EUROPEAN PARLIAMENT 2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

06.07.2012

WORKING DOCUMENT

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)

on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Jan Philipp Albrecht, Dimitrios Droutsas

1. The data protection reform - a strong reflection of the European Parliament's recommendations - a shared agenda

The reform of the data protection regime put forward by the European Commission in January 2012 is welcomed as it incorporates to a great extent Parliament's recommendations as formulated in its Resolution of 6 July 2011 on a comprehensive approach on personal data protection in the EU[1] as regards its four main headings: fully engaging with a comprehensive approach (1a), strengthening individuals' rights (1b), further advancing the internal market dimension and ensuring better enforcement of data protection rules (1c) and, finally, strengthening the global dimension (1d).

1a. The choice of a Regulation for the general framework on data protection in the EU replacing Directive 95/46/EC meets Parliament's request for "full harmonisation at the highest level providing legal certainty and a uniform high level standard of protection of individuals in all circumstances". At the same time the strong call that processing of personal data by institutions and bodies of the European Union, which is governed by Regulation (EC) No 45/2001, should be included within the scope of the new framework has not been mirrored in the draft General Data Protection Regulation (GDPR).

The political choice has been made by Commission that the legal framework of processing for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities is done by means of a Directive. The coverage of law enforcement data processing within Member States, a longstanding claim of the Parliament, is a welcome step in the area, but the Rapporteurs think that the level of ambition of the Directive should have been higher given the high sensitivity of the topic. This is particularly relevant considering that the Parliament has clearly underlined that "sector-specific rules should in no circumstances lower the level of protection provided by the framework legislation, but should strictly define exceptional, necessary, legitimate, narrowly tailored derogations to general data protection principles."

1b. The Rapporteurs consider that many important clarifications and improvements have been put forward in the current texts as regards principles and rights of the data subject. This is the case for the provisions on consent, especially its explicit character, the rules on transparency, detailed rules on information to data subject, the right to erasure and to be forgotten, and data portability, as well as those on sensitive data and data concerning children.

1c. Parliament’s calls for data protection officers, privacy impact assessments, for a general data breach notification, for a strong role and powers and adequate resources of data protection authorities, for the status of the Article 29 Working Party, for severe and dissuasive sanctions have also been reflected in the reform.

1d. The provisions for international data transfers, with respect to which the EP has requested a streamlining and strengthening effort, now explicitly include established practices such as binding corporate rules or standard contract clauses, and the clarification of the adequacy rating procedure is welcomed. The provisions on data transfers in the context of law enforcement cooperation have to be seen also in the context of on-going negotiations with

[1] P7_TA-PROV(2011)0323.

third countries, for example, the EU-US Data Protection Framework Agreement, on which the Parliament has also expressed its views several times.

2. Main elements of the reform

The main elements of the reform are the following:[1]

- data protection as a fundamental right as enshrined in Article 8 of the Charter and Article 16 TFEU, and in that regard improving the ability of individuals to control their data (freely given, informed and explicit consent, right to rectification, to erasure and to be forgotten, right to information and access to own data, data portability, the right to object);

- maintaining the principle of covering all kinds of situations and all kinds of sectors (except national security, common foreign and security policy, and exclusively non-gainful personal activity) with the same or a similar set of rules, whereby the same principles and mechanisms apply to the public and private sector, with necessary and proportionate limitations for the area of law enforcement;

- adapting data protection rules to the new technological progress in a technically neutral way (for example: privacy by design and privacy by default);

- providing effecting means for safeguarding the fundamental right to data protection (purpose limitation, responsibilities of the controller, notification and communication of data breaches, strong and independent national data protection authorities, data protection officers at all public authorities, in companies above a specific size, or in special situations, effective administrative and judicial remedies);

- preventing fragmentation and providing legal certainty for individuals, enterprises (as regards the single market) and public entities through the introduction of the so-called "one stop shop" system (competence of the data protection authority of the main establishment of the controller or processor), and the "consistency mechanism";

- providing harmonisation on basic data protection principles as regards the handling and exchange of data by police and judicial authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (data protection aspects being an essential part of existing and proposed EU legislation in that regard), thereby also ending the current situation where EU rules (Framework Decision 2008/977/JHA) applied only if a cross-border element was present;

- providing a safe and sound system of data transfers to third countries (either on an adequacy decision for a country, territory or processing sector - based, *inter alia*, on rights for effective administrative and judicial redress for data subjects residing in the Union - or on specific appropriate safeguards in legally binding instruments) and to promote the EU system abroad (including agreements with third countries).

[1] See also Commission Communication on Safeguarding Privacy in a Connected World, a European Data Protection Framework for the 21st Century (COM(2012)0009).

3. The package approach

The Rapporteurs consider that the two reform proposals give a unique legislative opportunity to develop two fully coherent, harmonious and high standard legal instruments as regards data protection by adopting a comprehensive, balanced, coordinated and parallel procedure for both texts. The "package approach" is consistent with EP's recurrent requests over the years for a strong and ambitious data protection framework which does away with fragmentation and legal uncertainty. Such an approach will specifically

- guarantee that coordinated legislative approaches will be taken, which will improve the substance and consistency of both files. In practical terms, each Rapporteur on the package is at the same time shadow Rapporteur in the other file. Coordination is also ensured by means of joint technical meetings, Committee debates and hearings (see below); similar calendars for the two procedures are currently being developed.

- accomplish the most efficient and comprehensive procedure from a legislative perspective as meetings and debates have been and will be combined, guaranteeing time efficiency and minimisation of use of resources while ensuring thorough work;

- guarantee that the same level of data protection will be applied at the same time in all fields of EU activities, thereby finishing with the existing anomalies of the pre-Lisbon time and guaranteeing an optimal control of the Court of Justice in all the fields.

4. Steps taken and the way forward

4a. Extensive discussions have already taken place on the data protection reform with shadow Rapporteurs, opinion committee Rapporteurs, Council Presidency and Commission. They will continue to do so, and will also work with stakeholders such as data protection authorities, national authorities, industry, civil rights and consumer organisations in order to ensure broad support for the Parliament's approach. On the regulation, LIBE has held a stakeholder workshop on 29 May 2012; a similar event will be considered also for the directive.

As agreed by LIBE coordinators, the LIBE committee will hold the annual inter-parliamentary committee meeting (IPCM) together with national parliaments in the area of freedom, security and justice on the data protection reform package on 9 and 10 October 2012. Further specific working documents on the regulation and the directive will be presented later this year. There is also discussion about an impact assessment from Parliament's side.

The presentation of draft reports is currently planned before the end of 2012. Your Rapporteurs hope to be ready for and start negotiations with the co-legislator in the course of 2013.

4b. Areas where a need for further debate and clarification has been identified by the Rapporteurs and shadow Rapporteurs include, but are not limited to:

- the role of the Commission through delegated and implementing acts and in the

consistency mechanism;

- the current exclusion of data protection rules for EU institutions and agencies from the reform;

- the relation between general Union law and national specific laws;

- the exact division of roles and responsibilities among data protection authorities in cross-border cases;

- clarifications on profiling, including a human element and a right to information about the logic involved in data processing, as demanded by Parliament;

- the notions of "legitimate interest", "public interest" and "public security";

- the inter-linkage of both legislative instruments, especially in cases of law enforcement access to personal data held by private entities;

- access requests or access orders for personal data stored in the Union by public authorities in third countries, especially for cases where the data controller also has an establishment there;

- stronger incentives for data protection by design and by default.