EUROPEAN COMMISSION

Brussels 17.9.2013
C(2013) 5903 *final*

Mr Valeriu Ştefan ZGONEA
President of the
Camera Deputaţilor
Palace of the Parliament
Str. Izvor nr. 2-4, sector 5
RO – 050563 BUCHAREST

Dear President,

The Commission would like to thank the Camera Deputaţilor for its Opinion concerning the proposals for a General Data Protection Regulation[1] and for a Data Protection Directive for police and criminal justice authorities {COM(2012) 11 final}, {COM (2012) 10 final}, {COM(2012) 9 final}, and apologises for the long delay in replying.

The Commission is pleased to see the interest and the special consideration that the Camera Deputaţilor has devoted to the data protection package and it welcomes the precise comments and suggestions you have put forward.

The Commission would like to underline that the data protection reform package proposed by the Commission last January aims to build a modern, strong, consistent and comprehensive data protection framework for the European Union. It would benefit individuals by strengthening their fundamental rights and freedoms with respect to processing of personal data and their trust in the digital environment and simplify the legal environment for businesses and the public sector substantially. This is expected to stimulate the development of the digital economy across the EU's Single Market and beyond, in line with the objectives of the Europe 2020 Strategy and the Digital Agenda for Europe.

[1] "Proposal for a Regulation of the European Parliament and of the Council 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)", COM (2012) 11 final ('Regulation').

Finally, the reform would enhance trust among law enforcement authorities in order to facilitate exchanges of data between them and cooperation in the fight against serious crime, while ensuring a high level of protection for individuals.

The package also responds to strong calls from the co-legislators, the Council[2] and the European Parliament[3], as well as from various stakeholders for a legal framework incorporating high standards and based on a comprehensive approach.

Notwithstanding the further assessment of the related issues in the course of the legislative procedures, the Commission would like to explain to you its position on the main issues raised in the Camera Deputaților's Opinion:

I. On the proposal for a Directive:

In relation to the proposed Directive for police and criminal justice authorities, which would replace Framework Decision 2008/977/JHA[4], the Commission has proposed as scope for application not only the coverage of cross-border data processing but also of processing activities by the police and judicial cooperation at national level.

First of all, the Commission would like to point out that neither Article 8 of the EU Charter of Fundamental Rights nor Article 16 Treaty on the Functioning of the European Union (TFEU), as introduced by the Lisbon Treaty, make a distinction between domestic and cross-border data processing operations, but refer to the possibility of adopting rules relating to the processing of personal data, and their free movement, in all areas falling within the scope of EU law. The Commission believes that Article 16 TFEU allows the Union legislator to adopt EU rules on the processing of personal data by police and judicial authorities in the criminal area regardless of whether such processing takes place purely at national level or has a cross-border element.

Moreover, the assessment carried out by the Commission in relation to the Framework Decision[5] has shown that the 'domestic vs. cross-border data' differentiation is an artificial distinction and – as confirmed by some Member States during the Commission's consultations – may also create practical problems for law enforcement authorities: it is difficult for a police officer to distinguish between data of different 'origins' during an investigation and to apply different rules to such personal data. In addition, it is not always foreseeable in advance that personal data collected by one Member State will then be subject to cross-border exchange. Therefore, common rules covering both 'domestic' data processing and

---

[2] Council Conclusions on the Communication from the Commission to the European Parliament and the Council - A comprehensive approach on personal data protection in the European Union, 3071st Justice and Home Affairs Council meeting, Brussels, 24 and 25 February 2011.

[3] European Parliament Resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union P7_TA_(2011)0323.

[4] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350/2008, p. 60 ('Framework Decision').

[5] See the Impact Assessment accompanying the data protection reform package (SEC(2012)72 final) as well as the Implementation Report concerning the Framework Decision (COM(2012)12).

cross-border transmissions between Member States are a precondition for the effective exchange of personal data and will enhance law enforcement cooperation in the EU.

As regards a precise definition for the concept of "national security", no definition of "national security" is provided for by the treaties or by any other instrument of EU law, though several references are made to it in the treaties. Article 4 of the Treaty on European Union (TEU) lays down that the European Union shall act within the limits of competences conferred by the Treaties by the Member States. Article 4 (2) TEU states that "national security remains the sole responsibility of each Member State". Likewise, Articles 72 and 73 TFEU refer to internal and national security as a competence of the Member States.

As regards data protection supervisory authorities (DPAs), both Article 8 of the Charter and Article 16 (2) TFEU require independent authorities to check that the rules for the processing of personal data are complied with. The role of these completely independent data protection supervisory authorities is essential for the enforcement of the rules on personal data protection. They are guardians of fundamental rights and freedoms with respect to the protection of personal data, upon which individuals rely to ensure the protection of their personal data and the lawfulness of processing operations.

However, the Commission has found that the status of independence, the resources and the powers of these national supervisory authorities vary considerably among Member States. Therefore, both the proposed Regulation and Directive would further enhance the independence of national data protection supervisory authorities implementing the requirements by the Court of Justice of the European Union (CJEU) by clarifying in more detail the necessary conditions for the establishment and for ensuring complete independence of supervisory authorities in Member States. They take inspiration from the relevant provisions in Regulation (EC) No 45/2001[6] while at the same time taking into account the constitutional traditions of the Member States as regards appointment of data protection authorities (i.e., by Parliament or the government).[7] As regards the provision of Article 39 of the proposed Directive according to which "Each Member State shall provide that one or more public authorities are responsible for monitoring the application of the provisions adopted pursuant to [the] Directive" this is in keeping with the logic of Article 25(1) of Framework Decision 2008/977/JHA and of Directive 95/46/EC.

II. On the proposal for a General Data Protection Regulation:

As regards your views on the DPAs and their appointment, the comments made above on the proposed Directive are entirely valid for the proposed Regulation. On the issue of financial control Article 47 of the proposal prescribes that "Member States shall ensure that the supervisory authority is subject to financial control which shall not affect its independence. Member States shall ensure that the supervisory authority has separate annual budgets. The budgets shall be made public." This must be understood in the general context whereby DPAs

---

[6] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data OJ L 8/2000, p.1.

[7] See also in this sense case *Commission v Germany*, C -518/07, paragraph 44.

must be free from political influence in the exercising their duties and powers and be – also in terms of resources and infrastructure – in a position to ensure effectively the protection of personal data – in their own country as well as in the cooperation with supervisory authorities in other Member States and within the consistency mechanism.

As regards the role of the Commission in the consistency mechanism several aspects must be underlined. The new consistency mechanism is intended to help streamlining the work between data protection authorities. The consistency mechanism would ensure a harmonised approach to any issue of European relevance, be it individual cases or general data protection issues. By helping each other, data protection authorities would reinforce their power of intervention. The consistency mechanism would also strengthen the data protection authorities' independence from and position towards national governments. Peer pressure on Member States would be much stronger than now, and problems of understaffing or lack of resources would be more visible.

The Commission's role in the consistency mechanism is clear: a possible intervention is a measure of last resort. The Commission is there as a backstop. Its power to suspend a decision of a data protection authority would be limited to cases where conformity with EU law is doubtful, or where there is a risk of an inconsistent application of our data protection rules. The Commission has no intention of becoming a "super-data protection authority". The deliberation and determination of individual cases is for the data protection authorities, not for the Commission.

With respect to delegated acts, Article 290 TFEU allows the European legislator to delegate to the Commission the power to adopt non-legislative acts of general application to supplement or amend certain non-essential elements of a legislative act (quasi-legislative acts). The proposed Regulation has been deliberately drafted as a technologically neutral legal instrument. It is designed to be open to the future and does not to try to anticipate all technological developments of the next 20 years, but should be broad enough for technological innovation and changing consumer practices. Delegated acts are the instruments foreseen by the Lisbon Treaty to allow for the rules and principles of the Regulation to be adapted to future developments without always leading to a full-fledged reform of the legislative text.

Furthermore, legal acts adopted by the European Commission in this way are subject to the ex-post control of the legislator. Delegated acts can only enter into force if no objection has been expressed by the European Parliament or the Council – in effect, the two legislators have a veto power. In addition, the legislator can reserve the right to revoke the European Commission's delegated powers at a later stage. At the same time the Commission is open to re-examine on a case-by-case basis the empowerments foreseen in the proposed Regulation.

On the issue that the tasks of the data protection officer (DPO) must be laid down by means of a Regulation this is currently the case as the proposed Regulation enshrines the tasks of the DPO in Article 37.

As regards the right to be forgotten this is the prolongation of the right to erasure and as designed in the proposal has strict limits. It does not provide for a "general deletion clause"

but allows erasure when data is no longer needed for other legitimate purposes. It is thus an obligation of means and not of result. Moreover, the definition of "reasonable steps" would depend on the specific situation. There is no 'one size fits all', nor indeed is the right to be forgotten confined to technical solutions. Sometimes, a simple e-mail to a third party website will be enough. Moreover, the Regulation provides for very broad exemptions in order to ensure that freedom of expression can be fully taken into account. This would allow for instance news websites to continue to operate on the basis of the same principles. The new provisions are clear: freedoms of expression, historical and scientific research are safeguarded. Notwithstanding further clarifications can be sought by the co-legislators in order to ensure maximum legal certainty. The same applies for the right to data portability which is a development of the right of access. The Commission will support the co-legislators in these efforts of clarification and fine-tuning of the text.

As regards Article 42 (Transfer by way of appropriate safeguards), for transfers to third countries appropriate safeguards must have been provided, in particular, by standard data protection clauses, binding corporate rules and contractual clauses. The possibility of making use of Commission standard data protection clauses is based on Article 26(4) of Directive 95/46/EC. As a new component, such standard data protection clauses could now also be adopted by a supervisory authority and be declared generally valid by the Commission. Binding corporate rules are now specifically mentioned in the proposed legal text. The option of contractual clauses gives certain flexibility to the controller or processor, but is subject to prior authorisation by supervisory authorities.

The Commission hopes that these explanations clarify the issues raised by the Camera Deputaților and looks forward to continuing our political dialogue in the future.

Yours faithfully,

[ ]
Vice-President/Member of the Commission