EUROPEAN PARLIAMENT 2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

8.10.2012

WORKING DOCUMENT 2

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)

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Jan Philipp Albrecht

1. Strengthening Europe's data protection regime: Steps taken and the way ahead

The discussion of the new data protection regime proposed by the European Commission in January 2012 has made progress in the EU institutions and Member States. As both rapporteurs for the regulation and for the directive made clear in their first working document[1], the reform package incorporates to a great extent Parliament's recommendations as regards (a) adopting a comprehensive approach, (b) strengthening individuals' rights, (c) further advancing the internal market dimension and ensuring better enforcement of data protection rules, and (d) strengthening the global dimension. It should be stressed that data protection is now a binding fundamental right under Article 8 of the Charter of Fundamental Rights and has a specific legal basis in Article 16 TFEU. We should therefore strengthen the protection of consumers and citizens ("data subjects") in the digital and globalised age.

Discussions on issues such as delegated and implementing acts, administrative burdens and the "consistency mechanism" are still ongoing across the institutions. The Council presidency has started the "friends of the presidency" mechanism to discuss such horizontal themes, whereas the Parliament will hear experts and discuss with stakeholders at the annual meeting of LIBE and national parliament's committees on 9 and 10 October 2012. The presentation of the draft report on the Regulation is envisaged by the end of 2012, followed by an extensive deadline that will allow Members to table their amendments in due time (end of February 2013) and an orientation vote in April 2013, allowing for a start of negotiations during the Irish Council Presidency. Committees asked for an opinion are planning their work accordingly. Due to the urgent need for a coherent legal framework in fast evolving environment, the aim of your rapporteur and the shadow rapporteurs is to achieve an agreement on the package with Council during this legislative term.

After four exchanges of views in the LIBE committee, at a LIBE workshop with stakeholders, and extensive discussions with shadow rapporteurs, opinion committees, Commission, Council presidency and stakeholders, your rapporteur hereby presents his more specific proposals and assessments. It is impossible at this stage to come up with a final answer to all pertinent questions raised. However, a few principles serving as guidance for the draft report can be presented. They are based on the existing data protection directive[2] and have been emphasised in Parliament's resolution of 6 July 2011 (Voss report).[3] Your rapporteur would like to achieve consensus on the following cornerstones for the draft report. This Working Document will address substantive aspects, while the institutional aspects will be covered in Working Document 3.

2. Strengthening key principles and clarifying definitions

The definitions of "personal data" and "data subject" are key, because they determine the scope and effective application of the safeguards contained in the Regulation to the various types of processing of personal data. The material scope of the Regulation in this sense should be the same as in current Directive 95/46/EC. As the data protection framework is an

[1] PE491.322v01-00, 6 July 2012.
[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031 - 0050
[3] Texts Adopted, P7_TA(2011)0323, 6 July 2011.

expression of a fundamental right, a limitation of the material scope is not in the hands of the legislator. However, legitimate concerns regarding specific business models can accordingly be addressed in different parts of the Regulation.

In order to reach the best level of data protection and enable new business models, we need to encourage the pseudonymous and anonymous use of services. Clearly defining "anonymity" should also help data controllers understand when they are outside of the scope of the Regulation. For the use of pseudonymous data, in sense of the data controller is able to single out individual persons by a pseudonym, there could be alleviations with regard to obligations for the data controller.

Consent should remain a cornerstone of the EU approach to data protection. Since it is an important legal basis which is commonly used to legitimise data processing, it is necessary that it is clearly defined in the regulation. Awareness of data subjects of what happens with their "digital selves" will be enhanced by their direct involvement and their free decision. We should clarify that technical standards that express a subject's wishes are a valid form of providing explicit consent[1]. Information to data subjects should be presented in easily comprehensible form, such as by "layered privacy policies" and standardised logos or icons[2]. To set incentives for data controllers, we may also reduce the burden by using a simple and easy means to request consent if a privacy impact assessment has been conducted and the system is certified as conforming to the principles of privacy by design and privacy by default. The notion of "significant imbalance" needs to be clarified. In particular, there should be a clear definition which cases market distortions such as monopolies or oligopolies lead to such an imbalance. Specific attention should be paid to the means of obtaining consent for the processing of children's personal data.

Other legal grounds for processing than consent should be clearly defined. The provision on data processing in cases where it is necessary for the performance of a contract should be extended to the provision of a service requested by the data subject. The definition of "legitimate interest" should not be left to a delegated act.

Purpose limitation is a core element of data protection, as it protects the data subjects from an unforeseeable extension of data processing, be it by public authorities or private companies. A change of purpose of personal data after its collection should not be possible only on the basis of a legitimate interest of the data controller.

Profiling, meaning the assessing data about individuals' preferences, behaviours and attitudes in order to take decisions about them, has become a widespread practice. In order to assure an informed consent to profiling activities, these need to be defined and regulated. Guidance could be taken from the Council of Europe recommendations.[3] As a result of profiling, data subjects may pay higher interest or insurance rates just for matching some criteria and predictive models that are even unclear to them. It is important that for any adverse

[1] For example, "Do Not Track" which is currently being developed in the World Wide Web Consortium (W3C) may become such a standard if the legal framework around it is the right one.
[2] Article 29 Working Party, 11987/04/EN, WP 100: Opinion 10/2004 on More Harmonised Information Provisions, 25 November 2004.
[3] Council of Europe, Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, 23 November 2010.

consequences of profiling, there always needs to be a human check.

The territorial scope of the Regulation is an important issue for the consistent application of EU data protection law. The rapporteur and shadow rapporteurs support the applicability of the foreseen regulation whenever data about EU citizens and residents is processed, no matter where the controller is established. For further transfers to third countries, the criteria for an adequacy decision may need to be strengthened. For transfers not based on an adequacy decision there is the question of how to enforce private agreements such as contract clauses and binding corporate rules (BCRs) in countries that lack data protection laws or with a legal system preventing this enforcement. Access requests by public authorities or courts in third countries to personal data stored and processed in the EU should only be granted if they also have a legal basis in EU law.[1] This will become even more important with the growth of cloud computing.

3. Strengthening individual rights and consumer trust

Specific rights for the individual vis-à-vis the data controller have always been a basis of data protection. These are to be guaranteed, but also strengthened and clarified in order to match the challenges of the digital age and provide legal certainty for consumers and businesses. On the other hand, the proposed regulation can be simplified by merging those rights that are very similar being two sides of the same coin. This will reduce administrative burdens for data controllers and make it easier for individuals to understand and exercise their rights.

Information provided to data subjects can basically be identical to internal documentation if a layered privacy notice approach is followed, where the consumer is first shown a standardised or stylised summary of the privacy policy and can get the full documentation on request. The right to receive intelligible information about the logic involved in data processing, which already exists in Directive 95/46 and was emphasised in Parliament's resolution of 6 July 2011 should be maintained. Data subjects need to be able to understand what happens with their data, while detailed trade secrets should to be protected.

The right to data portability - being able to move one's data from one platform to another - is merely an adequate form of the long established right to data access. In the digital age, citizens, also in their role as consumers, can legitimately expect to receive their personal information in a commonly used electronic format. This enables more competition in an area where natural monopolies based on network effects occur regularly, introducing a market-driven incentive to provide data protection-compliant services.

The right to erasure and the right to rectification remain important for data subjects, as more and more information are disclosed which can have significant impacts. The right to be forgotten should be seen in this light, as it clarifies these rights for the digital environment, while maintaining the general exception for freedom of expression. This should be specified in the wording.

The right to object to further data processing should always be free of charge. There also need

[1] There is strong concern across political groups about access of foreign authorities to European banking, medical and communications data, c.f. the oral questions and related debate with Vice-President and Commissioner for Justice Viviane Reding, 15 February 2012, CRE 15/02/2012 – 19.

to be better possibilities for effective redress, including by consumer groups.

4. Strengthening accountability and reducing administrative burdens

The processing of personal data offers many business opportunities to data controllers and processors. However, since personal data protection is a fundamental right, this processing also entails responsibilities. These obligations should be clear and understandable to avoid legal uncertainty for companies and authorities, as well as for the data subjects. Therefore, a much clearer division of duties and responsibilities between data controllers and data processors is needed. More debate is needed on the concept of "joint controllers". Furthermore, we need a clarification on the limits of what a processor can do without being instructed by the controller, including when a processor enlists a sub-contractor for processing.

Data Protection Officers in companies and public authorities are an important element of modern data protection practice, and their mandatory introduction across the Union as well as the proposals on their position and tasks are generally supported. Some clarifications may be necessary on details about their independence, powers and duties. There is a broad agreement that the threshold for the mandatory designation of a data protection officer should not only be based on the size of the enterprise, but mainly on the relevance of data processing. An appropriate measurement may be the number of individuals whose data is processed.

Data breach notifications and data security provisions need to be aligned with the e-Privacy Directive[1] and the upcoming Directive on attacks against information systems.

Data protection by design and by default is applauded as the core innovation of the reform. This would ensure that, for example, a smart phone app only accesses the data on the phone that is really necessary for the provision of a specific service such as routing or weather information. However, manufacturers and service providers need much clearer guidance and stronger incentives to implement these principles. Privacy Impact Assessments also need clarification and clearer guidelines. Both approaches also require a strong role for data protection officers.

Codes of conduct as well as certification and seals are generally supported, but also need incentives and clearer rules on the consequences with regard to lawfulness of data processing, liabilities, and related issues.

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201, 31/07/2002 P. 0037 – 0047.