Interparliamentary Committee Meeting on

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)?

Generally speaking, the regulation provides for greater clarity thanks to more precise definitions and provisions aimed at ensuring a more harmonised application of the law, thereby facilitating free data flow. Due to the nature of this instrument, the discrepancies in regulations of various Member States will also become limited, whereas current practice shows that such discrepancies have hitherto been rather considerable. Adopting the General Data Protection Regulation is going to align substantive data protection law, whereas rules of procedure will first and foremost be regulated by national law. Such a solution prevents a number of problems connected with performing data processing by entities established in various Member States or when such operations have a cross-border character. Such problems may currently arise, for example, whenever using foreign data protection law by data protection authorities is necessary.
At the same time, the proposed regulation better addresses contemporary challenges. The regulation reinforces the rights of persons concerned by data, *inter alia* by ensuring greater transparency, greater control over processing, data minimisation, special provisions pertaining to processing personal data of children, reinforced right of access to data, reinforced rights to object, the right to portability

of data, reinforced rights to delete data and a reinforced right to redress, both through data protection authorities and courts.
With respect to data controllers, the regulation leads to simplification and greater coherence, places more emphasis on their accountability with respect to data processing operations, *inter alia* through the protection of data by design and by default, establishing a Data Protection Officer (DPO), duties concerning notifying instances of a breach of data protection and adopting a discretionary approach with regard to international portability. Furthermore, binding corporate rules are explicitly stated as the tool for creating the framework for international portability.
With respect to the safety obligations imposed on processors, these are based on regulatory provisions; besides, a new obligation is introduced, i.e. controller liability transfer in specific data processing operations, where the processor goes beyond the controller's instructions with respect to the given processing operation (pertains to service providers offering "cloud processing").
With respect to data protection authorities, the regulation provides for greater independence and broader competencies, including the possibility to impose administrative sanctions and the obligatory consultation of legislative proposals with such authorities, as well as provisions that should ensure harmonised application and, if necessary, enforcement of law, in particular through the "compliance mechanism".
When referring to the proposed directive, one should remember that the proposed provisions should ensure a comprehensive and coherent system of personal data protection. From this point of view, the directive seems less ambitious than the regulation. However, presenting two legal instruments does not preclude the possibility of creating a comprehensive legal framework, provided that the uniform objective is maintained, i.e. achieving a high level of European citizens' data protection in all sectors, and if the instruments are going to follow a uniform approach, *inter alia* to data protection principles, rights of persons concerned by data and the obligations of controllers and processors. Still, from the point of view of the provisions currently applied in Poland, the proposed directive entails considerable progress.

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?

The right to the protection of personal data is stipulated in Art. 8 of the Charter of Fundamental Rights. By means of Art. 16 of TFEU, the Treaty of Lisbon has created a new legal basis for a more modern and comprehensive approach to data protection and free personal data flow, including police and judicial cooperation in criminal cases.
In particular, on that basis both cross-border and national personal data processing can be included in a revised EU data protection framework. This would allow to limit the discrepancies between legal systems of the Member States, with resulting general benefits in the area of personal data protection.

The principle of subsidiarity analysis indicates that the proposed measures are proportional, since they are included in the scope of the Union's competencies as defined in the Treaties and are necessary in order to ensure the uniform application of EU law, which guarantees effective and equal protection of the fundamental rights of natural persons.
In particular, this ensures credibility and a high level of data protection in a globalised world, while at the same time enabling free data flow.
Taking into account the supranational character of personal data protection legislation, the need to regulate data protection matters at the EU level should be acknowledged.

The regulation fulfils the ambitions of drafting a text that would reflect the enhanced importance of data protection in the EU legal order (Art. 16 of the Treaty, Art. 8 of the Charter).
It preserves and reinforces the basic data protection principles, imposes clear and uniform obligations on data controllers and processors, facilitates free personal data flow and ensures a reinforced legal framework for the purposes of uniform application of regulatory provisions by data protection authorities, whose competencies have been increased.
However, it should also be noted that the new legal framework may lead to lowering data protection levels already achieved in Member States in various areas. Especially in the public sector the data protection level varies because of traditions as well as constitutional and legal transformations. Consequently, the new legal framework should ensure harmonised standards in that respect, while at the same time enabling the Member States to adopt more specific regulations (as has already been set out in Chapter IX), without prejudice to the regulation. This also means that they could supplement the regulation.

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?

The current provisions of Directive 95/46/EC did not take into account the technological, social and economic developments of the last twenty years. At the same time, they introduced numerous notification obligations, which have no significant impact on ensuring personal data protection. The practice of applying the implementing rules of Directive 95/46/EC has shown that it does not safeguard the appropriate level of independence of data protection authorities and their competencies.
The main shortcoming of the Framework Decision 2008/977/JHA is its limited application to cross-border data processing operations only.

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?

The right to privacy and to personal data protection is a fundamental EU right and has to be enforced effectively, also on the Internet, using a series of means, ranging from the principle of respect for privacy from the very beginning in respective IT technologies to using deterring sanctions in justified cases. While relying on the recommendations of the Digital Agenda for Europe and the Communication of the Commission on Promoting Data Protection by Privacy Enhancing Technologies, the new personal data protection framework in the EU as proposed by the European Commission assumes that privacy protection by design is necessary during personal data processing preparations. The proposed technological solutions provide an opportunity for ensuring personal data protection in a more effective manner, although they entail further work.

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?

A new solution which appears in the "Rectification and erasure" section is the right to be forgotten and to erasure. Even though such a solution has already been foreseen in Article 12 of Directive 95/46/WE, Article 17 of the proposed regulation considerably expands it: if the controller is responsible for making the personal data public, he not only has to erase them, but also inform any third parties about such a request made by the relevant person, if he provided such parties with the data. This is a solution that is severely criticised by various stakeholders. While welcoming the specific inclusion in the regulation of the right to be forgotten and the right to erasure as a method of increasing natural persons' control over their personal data, it should be stressed that the wording of the proposal requires further work in that respect, since the current wording of these rights in the regulation and the actual functioning of the Internet may considerably reduce their effectiveness.

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?

Current regulations in the scope of personal data protection introduce the obligation of proving the existence of a specific legality premise with respect to certain personal data processing operations. This model has proved effective in the current practice and should be upheld. At the same time, it should be assumed that the consent of the person concerned by data is not the only legal basis for data processing, and often not the desired basis, especially in situations of personal data processing by public authorities, when such basis should be explicit legal regulations. With respect to the basis of data processing, a differentiation should be preserved between private sector entities and public authorities.

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.)?

From the point of view of preserving a coherent personal data protection system, personal data processing by law enforcement authorities may not be limited to cross-border cases only. Taking into account the fact that the right to personal data protection is a fundamental right safeguarded in Article 8 of the Charter of Fundamental Rights and the regulations in that respect are generally based on Article 16 of the Treaty on the Functioning of EU, as well as the practical problems connected with the existing various protection regimes, the future directive should also regulate purely domestic data processing operations.

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?

Unfortunately, neither the Regulation, nor the Directive take up the matter of collecting and transferring data actually meant for public order protection purposes by private entities or public authorities other than law enforcement authorities, as well as the later use of such data by law enforcement. A number of examples from the last decade (e.g. PNR, withholding telecommunication data) have clearly shown the need to establish rigorous provisions, especially if such processing is of an organised nature.
This is also valid the other way round: we also require rules that would safeguard data protection, when information is transferred by law enforcement or other "competent" bodies to the private sector or other public authorities. What follows is that this problem should be dealt with in a more precise manner.

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)?

Exceptions and thresholds aimed at reducing administrative burdens and negative consequences for micro-enterprises and small and medium-sized enterprises (MSME) were introduced into the Regulation. The thresholds were introduced in provisions on the obligation to appoint a representative in the EU (Article 25), documentation (Article 28(4)), DPO designation procedure (Article 35(1)) and imposition of administrative sanctions (Article 79(3)).
In addition, the project provides for the possibility to adopt delegated and implementing acts, which would allow the Commission to include additional issues

related to MSME in Article 12(6) on procedures and mechanisms for the exercise of rights by data subjects, Article 14(7) on the obligation to provide information to data subjects, Article 22(4) on accountability requirements and Article 33(6) on conducting impact assessments in the field of data protection.
It is important to consider if data subjects should enjoy the same degree of protection regardless of whether their data are processed by SMEs or by large companies. At the same time, it has to be acknowledged that some of the proposed obligations may turn out to be burdensome for SMEs. Therefore, it would be worthwhile to consider whether it would not be more justified to implement different restricting criteria.

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?

According to Article 51(1), the data protection authority is meant to be a competent authority on the territory of its Member State. This general rule is supplemented with Article 51(2), according to which the data protection authority of the Member State in which the controller has his main establishment shall be recognised as the data protection authority responsible for supervising processing operations in all Member States. Nevertheless, the rules establishing competence should be clarified in more detail in order to avoid problems during their practical implementation.
Perhaps the concept of a leading authority should be introduced, making it necessary to clarify the term "main establishment", which is particularly important for defining the competence of individual data protection authorities.
Similarly to controllers, the data subjects covered by the scope of competence of the EU data protection authorities should also have access to a “one-stop-shop”. The Regulation provides for several means in which data subjects can exercise their rights and seek justice. Data subjects can lodge a complaint with a data protection authority in every Member State (with its national data protection authority, with a data protection authority of the Member State in which the controller has his main establishment, or with another EU data protection authority). Data subjects may also institute proceedings before their national court or before a court in the country in which the controller has his establishment.
Even though the possibility to take such measures seems to improve the rights of data subjects, those measures can also lead to misunderstandings and uncertainty as to who will be ultimately responsible for providing the answer to the data subject's question.

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?

See answer to question 4.

SESSION V - Implementation, DPAs and ensuring consistency

1. 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?

The introduction of high sanctions has to be assessed positively, as they will enable the data protection authorities to fulfil their role of enforcement authorities and may, due to their dissuasive effect, contribute to improving the controllers' compliance with relevant provisions. Experiences of countries which introduced such an instrument are positive. At the same time, the data protection authority should be provided with a degree of flexibility in deciding when to impose a sanction, as the nature of an infringement is influenced by many different factors which should be taken into account when taking a decision on the imposition of a sanction. It also seems that introducing a threshold with regard to a first and non-intentional non-compliance would in practice exclude many controllers from the scope of this instrument. It would be more justified to take into account the number of data subjects who bore the (negative) consequences of particular operations, and not the number of employees of a given controller.

2. 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?

On the one hand, the role of the EC has an impact on the independence of the European Data Protection Board, while on the other hand one has to determine whether in light of the provisions of the Treaties the Council is capable of issuing binding adjudications. The consistency mechanism should ensure consistency only where it is necessary, and should not limit the independence of national supervisory authorities or interfere in the scope of competences of different entities.
The Board should be notified about cases of general importance for data protection and free flow of personal data throughout the EU.
Irrespective of the role of the Commission as a guardian of the Treaties, the function assigned to the Commission in individual cases, adjudicated under the consistency mechanism, may pose a threat to the independent status of data protection authorities and the Board. If a case is adjudicated or was adjudicated in cooperation with the European Data Protection Board under the consistency mechanism, the Commission should have the possibility to present its legal assessment, but should abstain from any further interference.

3. 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?

The introduction of a new model for cooperation between data protection authorities will require the allocation of additional human and financial resources for the purposes of personal data protection.

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

4. 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?

The Regulation rightly highlights the responsibility of controllers for ensuring that personal data remain protected when they are transferred outside of the European Economic Area (EEA). The Regulation makes this task easier for the controllers by establishing various "safe havens" in the form of adequacy decisions, simplified system of binding corporate rules for multinational companies, approved contract clauses and the granting of individual authorisations by a data protection authority. The Regulation also provides for various derogations under Article 44, which should, however, be treated as exceptional and be applied only in those cases, in which the processing is not massive, repetitive or organised. In addition, Article 42 introduces the possibility to use non-binding instruments in shaping the international transfers framework; it needs to be borne in mind, however, that the use of such instruments needs to be authorised by the data protection authority. Nevertheless, the binding nature has always been considered to constitute an important requirement for existing instruments used for shaping the international transfers framework (e.g. collective agreements, binding corporate rules, safe haven, decisions confirming the adequacy of the level of protection provided in a third country).

5. 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?

As above.

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