they were to be covered this would have substantial negative effects on freedom of expression, access to information etc. To provide legal certainty about the role and obligations of intermediaries INFSO suggests to insert the following paragraph 8 in Article 15: "*Service providers, other than controllers, acting only as conduits or merely providing automatic, intermediate and temporary storage or storage of information provided by a recipient of the service or allowing or facilitating the search of or access to personal data, shall not be responsible for personal data transmitted or otherwise processed or made available by or through them*".

IV. Controller and processor

IV.1. Requirements applicable to data processors

a) Chapter IV deals with controllers and processors. The current distinction between controller and processors becomes more blurred in the draft DP Regulation. INFSO is concerned as to whether this may create risks of confusion as to which entity is ultimately responsible. Some of the proposed provisions are likely to have a prohibitive effect on cloud computing as cloud providers are normally processors. To this end, INFSO suggests amending the following two articles (the words/paragraphs underlined reflects what INFSO proposes to add):

Article 23 (e): "~~insofar as this is possible~~ given the nature of the processing, ~~create~~ define in agreement with the controller the ~~necessary~~ appropriate and relevant technical and organisational measures ~~requirements for the~~ that support the ~~fulfilment of~~ ability of the controller's ~~obligation~~ to respond to requests for exercising the data subject's rights laid down in Chapter III";

Article 25: "Each controller ~~and processor~~ and, if any, the controller's representative, shall maintain appropriate documentation of the all processing operations under its responsibility and to share such documentation with the processor. The processor shall contribute to the establishment of such documentation insofar as the processor disposes of relevant information."

Articles 30 and 31 should apply to controllers only. Therefore, we suggest deleting the reference to processors.

Article 30(1) on ***Data protection impact assessment***: Prior to the processing of personal data, the controller ~~or the processor~~ shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data where those processing operations are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes.

Article 31(1) on Prior authorisation and prior consultation: The controller ~~or the processor~~ shall, where required, obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with the Regulation and in particular to mitigate the risks involved for the data subjects where:

b) For a processor to enlist another processor, Article 23(d) requires the first processor to have the permission of the controller and inform him of the intention to enlist another processor in such a timely fashion that the controller has the possibility to object.

Companies increasingly outsource the management of information and management systems, record keeping etc, to cloud computing service providers. The attraction of cloud computing in particular to companies with limited financial means such as start-ups lies in the fact that it can effectively replace the need for considerable up-front capital investment in expensive IT infrastructure with continuing operating expenses. Cloud computing services are often delivered by many providers, which may change over time. It would seem unfeasible in these circumstances for the processor to go back to each one of the controllers to ask them whether they want to object to a sub-processor.

DG INFSO fully agrees that data processors need to be authorised by data controllers to sub-contract and that sub-contractors should respect the contractual obligations to which the initial processors are bound. However, the requirement to obtain prior authorisation each time that a processor enlists a new sub-processor seems impractical and not in line with the practices in the business environment.

To this end, we have deleted part of Article 23(d) which now reads as follows: the processor shall (d) "*enlist another processor only with the prior permission of the controller".*

We understand that JUST agrees with this suggestion.

IV.2 Notification of personal data breaches

Articles 28 and 29 of the draft DP Regulation deal with notification of personal data breaches to supervisory authorities and to individuals respectively. The period for notification is "as a rule, not later than 24 hours" after the breach "has been established by the controller". The choice of 24 hours is to the best of our knowledge not based on any empirical evidence. The meaning of "established" is not explicitly defined. According to Recital 58, notifications are due "*as soon as the controller becomes aware that such a breach has occurred*". Thus, it appears that "establishing a breach" means simply becoming aware that a breach has occurred rather than becoming aware of the facts and circumstances concerning the breach, including the types of data that have been compromised, the number of individuals' affected, the effects of the breach, etc. The two concepts set out in Articles 28 and 29 and in Recital 58, respectively, are entirely different.

INFSO considers that a rule pursuant to which the notification is due 24 hours after the data controller becomes aware of a breach may in many cases (e.g. when the number of people affected by the breach is difficult to determine) be too short and impossible to comply with. Even if notifications were only due after the circumstances regarding the breach have been duly ascertained, the risk of a 24 hours deadline would be that controllers would take more time to establish the data breach, thereby delaying the start of the 24-hour period.

INFSO emphasises that Article 4(3) of the ePrivacy Directive, amended in 2009, sets forth a personal data security breach framework pursuant to which notifications are due "without undue delay", after the provider has become aware of the breach (Recital 61 Citizens Rights Directive). Thus, the ePrivacy differs from the draft DP Regulation both in the specific timing ("without undue delay" versus "as a rule, not later than 24 hours" and also in terms of the starting point of that period "becoming aware" versus "established"").

INFSO considers that the concept of the ePrivacy Directive is clearer, more practicable, more open to future evolutions, and provides for more legal certainty than that of the draft DP Regulation. The triggering event, i.e. the moment of "becoming aware", can normally be clearly identified and the reasonable period for notification can be assessed in a given case by reference to the necessary steps to ascertain the nature and scope of the breach; whereas the reference to the moment when the data breach has been established by the controller leaves a large discretion to the controller to delay the start of the notification period. Regarding the notification period, the concept of "without undue delay" is established in European and national law and a lot of interpretation guidance by courts. By contrast, the 24-hour period is clear-cut only at first sight as it is subject to ambiguity by the reference to "as a rule".

In the light of the problems outlined above regarding the use of "established" and in view of the advantages of the concept integrated in the ePrivacy Directive, INFSO strongly advises that the draft DP Regulation follows the ePrivacy Directive.

An additional argument for an alignment of the draft DP Regulation to the ePrivacy Directive is that the proposed deviation would create an unlevel playing field for providers of electronic communication services, which are subject to the ePrivacy Directive, and other controllers. There is no justification for such discrimination.

The above would require making the following changes in the draft DP Regulation: Article 28 "*In the case of a personal data breach, the controller shall without undue delay ~~and, as a rule, not later than 24 hours~~ after having become aware of it~~,~~ notify the personal data breach to the supervisory authority*". The same change is proposed in Article 29 regarding notifications to individuals.

In interpreting the notion of undue delay, both in the context of notification to individuals and to authorities, the guiding principles should include the following: (i) The notification should be given in such time as to enable the individual to mitigate the adverse effects of the breach. If all relevant facts surrounding the breach are immediately apparent, there is no reason for any delay and notification should be given immediately. (ii) Notwithstanding the above, before serving the notice to individuals, in some cases, particularly in criminal investigations, data controllers may have to take into account instructions of law enforcement agencies. Such agencies may require delaying the notification if they perceive that notifying could affect or prevent the criminal investigation. (iii) In some cases, it may also be necessary to delay notification to individuals, although not to authorities, until the security of the system has been restored. Any delay should not exceed the minimum required to patch the security problem by the swiftest means available.

IV.3. Data Protection impact assessment

Article 30 of the draft DP Regulation requires data controllers to carry out a privacy impact assessment. INFSO has proposed language with the purpose to make the proposal more stringent and better suited to identifying the real risks. INFSO has also connected it to the requirements on privacy by design and privacy by default. In particular, this is done in Article 30 (3) which would read as follows: "*The assessment shall contain at least a general description of the envisaged processing operations, an identification and assessment of the risks to the rights and freedoms of data subjects, a control implementation plan, from which residual risks are derived, the measures envisaged to address the risks, safeguards,* including solutions for privacy by design and privacy by default*, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.*" (the words underlined reflect what INFSO proposes to add).

Whilst INFSO supports the obligation upon controllers to carry out a data protection impact assessments, it is nevertheless concerned about the large number of processing operations to which such obligation applies, in particular in the light of the economic costs associated to such assessments. It should be taken into account that DPIA entail non-negligible costs. For example, according to the Impact Assessment a small scale assessment would cost 14.000 Euro, a medium scale 34.000 Euro and a large scale 149.000 Euro.

Under the draft DP Regulation, impact assessments are required when the processing presents specific risks. In addition to processing of sensitive data such as health, sex, race, using video surveillance, large scale filing systems etc, they are also required when the processing evaluates aspects relating to a natural person or for analysing or predicting in particular the natural person's performance at work, creditworthiness, economic situation, health, reliability or behaviour, which is based on automated processing and likely to result in measures that produce legal effects concerning the individual or significantly affect the individual, etc. In sum, it is difficult to imagine a situation where data protection impact assessments are not required. This is more worrisome if one takes into account that prior consultation with the national data protection authority is required when the privacy impact assessment indicates that the processing is likely to present a high degree of specific risks (which is likely to be often the case insofar as the types of processing operations subject to impact assessments are precisely those which present specific risks).

Against this background, we suggest redrafting Article 30.2 (a) to limit the situations where DPIAs would be required. In particular, we suggest to limit the requirement for DPIAs to the evaluation of personal aspects of a natural person as such for the purposes of predict performance at work, creditworthiness, economic situation. As currently formulated, the provision is too broad and it would include situations where in principle a DPIAs does not appear necessary. In fact, it is difficult to imagine a situation not covered by it. We have excluded the reference to location data for the same reason. .

"*In particular the following processing operations are likely to present such specific risks as referred to in paragraph 1: an evaluation of personal aspects* ~~*relating to a natural person or for*~~ *to analys*~~*ing*~~ *or predict*~~*ing*~~ *in particular the natural person's performance at work, creditworthiness, economic situation,* ~~*location*~~*, health,* ~~*personal preferences,*~~ *reliability or behaviour, which is based on automated processing and likely*

to result in measures that produce legal effects concerning the individual or significantly affect the individual; or"

IV.4 Data Protection Officer

Article 32 of the draft DP review requires the designation of a data protection officer (DPOs) by enterprises employing more than 250 employees. INFSO agrees with the proposal to appoint DPOs, however, INFSO is concerned about the costs that this requirement would entail for companies, particularly medium ones. While a minority of Member States legal framework already foresees the obligation to appoint a DPO in certain cases, such as Germany, and others foresee on a voluntary basis (such as France or the Netherlands), for the majority of Member States this requirement would be entirely new. It would therefore represent an entirely new source of expenditure. In this regard, INFSO suggests that it is only imposed upon organisations that employ more than 500. The proposed threshold of 250 employees seems too low as it would entail heavy expenses that are difficult to justify. As an exception to the rule, INFSO supports JUSTs proposal in Article 32(1)(c) which makes it mandatory in situations of fewer employees but when the processing is highly sensitive .

In addition to the above, INFSO suggests making sure that only one DPO will be necessary for all European subsidiaries of one entity, i.e. one DPO should not required for each Member State. To this end, we suggest amending *Article 32*

"1. The controller or the processor shall designate ~~a~~ **one** data protection officer in any case where" and amending Recital (62) as follows:

Where the processing is carried out in the public sector or where, in the private sector, processing is carried out by an enterprise larger than a small or medium-sized enterprise, or where its core activities, regardless of the size of the enterprise, involve processing operations which require regular and systematic monitoring, a person should assist the controller or processor to monitor internal compliance with this Regulation. As the internal structure of a company or group of undertakings should not influence the obligations under this Regulation, a group of undertakings may appoint a single data protection officer. Such data protection officers, whether or not an employee of the controller, should be in a position to perform their duties and tasks independently (the words/paragraphs underlined reflects what INFSO proposes to add).

IV.5. International Data Transfers

Articles 37 to 44 of the draft DP Regulation deal with international data transfers. Transfers to third countries which are not deemed "adequate", can be made under Article 39 if the exporter puts in place "*adequate safeguards*" (for instance, by entering into model clauses or establishing binding corporate rules).

In particular, the draft DP Regulation lists in as adequate safeguards, standard data protection clauses adopted by the Commission (Article 39(2)(b)) and standard data protection clauses adopted by the authorities using the consistency mechanism (Article 39(2)(c)). In such cases prior authorisation from the supervisory authorities is not necessary. In addition, Article 40 lays down that such adequate safeguards can also be

provided by Binding Corporate Rules ("BCRs"). BCRs have to be authorised by supervisory authorities.

If the exporter uses other types of clauses - ad hoc clauses - specific prior authorisation from the authorities is necessary. In addition, data transfers can be carried out if one of the derogations such as consent applies. A new derogation has been added under Article 41(h) allowing data transfers if the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor.

DG INFSO welcomes the provisions streamlining the rules on the adoption of BCRs and the broadening of their scope. DG INFSO also welcomes the addition of the new derogation, although it believes that, as currently drafted, the scope would be unduly restricted. In particular, according to Article 41(h) and the corresponding recital 72, the derogation does not apply to structural, massive or frequent transfers. INFSO note that as a matter of law, exemptions from a general principle should be interpreted restrictively. If in addition to this general principle, the draft DP Regulation adds additional ill-defined restrictions excluding transfers that are massive, structural or frequent, the scope of application of the derogation becomes close to nil. Furthermore, it is a general principle of law that the exceptions are to be interpreted in a restrictive way.

Furthermore, the requirement to inform the authorities of such transfers also constitutes an unnecessary burden. It is not explained why transfers carried out on the basis of other derogations would not trigger similar information requirements. DG INFSO has suggested a number of changes in Article 41(h) to make this derogation more workable in practice.

It would read as follows: "*The transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor,* ~~cannot be qualified as frequent, massive or structural,~~ *and the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary".*

Article 41 (6) should be amended as follows: " The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in paragraph 1 (h) in the documentation referred to in Article 25 ~~and shall inform the supervisory authority of the transfer~~ *"*

In addition, INFSO proposed that a recital be added to clarify how to make a determination about whether the controller has such legitimate interests as follows: "*In making that determination the controller should take all individual circumstances of the particular case into account, such as the nature of the personal data, the country to which the data is transferred, whether the country has acceded to Council of Europe 108 Convention and relevant protocols thereto, contracts between the controller and the transferee and the existence of appropriate technological protection measures including privacy by design and by default as well as the continued security of the processing and whether the data appears in public sources*".

Rather than deleting the restrictions excluding transfers that are massive, structural or frequent, JUST proposes to make these restrictions applicable whenever one of the exceptions listed in Article 41 apply. This is not acceptable as it achieves the opposite result.

Article 40 refers to the use of Binding Corporate Rules as a tool to transfer personal data to countries without adequacy status. Unfortunately, the current system applies only to data that is processed within a corporate group as a data controller or as a processor. This means that, in principle, this tool would not be available in the relation to data transfer between two distinct groups of undertakings. There does not appear to be a fundamental reason why BCR could not be extended to cover this situation.

Therefore, we suggest clarifying in Articles 3 Nr.17 and 40 of the draft DP Regulation that Binding Corporate Rules can also be agreed between controllers and processors that are not part of the same group of undertakings.

V. Relationship with the ePrivacy Directive

Articles 88 and 89 deal respectively with "repeals" and "the relation between the Regulation and the ePrivacy Directive".

Regarding repeals, Article 88(1) and (2) provide that Directive 95/46/EC shall be repealed and references to the repealed Directive shall be construed as references to the Regulation. INFSO suggests adding a third paragraph to address references in the ePrivacy Directive to the current Data Protection Directive. The proposed Article 88(3) has two main components. A general provision setting forth that any reference in the ePrivacy Directive to the repealed Data Protection Directive will be understood as reference to the Regulation. In addition, it integrates the current Article 89 of the draft DP Regulation, which specifies that Art. 15(2) of the ePrivacy Directive – dealing with sanctions - should be understood as reference to the Regulation. For consistency reasons it appears more appropriate to include it in Article 88 dealing with repeals.

In addition, Article 89 has been amended and broadened to address the relationship between the Regulation and all other, existing and future, Union legislation relating to data protection, including the ePrivacy Directive. The wording, which was discussed with the Legal Service, is the same as in Article 15(2) of Regulation 765/2008 on Accreditation and Market Surveillance. It reads as follows: "*Each of the provisions of this Regulation shall apply in so far as there are no specific provisions with the same objective in other Union legislation"*. It recapitulates the *lex specialis* principle (applied in ECJ case C 45-09, C-582/08, C-252/05). Thereby the relationship between the Regulation and all other Union legislation is clarified once for all, regardless of the final wording of the Regulation.

This has been complemented with a recital as follows: "*The framework for data protection, privacy and free movement of personal data established by this Regulation should complement and strengthen other provisions in Union legislation relating to the same area and the enforcement of such provisions. However, in accordance with the principle of lex specialis, this Regulation should apply only in so far as there are no specific provisions with the same objective, nature or effect in other existing Union legislation, such as in Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector [fn] and [police Dir], or in future rules of Union legislation. Corresponding provisions of this Regulation should therefore not apply in the areas covered by such specific provisions in other Union legislation.*"

This is irrespective of any future amendments to the ePrivacy Directive that may be proposed in the near future.

VI. Review clause

The development of ICT has often raised difficult questions regarding the application of the principles, rights and obligations of the data protection framework. This has been the case since the adoption of the Directive and it will continue as new information and communication technologies further develop. The Article 29 Working Party, in its advisory role to the Commission, has provided input on the application of the data protection principles to social networks, search engines, geolocalisation services, OBA, etc. Currently it is working on a cloud computing opinion. Article 29 Working Party contributions provide input. However, DG INFSO considers that additional voices, including those from civil society, data controllers, academics, manufacturers of ICT and citizens at large are necessary in order to have a comprehensive vision of the problems at stake and the possible solutions.

To ensure input from this constituency, INFSO suggests including the following provisions:

Article 90 deals with the need to submit reports on the evaluation and review of the DP regulation. We suggest adding the following lines: *For the above purposes, the Commission shall (i) monitor the effectiveness of the current legal and regulatory data protection and privacy framework to reach its intended objectives in the light of developments of information communication technologies and social behaviour; (ii) assess the evolving notion of data protection and privacy in view of the technological evolution; (iii) envisage possible complementary policy solutions (self- and co-regulatory processes, new legislation, research orientations). For the purpose of the evaluation, the Commission shall involve all interested parties, including data protection authorities, electronic communications regulators, business sector, civil society organisations, experts in the field, and academics, inter alia through the High Level Group set up in accordance with Article 90A to represent these interests*

In addition to the above, a new article (90A) has been added creating a High Level Group, as follows: *A high level group ("HLG") will be constituted within 12 months of the date set out in Article 91.2 on the basis of a proposal from the Commission. It will be composed by representatives of the range of interested parties mentioned in Article 90A. The HLG will be convened and chaired by the Commission. The purpose of the HLG will inform about the new conditions arising from ICT developments in the policy process, in order to maintain a high degree of data protection and privacy while reaping the benefits from the digital transition and to advise the Commission at its request or on its own initiative. To this effect, the HLG, on its own initiative or at the request of the Commission, will in particular: (a) advise the Commission on issues related to the protection of personal data and privacy related to the development of information and communication technologies and social behaviour, including on any proposed amendment of this Regulation; (b) issue reports, on request from the Commission or on its own initiative on the application of this Regulation to new data processing operations that take place as a result of the development of information and communication technologies, including providing recommendations for policy developments.*

The above is complemented with a recital that reads as follows: "*The Commission should periodically review the effectiveness of this Regulation in light of its objectives of protection of personal data and privacy and enabling the free movement of personal data within the Union. The reviews should inter alia assess whether the obligations imposed on controllers continue to be necessary and efficient for the purposes of the protection of personal data and privacy and whether data subjects are able to effectively exercise their rights. In undertaking the reviews the Commission should consider all relevant factors, including experience gained on the effectiveness of this Regulation, the evolution in the field of data protection and privacy, including social behavior and technological developments. The reviews should be based on consultation of all relevant stakeholders and take full account of the views of the high level group".*

There are provisions for similar networked evaluation and learning in, for example, the Services Directive, and such practices are part of the SR/CR/SCR vision recently laid out by the current College. If the precise wording set out above seems improvable, we are open to further discussion. But we believe that, precisely in order to embed the proposed revision for the long term, it would be important to develop an explicit mechanism to capture the evolving debate around privacy on terms that empower the Commission to continue to steer the process.

In addition to the above and for the same reasons, INFSO considers that the mechanisms for coordination in the data protection field (namely, the European Data Protection Board) would benefit from structured inputs from the same range of stakeholders. In particular, taking into account that the EDPB guidance will be frequently called upon to shape the application of the legislation in the light of evolving technology and social practice, the need for such input is further emphasized. To achieve so, INFSO suggests adding a new paragraph under Article 65 "Task of the European Data Protection Board".

INFSO suggests adding a new paragraph 2 (2 bis) which would read as follows:

"Where the European Data Protection Board advises the Commission pursuant to Article 65(1)(a) , the European Data Protection Board shall, where possible, consult the High Level Group established pursuant to Article 90A".

VII. Other points

In addition to the above, INFSO wishes to highlight the following additional points:

VII.1 Directing activities

Article 2(2) stipulates that the Regulation applies to controllers established outside the EU where the processing activities are directed to EU based data subjects, or serve to monitor the behaviour of such data subjects. Recital 15 explains how such principle should be understood. INFSO considers that this principle should be further clarified, including the meaning of "monitoring behaviour". For example, a recital could be added along the following lines:

" Monitoring individuals' behaviour should encompass a set of activities by which the data controller tracks and collects pieces of information related to individuals sufficiently broad to show their actions over a given timeframe, for example, their internet surfing

behaviour. The logging of client behaviour within a website only, for example, by the publisher of the website setting first party cookies to recognize a user when he/she returns to the site should not qualify as such monitoring".

In addition, we have amended Recital 16 to clarify that one criterion to determine whether a controller is "directing" EU citizens is the use of top level domain names of EU Member States or the ".eu".

VII.2 Definition of a child

Article 3 Nr.18 defines a 'child' as any person below the age of 18 years. Consent of a child is only valid when given or authorized by parent or custodian. INFO questions the need to include the definition of a child within the scope of the current Regulation. Furthermore, even if such definition was considered necessary by JUST, INFSO has not been shown sufficient evidence to justify the age limit of 18 years. It appears that 13 years is more in line with current views and practices. INFSO notes that choosing 18 years as age limit would have important effects on access to online content for teens for activities which they currently do without their parents' consent, such as opening an account with a provider of social network services.

In the light of the above, INFSO suggests keeping the definition as it is and instead setting for the age limit of 13 years old to determine when parental authorization is required. This threshold reflects current views and practices. For example, the guidance from the International Working Group on Data Protection in Telecommunications proposes the threshold of 12 years, the highest specific age of consent in the EU is 14 (in Spain). In the US, the Children Online Privacy Act ("COPPA") sets 13 as the threshold is in line with current practices and Therefore, INFSO proposes introducing the following: "Consent of a child below 13 shall only be valid when given or authorized by the child's parent or custodian."

Furthermore, in order to enable taking into account the specific features of different data processing sectors, codes of conduct drawn up and decided as having general validity under the Regulation ex Article 35 may provide for a differing definition.

VII.3. More harmonisation

Despite the clear trend towards harmonisation, INFSO notes that some provisions such as freedom of expression (Article 80), health data processing (Article 81) still leaves some room for national discretion. INFSO is concerned that this will limit the benefits of a single law applying to all. Furthermore, it will introduce questions about applicable law which the draft DP Regulation intends to solve (e.g., a court in country A assessing the application of the national measures adopted by virtue of the Regulation by another country). Therefore, INFSO invites JUST to better define the scope of the national measures in these respective areas.

VII.4 Health data (processing for health purposes)

Articles 81 and 8 deal respectively with the processing of data for health purposes and the processing of special categories of data, which include data related to health. INFSO is concerned about the interplay between these two articles and supports a revised version of Article 81(1) which would read as follows:

1. Within the limits of this Regulation and ~~in particular~~ in accordance with Article 8~~(2)(h),~~ ~~and subject to specific and suitable safeguards so as to protect the fundamental rights and the personal data of individuals,~~ Member States shall ensure that data concerning health may be processed only if processing of those data is subject to specific and suitable safeguards so as to protect the fundamental rights and the personal data of individuals and necessary for: (…).

In addition to the above, INFSO supports adding a recital that would clarify that Article 8.2(c) applies rather than Article 81, when there is a **medical emergency and processing of data is necessary** –as follows: "The processing of personal data should equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data subject's life.

INFSO further supports an amendment to Article 8(2)(h) clarifying that the general principles of Article 4 also apply to health data as follows:

"(h) processing of data concerning health is necessary for health purposes and subject to the conditions and safeguards referred to in Article 81"

In addition, INFSO supports adding a new paragraph to Article 81(1)(b) as follows:

"(b) the purposes indicated in Article 83" to ensure that data concerning health may be processed for research related purposes.

VII.5. Processing of data for security purposes

As part of their job to prevent and investigate incidents on the Internet, Computer Security Incident Response Teams (CSIRTs) often handle information that is associated with identifiers such as Internet Protocol (IP) or e-mail addresses. For example a compromised computer used to send spam will often contain all the e-mail addresses to which spam was sent and the IP addresses of the hosts from which it came, while logs from firewalls and intrusion detection systems will normally be tagged with the IP addresses of the computers that may have been the sources and targets of hacking or denial of service attacks. To resolve incidents, CSIRTs need to use this information themselves and may also wish to disclose it to others, for example to inform individuals or banks of a phishing attack or to warn potential victims of a new virus threat.

If such information is personal data, CSIRTs must have legal grounds legitimising this processing. CSIRTs should be able to rely on the former Article 7 (f) of the Directive, which corresponds to Article 5 (f) of the draft DP Regulation according to which data controllers may process personal data if doing so is *necessary for the purposes of the legitimate interest pursued by the controller*. The possibility to rely on the "legitimate interests" was explicitly recognised in Recital 53 of Directive 2009/136/EC (Citizens' rights Directive) amending the ePrivacy Directive.

INFSO has updated the Recital to align it to the draft DP Regulation and to mention explicitly CERTs and CSIRTs. INFSO suggests including it into the draft DP Regulation.

"The processing of 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 networks 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"

VII.6 Sanctions

Article 79 (Administrative Sanctions) of the draft DP Regulation appears to be strongly inspired by similar provisions in EU competition law. However, both Article 23 of Regulation 1/2003 (antitrust) and Article 14 of Regulation 139/2004 (Merger Regulation) provide discretion regarding both the issue of "whether to pursue" and on the amount in using the term "may". By contrast, Article 79 of the draft DP Regulation uses the term "shall" thereby excluding the DPAs' discretion as to whether to fine or not. This is likely to lead to burdensome and bureaucratic procedures for minor infringements; in addition there are certainly circumstances under which the imposition of administrative sanctions would be disproportionate.

We therefore urge JUST to replace "shall" by "may" throughout the entire Art 79. Art 79(5) contains sufficient guidance for the DPA's on how to use their discretion.

In addition, the maximum level of fines (up to 5% of worldwide turnover) may be considered as too high.