The reform of the EU Data Protection framework - Building trust in a digital and global world

9/10 October 2012

Questionnaire addressed to national Parliaments

Please, find attached a number of questions that will serve as the basis for the panels of the Interparliamentary Committee Meeting on 9/10 October 2012.

Replies to the questionnaire (in English, French or German) should be sent by Friday, 21 September 2012 to libe-secretariat@europarl.europa.eu.

Please, find below for your convenience a link to the website of the European Commission on EU data protection in general and specifically on the two legislative proposals on data protection (General Data Protection Regulation and Data Protection Directive on criminal law):

http://ec.europa.eu/justice/data-protection/index_en.htm

SESSION I - The reform of the EU Data Protection framework - Building trust in a digital and global world

1. Do you see a necessity and added value in the proposed EU Data Protection reform (questions on subsidiarity and the chosen legal form - two instruments - regulation and directive)?

AW: The proposed package has long been expected in order to provide for a comprehensive, high level of protection of personal data. We, moreover, see an added value and necessity. Especially, as regards the Regulation, globalization and new technological developments and lack of harmonization under the Directive 95/46/EC make the new proposal necessary and this new proposal makes a substantial step forward to strengthen the fundamental right. Nevertheless, the Directive lacks of the same high level of protection which is not duly justified with regard to the specific sector of law enforcement (deficiencies may be found with regard to the definition of competent authorities, scope of application, data processing principles, data subject rights, data controller's obligations incl. security measures, international transfers, transfers to non law enforcement bodies, powers of supervisory authorities). Therefore, in the field of the Directive, it should be thoroughly examined whether the lower level of protection is justified. A high level of protection in this field would make obsolete some expressed concerns about the issue of subsidiarity. Recital 10 of the Directive 95/46/EC provides for that the level of protection should not be lower than the one provided by the MS legislation and the same should apply with regard to new package.

2. How do you see the relation between Union and national legislation (questions on subsidiarity and the chosen legal form - two instruments - regulation and directive)? Should there be more flexibility for Member States to regulate data

processing in special situations? How would this affect the harmonisation of the internal market?

AW: The more flexibility is provided the less the harmonisation effect. The current drafts build already on national law (i.e. for defining a legal obligation or a public interest according to the national law) which is inevitable taking into account the existence of national rules in different fields, i.e. employment, taxation etc. Moreover, some other provisions of the draft Regulation provides for the power of the MS to adopt national laws in the context of employment, health and freedom of expression (Chapter IX). These provisions should be thoroughly examined towards a higher level of harmonisation. Finally, article 21 of the Regulation provides for restrictions to the application of the Regulation which may allow considerable divergences and, therefore, it should be reconsidered in the light of harmonisation and safeguarding a high level of protection. For instance, the public interest should be clearly identified and the exception of the application of the principles as enshrined in article 5 should be deleted.

3. What are in your opinion the main missing elements, if any, of the current EU system of data protection based on Directive 95/46/EC and Framework Decision 2008/977/JHA?

AW: The main principles of the Directive 95/46/EC are not disputed. The draft Regulation, however, keeps paces with the globalisation and technological developments, enhances the accountability of the data controllers, strengthens the data subject's rights, strengthens and harmonises the powers of the supervisory authorities, and provides for more harmonisation in the internal market.

The draft Directive regulates also domestic data processing which is not the case within the Framework Decision. This element is, however, important since it is not consequent to regulate the cross-border data transfers but do not provide for the same level of protection regarding purely national data processing. It is also not practical to keep two different legal regimes, one for cross-border transfers and one for domestic data processing. However, as mentioned above, the draft Directive does not provide the same high level of protection as the Regulation, while this is not duly justified according to the nature of processing. In some cases, it does not even provide the same level of protection as the Framework Decision 2008/977/JHA, i.e. in case of security measures which in the draft Directive do not include the accidental loss of data and in case of data transfers to other MS where the receiving MS is not obliged to respect any limitation of processing imposed by the transferring MS (article 37 of the draft Directive).

4. How to ensure that the envisaged legislation will keep up with technological developments? Are, in your opinion, the principles of "privacy by design" and "privacy by default" an adequate approach?

AW: These principles are an adequate approach. Nevertheless, stronger incentives for these principles should be foreseen.

SESSION II - Data protection rights and principles - Harmonised rights for a clear and better protection, easier enforcement and building more trust

5. What is your opinion about the provisions regarding the rights of data subjects and their applicability in practice, such as portability, right to be forgotten, deadlines to address requests for access, rectification?

AW: As a general remark, the Regulation strengthens the data subject's rights in accordance to the nature of the right to data protection as a fundamental right and in line to the technological developments.

Regarding the deadlines these are appropriate and constitute an improvement in comparison with Directive 95/46/EC. In the Greek data protection law (even shorter) deadlines are already laid down.

Regarding the right to be forgotten it should be further clarified that the data subject may, in addition, exercise its rights towards the third parties, whose position is not clear in the Regulation (are third parties qualified as controllers, and if yes, under which conditions), and in cases the controller may not be contacted. Moreover, the provision of article 17 (3) (d) does not provide for an added value since article 21 provides for the same issues.

The right to data portability also enhances data subject's position, without unnecessary or unrealistic burden for the controller. The limitation in article 18 (2) to consent and contractual relationships is not, however, self explaining and should further examined whether it is justified. Finally, it is not obvious why in case of article 18 (2) the controller shall "only" restrict the data in accordance with article 17 (4) (d), should these data be not anymore necessary for the accomplishment of the purposes of the controller and could be erased. Therefore, we suggest also the deletion of article 17 (4) (d).

With regard to the right to object, it should be clarified that if there is a disagreement between controller and data subject the data may be restricted (similar to the cases described in article 17 (4) (b).

With regard to profiling, article 20 (2) should at least come to the same level of protection as the current article 15 of the Directive 95/46/EC, i.e. the data subject shall have the right to submit its point of view (the right to obtain human intervention does not mean that the data subject shall be heard).

As to the restrictions of article (21), it shall be first noted that there are placed in the wrong chapter since the restrictions apply not only to the rights. Moreover, article 21 provides for too broad restrictions, not duly justified, and goes far beyond current article 13 of the Directive 95/46/EC. In this context, the public interest shall be further specified and, to this end, the list in (c) shall not be indicative. Moreover, there is no need that the restrictions in article 21 (1) include also the principles of article 5. This practice which indeed has been followed in article 13 of current Directive 95/46/EC is against the case law of European Court of Human Rights, which always require that an inference with a human right must be provided by a law, which is concrete and foreseeable, and does not fail the test of proportionality. The principles of article 5 therefore should be adhered in any case of restriction of the right to privacy / data protection.

6. What is your opinion about the principles underlying these rights, such as the need for a legal basis for data processing, the conditions for consent, or the notions of "public security" or "legitimate interest" as a basis for data processing?

AW: Some terms shall be further specified, such the "compelling legitimate interest".

SESSION III - Data protection and law enforcement/SESSION VI - Police data sharing and access to private data bases

7. Should such a new framework also apply to purely domestic processing activities by law enforcement or should it be limited to cross-border cases only (question of reversed discrimination, data protection as a common fundamental right from the Charter, subsidiarity, etc.)?

AW: See our answer in question 3.

8. There is a growing tendency by law enforcement to have access to data held by private companies for commercial purposes; how to ensure a proper balance between law enforcement needs and fundamental rights?

AW: It should be made clear that there is no obligation of data controllers to process data for law enforcement purposes "just in case", unless a Union or MS law provides for. Such law shall meet the criteria as recalled in recital 59 of the Regulation.

SESSION IV - Data controllers and processors in the private sector and free flow of information in the internal market

9. Is the proposal reducing regulatory/administrative burden for data controllers, especially as regards small and medium enterprises (SMEs)?

The Regulation provides for a series of obligations for data controllers, in line with globalisation and the developments of new technologies and on the basis of the experience gained from the application of Directive 95/46/EC. Currently, the criterion for lessening the burden is the number of employees, i.e. less than 250. Nevertheless, it should be reconsidered whether such a criterion is appropriate. First, if such criterion would apply, the Regulation will render inapplicable, as 99,5% of the enterprises in the EU are SMEs. Since the right to data protection is a fundamental right other criteria should be considered, such as the nature of the processing and the amount of the data processed.

10. How will the "one-stop shop" mechanism impact on the laws of the Member States and on the rights of the data subject (legal and linguistic obstacles, etc.)? How to guarantee that decisions are lawfully enforceable in the Member State of residence of the data subject?

AW: Current scheme of the "main establishment" does not take due account that many questions require analysis of national law (i.e. in the employment or taxation field etc combined with the legal basis of legal obligation of the controller or MS law) and can not be appropriately dealt with by the DPA of the main establishment. Moreover, the current scheme would make data subject's right to access to justice very difficult, shall this bring proceedings before the courts of the MS where the DPA is established (article 74 (3)). The alternative provided for in article 74 (4) is not appropriate, because apart from the burden that this means, the DPAs role is primarily to enforce the law and cooperate with each other towards this aim, not bring proceedings against each other.

The one stop shop mechanism may be used for "administrative" issues, such as already the case with BCRs where a leading authority uptakes the coordination.

11. How to ensure that the envisaged legislation will keep up with technological developments? Are, in your opinion, the principles of "privacy by design" and "privacy by default" an adequate approach?

AW: See our answer in question 4. Moreover, the Regulation is technologically neutral and may, thus, keep up with technological developments.

SESSION V - Implementation, DPAs and ensuring consistency

12. How do you evaluate the proposed sanction mechanism (level of sanctions, proportionality, discretion, legal remedies, etc.)? How would this affect provisions in your Member State, and what are the experiences with the current model?

AW: The Regulation should leave a higher discretion as to whether the supervisory authority shall impose a sanction (fine) or warning, taking into account all circumstances, including the clarity of the obligations of the controller. Moreover, the Regulation shall clarify whether sanction shall be combined with other enforcement powers, such as, the ban of processing. According to the Greek experience fines are combined with other enforcement powers. Finally, it should be clarified to what extent criminal penalties may be imposed taking into account the ne bis in idem principle.

13. How do you evaluate the proposed consistency mechanism (the fact that national DPAs will be required to abide by the decision taken within the consistency mechanism, and the questions of their independence and the risk to act in breach of national law)? How do you perceive the proposed role of the Commission in that regard, especially as regards the question of independence of the European Data Protection Board?

AW: First of all, it is problematic in the context of independence of national DPAs the role of the Commission with regard to its power to suspend the adoption of draft measures and the obligation of the national DPA to take utmost account of Commission's opinions. With regard to the European Data Protection Board account shall be taken to its obligation to issue an opinion on a matter dealt with in the consistency mechanism upon request of the Commission.

As to the first part of the question, a consistency mechanism is necessary to ensure a harmonised approach in the cases described therein. One may not easily say that the independence of the DPAs is affected merely because they have to take account of the opinions of the European Data Protection Board which consists of peers. The issue of contrary national law shall also be part of the deliberations before issuing an opinion.

14. How do you evaluate the resources of the data protection authority/authorities in your Member State? How to ensure they are sufficient in a world of ever more data processing?

AW: According to the annual reports of the Hellenic Data Protection Authority, which are submitted to the Parliament, it lacks sufficient human and financial resources to perform effectively its duties. On the basis of current resources considerable delays may be noticed in the investigation of complaints and the performance of other tasks.

To ensure the resources are sufficient in a world of ever more data processing, we consider that DPAs should be given the means to flexibly and rapidly adapt their resources to the workload faced.

SESSION VII - Data Protection in the global context- Protecting rights in the global world

15. How do you evaluate the proposed international transfer mechanism in both proposals taking into account that the EU and third states frameworks are not always based on same principles and do not offer the same protections for individuals?

AW: As regards the Regulation two provisions allow for the transfer without appropriate safeguards. First, article 42 (5) provides for a transfer without legal binding effect of the appropriate safeguards, where the national DPA has approved such transfer. This provision should be deleted because the binding effect is an essential element of the appropriate safeguards, without which it is questioned how a national DPA may assess the transfer. Second, article 44 (1) (h) should be amended in order to allow the transfer only in case such transfers cannot be qualified as massive, structural and repetitive.

As regards the Directive this does not provide for the same level of protection. First, it should be clarified that onward transfers shall be made only to competent authorities within the meaning of this Directive (article 33) and upon prior consent of the transferring authority. Where there is no adequacy decision the controller or processor shall not be allowed to transfer the data merely on the basis of a self assessment, as currently article 35 (2) provides for. The assessment by the controller itself may not be considered as appropriate safeguard, and an authorisation by a DPA is impossible without clear criteria. We would therefore suggest its deletion.

Moreover, where there is a non-adequacy decision than the transfer shall be allowed only on the basis of stricter derogations, i.e. if appropriate safeguards by means of a legally binding instrument are taken or in cases of article 36 (a) and (c). To this end, article 34 (6) shall be amended, respectively.

Finally, it should be clarified in article 36 that such transfers are not massive, frequent and structural.

16. The Commission has indicated that its proposal aims at simplifying international transfers and overcome burden for controllers. Does this mean that data subjects' rights will be less protected?

AW: No, if necessary amendments and clarifications are made (see our answer in previous question).

17. Do you have any other remarks as regards the proposed reform package?