EUROPEAN COMMISSION

Brussels, 14. 12. 2012
C(2012) 9642 *final*

Ms. Ene ERGMA
Riigikogu Esimees
Lossi Plats 1A
EE-15 165 – TALLINN

Dear President,

The Commission would like to thank you for the Opinion of the Riigikogu concerning the European Commission's proposals for a General Data Protection Regulation {COM(2012) 11 final} and a Data Protection Directive for police and criminal justice authorities{COM(2012) 10 final}, and apologizes for the delay in replying.

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.

The package also responds to strong calls from the co-legislators, the Council[1] *and the European Parliament*[2] *as well as from various stakeholders for a high quality legal framework based on a comprehensive approach.*

As regards the Riigikogu's detailed comments and questions, the Commission would like to provide clarifications in the annex to this letter.

---

1 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.

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

The Commission is convinced that a comprehensive and effective system for the protection of personal data is needed in the European Union and that this can be better achieved at European Union level.

The Commission hopes that its reply clarifies the issues on the proposals for new legal data protection instruments raised in your Opinion and looks forward to continuing the political dialogue with the Riigikogu in the future.

Yours faithfully,

Maroš Šefčovič
Vice-President

ANNEX : COMMISSION POSITION ON THE OPINION OF THE RIIGIKOGU ON COM(2012) 10 - 11 FINAL

1) As far as the choice of legal instrument is concerned, Article 16 (2) of the Treaty on the Functioning of the European Union (TFEU) mandates the European legislators to adopt 'the rules relating to the protection of individuals with regard to the processing of personal data', without, however, specifying the type of legislative act to be chosen. Although the objective of Directive 95/46/EC[3] was to ensure an equivalent level of data protection within the EU, there is still considerable divergence in the data protection rules across Member States. As a consequence, data controllers may have to deal with 27 different national data protection laws and requirements within the EU. The result is a fragmented legal environment which has created legal uncertainty and unequal protection for data subjects. This has caused unnecessary costs and administrative burdens for controllers, in particular for cross-border operating businesses. This inconsistent level of protection across the EU constitutes a disincentive for enterprises and affects the competitiveness of European companies. At the same time, the fundamental right to the protection of personal data requires the same level of data protection for individuals throughout the Union. Additional common EU rules are therefore necessary to avoid the risk of different level of protection in the Member States.

In order to build on the existing standards of Directive 95/46/EC and to remedy its shortcomings, the European Commission considers a Regulation to be the most appropriate legal instrument to define the general framework for the protection of personal data in the Union: the direct applicability of a Regulation in accordance with Article 288 TFEU would reduce legal fragmentation, provide greater legal certainty, improve the protection of individuals and contribute to the free flow of personal data within the Union. This would also contribute to growth and the functioning of the internal market. Estonia is a Member State where a lot of companies have intra EU operations, for instance with Finland or Germany. These would greatly benefit from the proposal.

A case has also been made about the possible over-prescriptive character of the proposed Regulation. The Commission does not consider this to be the case. The Commission has, for example, reduced many ex-ante formalities – such as notifications or prior authorisations to international transfers – and thus reduced red tape. Moreover, there is no "one-size-fits-all" approach: the specific situation of SMEs has been duly taken into account in the Commission's reform proposals, and particular attention has been paid to avoiding undue administrative burden: -SMEs are exempted from several obligations (e.g. documentation, Data Protection Officers (DPOs) and Data Protection Impact Assessments (DPIAs) as a general rule), and the "think small principle" is enshrined in several provisions. And SMEs would also fully benefit from the simplification of the regulatory environment brought about by the proposed Regulation and the "one-stop-shop". I believe that the elimination of the existing barriers within the internal market - in terms of costs and administrative burden created by the current, fragmented legal environment – would be highly beneficial to SMEs as it would constitute an incentive to cross-border expansion.

---

[3] *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 [1995] OJ L 281/31.*

On the reconciliation of the fundamental right to the protection of personal data with other fundamental rights and freedoms, such as freedom of expression and key values such as transparency of government activity on which the Commission is aware that there are specific concerns in Estonia, let me point out that the reform package, and particularly the proposed Regulation, fully takes into account this essential aspect. Given that these are areas where national cultural traditions are very different – and different models exist in Member States' national laws on this – it has not been considered appropriate to provide for a full harmonisation at EU level on how to achieve this "reconciliation". The data protection package therefore does not change the current situation: the national legislator would continue to have the possibility to legislate and balance the importance of the right to freedom of expression in every democratic society as well as the public interest of having a transparent government and administration with every data subject's legitimate interests or fundamental rights and freedoms, including the right to data protection.

The Commission firmly believes that the right to privacy reinforces the freedom of expression in the internet. The internet allows citizens to express their opinions and exchange views freely on any topic at any time. This explains the phenomenal success of social networking websites. But citizens will only continue to engage in this way if they are confident that the ideas, likes and dislikes they share will not be misused by the platforms they use. In the long term, this can only be guaranteed by a solid, reliable privacy framework.

Moreover, the provisions on the right to be forgotten that the Commission has proposed are little more than a codification of the existing principles, enshrined in the data protection Directive since 1995. Indeed, the Directive, which has been in force for 17 years, states that data stored needs to be 'up to date' and 'accurate'. The right to be forgotten builds on this basis – it is a reformulation of the principle. But the reformulation is important because it empowers citizens, allowing them to take control of their data. The Commission trusts that the Riigikogu can also support this objective.

Article 80 of the proposed Regulation specifically obliges Member States to provide for exemptions or derogations from data protection rules in order to reconcile the right to data protection with the rules on the freedom of expression. On the question of public access to documents, a specific recital has been included in the proposed Regulation – like in the current Directive 95/46/EC – to specify that "[the] Regulation allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Regulation" (recital n° 18).

2) With respect to delegated acts, Article 290 TFEU allows the European legislator to delegate to the European Commission the power to adopt non-legislative acts of general application to supplement or amend certain non-essential elements of a legislative act. 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 try to anticipate all technological developments of the next 20 years, but should be flexible enough for technological innovation and changing consumer practices. Delegated acts are the instruments foreseen by the Lisbon Treaty to allow the non essential elements of the proposed Regulation to be updated to take account of technological developments without triggering 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[4]. 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.

3) The proposed new Data Protection laws, in particular the proposal for a Regulation provide only for a limited number of specific cases where the Commission should be conferred delegated powers, in line with the Treaty provisions. However, neither of these entails adoption of essential elements. Anything which is an essential element is to be found in the Regulation proposal.

4) The "one-stop-shop" for businesses means that data controllers, even when acting in several Member States, would only have to deal with a single Data Protection Authority (DPA), namely that of the Member State where the company's main establishment is located. This is an important simplification and is very much welcomed by the business world. The strengthened cooperation and mutual assistance between DPAs and the proposed "consistency mechanism" would ensure that DPAs apply the Regulation in a consistent manner throughout the Union. Decisions which have an impact also on data subjects in other Member States should be subject to consultation with the other DPAs in the new "European Data Protection Board" (a strengthened Article 29 Working Party), with the possibility of Commission's intervention only as a very last resort. Moreover, individuals keep the right to address themselves to their DPA of residence, which would have to coordinate and cooperate with the competent DPA, using the means and the mechanism described above.

5) As you know, both Article 8 of the Charter of Fundamental Rights 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 European Commission has found that the status of independence, the resources and the powers of these national supervisory authorities vary considerably among Member States.[5] In some cases, they are unable to perform their enforcement tasks in a satisfactory way. Cooperation among these authorities at European level – especially via the existing Advisory Group (the so-called Article 29 Working Party)[6] –

---

[4] *See Communication from the Commission to the European Parliament and the Council – "Implementation of Article 290 of the Treaty on the Functioning of the European Union", COM (2009) 673 final.*

[5] *For more details on this aspect, see the Impact Assessment accompanying the legal proposals, SEC (2012) 72.*

[6] *The 'Article 29 Working Party' was set up in 1996 (by Article 29 of Directive 95/46/EC) with advisory status to the EU Commission and is composed of representatives of national Data Protection Supervisory Authorities, the European Data Protection Supervisor and the Commission. See http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.*

has not always led to consistent enforcement in the past. As a consequence, the proposed Regulation further enhances the independence and powers of national data protection supervisory authorities to enable them to carry out investigations, take binding decisions and impose effective and dissuasive sanctions. In particular, the proposal implements the requirements by the Court of Justice of the European Union[7] by clarifying in more detail the necessary conditions for the establishment and for ensuring complete independence of supervisory authorities in Member States, taking inspiration from the relevant provisions in Regulation (EC) No 45/2001[8].

6) On the question of administrative sanctions, the Regulation proposal defines the maximum amounts to be used in the most serious cases, taking into consideration that these must be appropriate and dissuasive. Infringements of data protection rules can bring huge profits; there must be a correlation between the benefits derived from breaking the rules and the amount of the sanctions. The principle is the same as applied when calculating sanctions in other legal areas, but the actual fines would depend on the severity of the individual cases and on other circumstances (e.g., the intentional or negligent character of the infringement, the degree of cooperation of the data controller with the DPA) and would not often reach the maximum. In some cases, there may even be only a warning and no sanction at all.

7) As to the proposed Directive for police and criminal justice authorities, the entry into force of the Lisbon Treaty, and Article 16 TFEU as the new legal basis for EU data protection legislation, call for the establishment of a comprehensive data protection framework which covers also the processing by police and judicial criminal authorities. As regards criminal investigations and proceedings, there is a specific provision on personal data contained in a judicial decision or record (Article 17), which allows Member States to provide that in such cases data subjects' rights are implemented in accordance with national rules on judicial proceedings. The differentiation between categories of data subjects, or the obligation to distinguish between data according to their reliability, is something which is already implemented in practice in several Member States and should therefore not be problematic. For example, personal data on suspects or convicted persons should be subject to different rules than data on victims or witnesses.

---

7 *CJEU C-518/07 Commission v Germany [2010] ECR I-01885.*

8 *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, [2001] OJ L 008/1.*