COUNCIL OF THE EUROPEAN UNION

Brussels, 25 February 2014

6278/13 ADD 1

LIMITE

DATAPROTECT 12
JAI 88
MI 102
DRS 22
DAPIX 16
FREMP 10
COMIX 86
CODEC 300

Interinstitutional File: 2012/0011 (COD)

NOTE

from:	Slovak Republic
to:	Working Group on Information Exchange and Data Protection (DAPIX)
No. prev. doc.:	16529/12 DATAPROTECT 133 JAI 820 MI 754 DRS 132 DAPIX 146 FREMP 142 COMIX 655 CODEC 2745 5702/13 DATAPROTECT 2 JAI 47 MI 44 DRS 17 DAPIX 6 FREMP 3 COMIX 40 CODEC 155
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)

Delegations find attached additional comments from the Slovak Republic on Articles 28 - 39a on the draft General Data Protection Regulation.

Article 28

We agree with UK and we welcome replacement of the term "documents" by term "records".

Form of record should not cause a problem so it is necessary to safeguard the controller choice whether he wants to have in writing, electronic or both forms. Decision should be on controller and regulation should not enter into it. We would welcome enlargement of provision of paragraph 2a namely at least for the purpose of personal data processing when this one is not absolutely clear directly from the business activity or it does not result from the European legislation or legislation of the MS. We support paragraph 3a.

Well formulated appurtenances of the processor record keeping on his/her processing activities could be essential for elimination of uncertainty related to determination of responsibility in legal relations which arise from cloud computing. We fully support provision of paragraph 3.
We are of the same opinion to paragraph 4 as delegation stated in the note no. 226. We apprehended (b) as rather controversial provision. We understand the ambition to unload SMEs as far as the most possible from the administrative burden but we fear that this provision will be abused that the controllers employing less than 250 people avoid obligation of record keeping although it will concern to risky processing of personal data.

Article 29

We support deletion of this article due to its redundancy.

Article 30

In general we support the wording of this provision however we consider as necessary explore if recently changed ENISA mandate, mainly in the context of administrative, capacity and financial appurtenances could fulfil such a function, and if yes thus for what scope. We express doubt above deletion of paragraph 2 because according to us, it appropriately shows to concrete phenomenon that the adoption of measures pursuant to paragraph 1 has primary to eliminate. Further, we appreciate amendment of paragraph 2a. We consider it as rational in the context of alone certification. Similarly, we welcome and support the addition of paragraph 2b. In our national law on personal data protection we already have established obligation to remain silent so-called authorised persons, what correspond to objective term. We consider positively the deletion of paragraphs 3 and 4. In the same way we believe that the whole "Section 2 Data Security" should be analyzed in the context of legislation Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high level of network and information security within the Union.

Article 31 (1)

We support revised wording of this provision and we appreciate rational changes. We propose to harmonize the deadlines of notification of data protection breach and process of notification with other legislation, also with currently prepared, to not put on the controllers duplicate or sometimes triplicate obligation of notification based on various legal acts (ex. with telecommunication framework, ePrivacy directive, current proposal of regulation to ensure a high level of network and information security). It is necessary to preserve the provision of Article 30 (6). It is more than necessary from the perspective of the standardization process through notification templates or forms and from the perspective of harmonisation with other legislation. It ensure reduced administrative burden for controllers and it will facilitate practical performance. It would be ideal if there was even a common form for controllers concerning both notifications of data protection breach and also other incidents of disruption of information systems as described by proposal of regulation to ensure a high level of network and information security. From the perspective of security incidents it is necessary to take also into account just creating mechanisms in relation to ENISA. We do not agree with ES proposal stated in the note no. 426 (document 8004/13). We consider as more appropriate solution creation of list of minimum content of notification requirements. Even it seems to us inappropriate to the deletion of the provisions of (c). Our DPA would appreciate such a base from the side of the controller but we understand that not in all cases it could be truly needed and useful for more effective protection of data subject. Maybe such recommendations should be notified to DPA on request of DPA presented to controller. We support BE proposal in no. 232.

Article 32

The Slovak Republic appreciates revised wording of this provision which proportionally decreases extent of administrative burden, takes into account "risk based approach" and in the same time undertakes sufficiently information of data subject about data protection breach and about related risk. However we would like to remain our scrutiny reservation stated in note no. 239 because it is important provision which we want to analyse. We support BE proposal in footnote no. 232.

We consider as disputable the provision of paragraph 3 point a) and its technical impact should be further analysed by IT experts. We are of the opinion that it is at least questionable because performance of additional technical operation precluding further disclosure of already intelligible data by their "encryption" ensures their safety and if it is a sufficient reason to grant an exemption from obligation of security notification. We appreciate clarification stated in the preamble (68a). We support the wording of Paragraph 3 point a) to b), as well as deleting the Paragraph 5.

Article 33

In general the Slovak Republic welcomes the aim of this article however it still insists on its remark that it can cause inadequate administrative burden for same cases in application practise for "small" controllers. In the same way we are not identified with it that the obligation under paragraph 1 extends to the processor too, we want to be add to the delegations stated in the footnote no. 251. Primordial responsibility for data processing should repose on controller even at the level of fullfilment of the obligations. In relation to the processor is needed that this one is able to guarantee appropriate security measures for conditions of concrete personal data processing, for what he/she should be responsible concretely in intentions of agreement concluded with controller. We would also welcome to take into account possibility of adoption of exemption for public authorities. Public authorities in Slovak Republic already have an obligation to elaborate so-called security policy aimed at security of IT systems of public administration. We are concerned that failure to differentiate between public and private controllers could lead to increased administrative burden for public sector without creation of added value in the area of data protection ensuring higher level of security.

In regards to the Article 33 Paragraph 1 we are of the opinion that the formulation "present specific risks for the rights and freedoms of data subjects" could be more specified acording to Luxembourg proposal stated in the note no. 454 (document 8004/13). Identity theft or financial loss financial loss could be specified together with other specific and frequent risks existing in data processing (ex. automatic processing of large amount of personal data stated in paragraph 2). Provision of the paragraph 2 point a) seems to us as more appropriate to emphasize such a concrete specific risk relating to personal data processing.

The Slovak Republic mentions to paragraph 2 that it insists on its remark to the term "on a large scale" which is, according to us, necessary to specify further. Under the current wording of the paragraph 2 point e) in connection with provisions of paragraphs 2a and 2b it is not clear if different conditions, respectively list of processing operations which will be necessarily different for some MS pursuant to the paragraph 2 point e), will not mean an unjustified different applications of the obligation to elaborate an evaluation pursuant to the paragraph 3. We deem provision of paragraph 2 point e) as a good possibility to answer to different conditions in different MS allowing flexible modification of this obligation which may have risk intervention to the rights of privacy and data protection of data subjects. However it is not clear for us what concrete should be adopted for the mechanism of establishment of duty to adopt. Risk assessment pursuant to the paragraph 2 point e) will mean obligation of precedent communication DPA with European Data Protection Board pursuant to paragraph 2a. We consider it as appropriate to establish expressly whether the consent of EDPB is needed in such a case. If consent of EDPB for determination and issuing of list of kinds of data processing operation which will fall under the obligation to adopt impact assessment to data protection pursuant to paragraph 2 point e) is not needed we propose deletion of obligation of communication between DPA and EDPB or replace the word "communicate" in paragraph 2a by word "announce".

Article 34

The Slovak republic welcomes especially changes in paragraph 3. We apprehend positively interconnection of paragraph 2 and 3 as well as reduction of DPA obligation to provide prior consultations. We would not that the obligation of prior consultation "hide" in itself possibility of authorisation of processing operation arising from provision paragraph 3a, therefore we appreciate the deleting of this provision. We see a sense rather more in informal guidelines which can help to build confidence and cooperation between DPAs and responsible subjects. The result of negative consultation shouldn't be right possibility of DPA to prohibit the processing operation in question for the reason of its risk but rather the obligation of DPA to issue recommendation for controller and processor how to advance to mitigate the risk. Only in the case of disobedience of recommendation and performance of risk operation the DPA would have to have a possibility to react, e.g. by disclosure of such controller and its processing operation or in high-risk cases by prohibition of processing in question. Financial sanctions, without the occurrence of adverse effects arising from performance of such risk operations, would not be included into these legal relations, as the controllers and processors would be motivated to consult in advance. This specific competency of DPA would ask for its incorporation to Article 53. In Paragraph 6 we propose narrowing the group of information, which can be requested by DPA from formulation "*any information requested by...*" on formulation *"information related to the subject matter of the prior consultation...".*

In general we understand and support the motivation, which is beyond the provision of Paragraph 7a, but we have concerns about the possibility of practical application. This provision will have significant impact on the activities of DPA. In the framework of national legislation are adopting huge amount of legal acts, which in some way contains processing the personal data from the point of view of public interest. We are still not sure about the meaning of the legal concept of "public interest" on the purposes of the proposal of this regulation. This situation is concerning. In terms of our national perception of the concept of public interest it is generally a vague legal term, which may be for specific laws specifically defined. From this point of view at this problem, we consider it necessary in the normative text finally solve the problem of distinction and meaning of the definitions of the public interest and important public interest for the purposes of this legal act. In regard to the fact, that Slovak DPA is small body limited by personal capacity, despite the planned strengthening in the future as one of the results from European data protection reform, we have significant concerns regarding to the practical performance of agenda, which results from the Paragraph 7a. We would appreciate clarification of this distinction and the concept of public interests, which could then be used in the actual provision of the Paragraph 7a in the way that it would be replaced the "public interest" by "important public interest", what could decrease the amount of cases for prior consultation and administrative burden for DPA.

SK supports reached compromise which it is necessary to develop further by specification of a processor´s obligation to help the controller with fulfilment of duties under Articles 33 and 34 and by including the DPO into this process.
We agree with PT, NL. DE, UK and COM, which requested the elaboration of risks list in Art. 33 (2) in not an exhaustive manner.
SK also supports RO, MT, FI and DK in their opinion that the national DPA should not have a time-limit for execution of prior consultations.
SK further supports opinions of LV, HU and IT which expressed a request to give national DPAs a possibility to give prior consultations and prohibition of the processing

Article 35

In Article 35 Paragraph 1 the wording “or where required by Union or Member State law shall” is too general. We more prefer direct regulation with particular conditions or criterions based on risk approach for designation DPO. Such criterion could be e.g. number of persons who are processing personal data for controller (so-called “entitled persons” under our national law) or other risky criterions such as automated means of processing connected with internet, processing of special categories etc. In practise was confirmed the situation, that the greater number of persons coming into contact with personal data caused the increase of likelihood of threat of security of personal data, so the supervision of the DPO is more needed. This concept would be support by obligation of controller to authorize the DPO in writing. The written authorisation is important mainly from the reason of provability to the DPA (e.g. during the exercise of control), that such a person was really designated for internal supervision of personal data protection.

In Article 35 Paragraph 2 we support Germany (footnote no. 490 in document 8004/13). For groups of undertakings could be designation of just one DPO insufficient. The performance of supervision of personal data protection by one DPO for multiple controllers could be from territorial and time reasons in practise very often unreal.

In Article 35 Paragraph 3 we insist on scrutiny reservation on terminology “public authority or body”. In our legal understanding in the terms of influence to our national legislation seems more appropriate use just “public authority” (eventually “bodies of public administration” or “bodies of public power”).

In the Article 35 Paragraph 5 is missing some arrangement or way of verification of qualities, knowledge and abilities to fulfil the tasks of the DPO. Our practical experience force us request regulation for this problematic, so we propose to add that the DPO can be designated only after the fulfilment of conditions which can be stated under Member state law. We consider as necessary, in order to the knowledge and abilities of the DPO wasn´t just formal, but also real. We also support Poland in the footnote no. 281. In this provision is from our point of view missing positive and negative specification, who can be and can´t be the DPO. We propose to add, that DPO can be only natural person enjoying the full legal capacity, without criminal record, who fulfilled the conditions for performance of function of the DPO stated under the Member state law. Next we propose also basic negative criterion for creation the DPO. Due to the possible conflict of interests the DPO can´t be a natural person, who is a statutory authority of the controller and a natural person, who is entitled to act on behalf of the statutory authority of the controller.

Article 36

In the Article 35 Paragraph 4 we agree, that character of this provision is prescriptive, but we consider it necessary. Possible conflict of interest between the DPO and controller or processor must be covered, so we support the request of French delegation for further clarification (footnote no. 286).

Article 37

We propose the addition of Paragraph 1 by this text: ***"****Before commencement of the processing of personal data in the filing system the data protection officer shall assess whether any danger of violation of the rights and freedoms of data subjects arises from their processing. The personal data protection officer shall notify the controller in writing without undue delay of any determination of violation of the rights and freedoms of data subjects before commencement of the processing or of determination of a breach of statutory provisions in the course of the processing of personal data; if after the notification the controller fails to rectify the situation without undue delay, the personal data protection official shall notify the supervisory authority of it."*

In the case of adoption certain criterions which will determine the possibility to perform the function of the DPO should be added also the obligation of the DPO to announce the lost of capacity (e.g. breach of the positive or negative criterions) to perform his/her function to the controller.

Article 38

Slovak Republic would point out on not clear added value resulting from this provision. As a deficiency of Codes of conduct we perceive that, from the applicable legislation do not result to this legal institute no important legal effects, as well as no motivation for their implementation to the particular sectors by controllers or processors. Also the issue of legally binding effects of Codes of conducts are not clear. Will be the Codes of conducts prior legal acts after their authorization, than regulation? Actually we perceive the Codes of Conduct as academic documents, which may have guidance value for right application of regulation in some specific sector (e.g. health care, insurance industry), so the present concept of obligation to monitor compliance by independent body under Article 38a seems too heavy and we do not quite agree with this. Codes of conducts as well as certification mechanisms we perceive as foreign elements, because in the national legislation of personal data protection we have not any experiences with them. Therefore we appreciate proposals of other more experienced delegations and still insist on our scrutiny reservation on whole Article 38 and Article 38a. But on the other hand our basic position to the Codes of conduct is *apriori* positive and the last update of these provisions it seems as significant step forward.

Article 39 and 39a

Slovak Republic has not any fundamental objections. We appreciate work of German and Spanish delegations as well as the Presidency, which help this provision significantly improve. We support the basic importance of certification, which allows the data subject immediately recognize the controller and processor who guaranteeing safe level of processing personal data. We are for linking with Article 23. Provisions of Article 39a we see more problematical. In Article 39a Paragraph 1 are introduced accreditation scheme, which is not in compliance with standard accreditation procedure established for certification of products and services in general. Therefore we are not like to see the DPA in the position of accreditation body of independent certification bodies. Also it is not quite clear whether there should be certification bodies only the public authorities or can be also subjects from private sector. This could be to clarify. In Article 39a is absent the legislation which would clarify the issue, importance and distinguishing of certifications marks and seals.