EUROPEAN COMMISSION

Brussels, 18.3.2013
C(2013) 1430 *final*

Mr Milan ŠTĚCH
President of the Senát
Valdštejnské naměstí 17/4
CZ – 118 01 PRAHA 1

Dear President,

The Commission would like to thank the Czech Senate for its Opinion, concerning the European Commission's proposals for a General Data Protection Regulation[1] *and for a Data Protection Directive for police and criminal justice authorities*[2] *and apologises for the long delay in replying.*

We are pleased to note that the Czech Senate supports the need for reforming the current EU data protection framework, in particular to adapt it to rapid technological developments, while expressing concerns about the proposed Directive and requesting further clarifications as to the reasons for replacing the current Directive 95/46/EC by a Regulation.

I 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.

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.

---

[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').

[2] "Proposal for a Directive 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", COM (2012) 10 final ('Directive').

The package also responds to strong calls from the co-legislators, the Council[3] and the European Parliament[4] as well as from various stakeholders for a legal framework based on high standards and a comprehensive approach.

In relation to the proposed Directive for police and criminal justice authorities - which will replace Framework Decision 2008/977/JHA[5], whose scope is limited to cross-border data processing - the Czech Senate argues that such proposal would be in breach of the principle of subsidiarity to the extent that its scope covers also processing at national level (or 'domestic' processing).

First of all, the Commission would like to point out that neither Article 8 of the EU Charter of Fundamental Rights nor Article 16 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 Articles 16 TFEU allows the Union legislator to adopt EU rules on the processing of personal data by police and judicial authorities in the criminal areas 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[6] 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 cross-border transmissions between Member States are a precondition for the effective exchange of personal data and would enhance law enforcement cooperation in the EU.

In the light of the above, the Commission considers that the Union is fully competent to regulate data processing activities by law enforcement authorities carried out at domestic level and that the objective of ensuring a smooth exchange of information between such authorities in Member States can only be effectively achieved if common rules are established at EU level to regulate such processing.

As regards the proposed Regulation, the Commission considers that this was the most appropriate way of ensuring a more harmonised and uniform application of the common rules in this area, to the benefit of individuals and EU businesses. Nowadays, despite the aim of the current Directive to ensure a consistent and equivalent level of data protection

---

[3] 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.

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

[5] 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').

[6] 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).

in Member States, the fragmentation of the legal data protection framework - due to the different data protection standards and requirements in Member States - has led to unnecessary financial and administrative burdens for data controllers, which affect the competitiveness of European companies. This is also a problem for individuals, as they have different levels of protection of their personal data depending on the Member States in which they are. This is not acceptable when we are talking of a fundamental right, enshrined in the EU Charter of Fundamental Rights and in the Treaty.

The direct applicability of a Regulation would reduce legal fragmentation and provide greater legal certainty by introducing a harmonised set of rules, improving the protection of fundamental rights and contributing to growth and to the effective functioning of the internal market. In addition, the proposed Regulation provides for several measures aiming to the simplification of the current legal framework; one of the most significant is the so-called "one-stop-shop", by virtue of which businesses with processing activities in several Member States would also have one single supervisory authority to deal with. The Regulation also proposes to set up a "consistency mechanism" to ensure a very strong cooperation and mutual assistance between supervisory authorities and, eventually, guarantee a consistent application and enforcement of EU data protection rules.

The Commission hopes that these explanations clarify the issues on the proposals for new legal data protection instruments raised in your observations and questions and looks forward to continuing our dialogue in the future.

Yours faithfully,

Maroš Šefčovič
Vice-President