Parliament of Romania
Chamber of Deputies
Committee for information technologies and communications

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

9/10 October 2012-09-24
Questionnaire addressed to national Parliaments

1. The proposed EU Data Protection reform aims to ensure a better protection of the privacy and personal data of European citizens, through increasing the level of harmonization of national legislations. Currently, the EU regulatory framework on data protection is implemented in different manners, in different member states, and this leads to legal uncertainty among the companies activating at European level (and which, in the performance of their economic activities, are subject to the EU legislation on data protection), on one side, and to a non-uniform level of protection with regard to EU citizens privacy and personal data. Under these circumstances, the new regulatory proposals launched by the European Commission bring added value to the existing EU concept of privacy and data protection, through ensuring that, once adopted, they will lead to more legal certainty and to better protection, thus benefiting both citizens and businesses. In addition, the new provisions included in the proposed framework (strengthening the right to be forgotten, giving citizens easier access to their data, consolidating the powers of the national data protection authorities, creating the data protection officer position) are aimed at ensuring that citizens fundamental right to privacy and data protection is exercised in a proper manner and respected as such by all relevant actors.

2. As mentioned above, the increase level of harmonisation of the European national data protection legislations is a legitimate aim, as it can contribute to a better protection of a fundamental human right. However, given that several national parliaments have questioned whether the proposed regulation is fully in line with the subsidiarity and proportionality principle, it is our view that these issues still need to be carefully analised, in order to clarify whether the rules established under the proposed regulation should be directly applicable to member states, as proposed by the European Commission, or whether member states should be given the possibility to transpose them in their national legislations, while taking into account their internal realities.

3. The current legal framework on data protection is not fully adapted to the continuously evolving technological environment. For example, the privacy by design and privacy by default concepts are missing from the existing framework, but the level of use of technological devices whose functionalities have implications for data protection requires the respective concepts to be included into legislation. A strengthened right to be forgotten, the right to data portability and increased authority for the national DPA are other examples of provisions that are not included in the existing legislation, but whose introduction would benefit European citizens.
4. The privacy by design and privacy by default concepts constitute an adequate approach, as they consitute an attempt to adapt the data protection legal framework to the technological developments. It is important that new devices and services are built while taking into account the need to ensure and protect users' right to privacy, as opposed to the numerous existing models, in which users are invited to activate privacy options after they start using the service or device. These existing models often lead to citizens rights to privacy being violated, mainly as a consequence of the fact that users are not aware of the way in which they data are used and of the features they could activate in order to better protect themselves. However, it shall be noted that legislation must be technologically neutral and that any further step towards legislating means in which the two concepts should be implemented would represent a violation of this principle.
5. The mentioned rights of data subjects represent a step forward toward ensuring a better protection of the fundamnetal right to privacy and data protection. The right to data portability, the better framed right to be forgotten, the obligations of data controllers with regard to users' request for access to data and rectification of data bring more value to the concept of privacy and data protection and are meant to ensure that data subjects are aware of the way in which their data are used and are able to exercise full control over such data, at any moment in time, and irrespective the controller that processes the respective data.
6. The principles underlying the above mentioned rights constitute necesarry provisions whose implementation would lead to a better and more explicit form of protection of these rights.
7. We consider that further analysis should be undertaken with regard to the implementation of data protection rules with regards to data processing by law enforcement authorithies. Also, special attention should be given to already-existing conventions between member states and non-member states. Member states have different national frameworks in which their law enforecement authorities activate, and any new rules imposed on these authorities should take into account these existing frameworks and their specificities. Therefore, the implementation of new data protection rules with regard to the domestic activity of LEA should be made in accordance with national existing frameworks and member states should be given the possibility to choose the most appropriate solution to implement.

8. LEA access to data held by private companies should be subject to judicial control. Thus, LEA access to personal data shall be permitted only with authorisation from a judicial authority and only where sufficient evidence exist that the data subject has commited a crime. In addition, the data subject should be informed in due time with regard to the fact that his data have been accesed by LEA.
9. In our view, the compliance with the rules proposed under the new framework would place significant administrative and financial burdens on private data controllers. For example, the idea of a data protection officer as mandatory for large enterprises in the private sector, as well as the obligation for the controllers to inform third parties which are processing the personal data that have been made public by the controllers about data subject requests to erase any link to or copy or replication of that personal data would have serious administrative and financial implications for the controllers. While we also acknowledge the fact that privacy and data protection are fundamental human rights that need to be fully protected and respected, it is our view that this protection can be ensured without imposing significant additional burdens on the controllers. We therefore consider that some of the new obligations to be imposed on controllers can be further analyzed in order to determine whether they can be reviewed in such a way as to limit the additional burdens to what is strictly necessary for ensuring an adequate level of data protection.
10. Article 51 of the proposed Regulation provides that, where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States. This provision is meant to ensure unity in application of data protection rules at the entire EU level, with respect to all citizens whose data are subject to processing by one controller acting in several states. It also offers more legal certainty to the controller, which will now know exactly what rules are applicable and what authority is responsible for supervising the application of such rules. However, this may generate difficulties for national DPA, who would have to deal with cases in which the processing of personal data has happened in another member state and in which the controller will have to apply decisions in another member states, under circumstances that may not be familiar to the DPA in question. The implementation of such decisions in a MS other than the MS in which the decisions were taken would require for the deciding DPA to be able to monitor the implementation of the respective decisions and to cooperate with national authorities in the other member state. Also, EU citizens may face difficulties with regard to cases which they would have to address to DPAs established in another member state – not only linguistic, but also cost-related barriers. These barriers may be addressed through establishing a better cooperation between national DPA, so that a citizen may be able to address to the responsible DPA through the DPA established in his/her own country, who would act as a middle man facilitating the communication between the two parties.
11. See the answers to question 4.
12. The proposed sanction mechanisms are adequate and proportional. However, their implementation by the national DPA would require new resources to be made available

to the authority. The introduction of new rights for data subject and the role of the DPA to supervise the implementation of these rights, to monitor the activity of data controllers and to take actions in case of non compliance would bring new attributions to the DPA, and, thus, new challenges which the DPA needs to be prepared to face.

13. The consistency mechanism requires that a national DPA asks for the opinion of the European Data Protection Board and the Commission before adopting a measure that falls under certain categories clearly delimited in the proposed framework. This mechanism is aimed to ensure that the national DPAs apply the regulatory framework in a consistent and coherent manner. This would contribute towards ensuring unity in the application of the EU legislation. This provision has the advantage of contributing to a better protection of citizens right to privacy and data protection and to avoiding cases in which national DPA may act abusively against certain controllers. It does not undermine the independence of national DPAs, as it is only a mechanism meant to ensure that the DPA are fully abiding to the EU legal framework. In addition, the DPA concerned by a opinion submitted by the European Data Protection Board with regard to a certain measure is free to decide where it maintains or amend its initial decision.
14. As mentioned above, in view of the new provision of the proposed regulatory framework and the new responsibilities to be imposed upon national DPAs, the national DPA would need to be enhanced with additional resources meant to ensure a proper functioning and fulfillment of its increasingly important role. These resources concern both the financial aspect, as well as the staff number and the level of professional competence of the staff. It is thus important for the DPAs to develop strong policies on training or hiring of subject-matter experts, especially in the ITC field, in order to have the right competences to deal with technological advances.
15. Data protection rules vary considerably at international level, with some states/regions granting higher level of protection to citizens right to privacy and data protection. Under these circumstances, it is essential that national and European authorities ensure that European citizens rights are protected when their data are transferred outside the EU borders. Therefore, the provisions regarding the fact that transfer may take place where the Commission has decided that the third country ensures an adequate level of protection are meant to ensure the appropriate protection of EU citizens. In cases where the transfer is made to a country with regard to which the Commission has not decided whether it ensures an adequate level of protection, this transfer may take place if the controller has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument. The detailed provisions regarding these appropriate safeguards, as well as the cases in which authorization is needed for the transfer create an adequate framework under which cross border personal data transfer are subject to clear data protection rules.
16. The proposed international data transfer rules do not undermine the protection of EU citizens rights. The fact that the cross border transfers are no longer subject to notification to national DPA do not mean that the transfer can be made in all cases, and without adequate safeguards. On the contrary, new mechanisms are put in place meant to ensure an adequate level of protection of the transfer data, but under a framework that is less burdensome for controllers. If the European Commission has decided that certain countries and organizations have adequate level of data protection, then a notification to the national DPA would have no effect but to overload the authority with notification and

to impose meaningless burdens on controllers. Where the Commission has not made such decisions, there are clear rules regarding the appropriate safeguards that need to be adduced by the controller.

Valerian Vreme - Deputy