Eerste Kamer der Staten-Generaal

European Commission
Mr M. Šefcovic

Binnenhof 22
postbus 20017
2500 EA Den Haag

telefoon 070-312 92 00
fax 070-312 93 90

e-mail postbus@eerstekamer.nl
Internet www.eerstekamer.nl

Date *15 May 2012*
Re *European Personal Data Protection Proposals COM(2012)10 and 11*

Courtesy translation

Dear Mr Šefcovic,

The standing committees for Immigration & Asylum / Justice and Home Affairs (JHA) Council and for Security and Justice of the Senate of the States General have taken note with interest of the proposal of the European Commission for a General Data Protection Regulation[1] and of the 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.[2] The committees would like to put some questions to you and make some observations about these two proposals.

Questions about the General Data Protection Regulation

1. The committees take a positive view of the introduction of an obligation to carry out an assessment of the impact of envisaged processing operations on the protection of personal data, as set out in the draft Article 33. However, it strikes them as strange that public authorities or bodies are exempted from this obligation in certain cases. The committees consider that it would, on the contrary, be desirable for these authorities too to carry out data protection impact assessments in advance. The committees therefore request the European Commission to drop this exemption.

2. It is noteworthy that under Article 35 public authorities or bodies are obliged to designate a data protection officer. The committees can well imagine that this is necessary as it is the role of these authorities and bodies to set an example. However, they wonder what the European Commission envisages will be the precise nature of this role. Article 35 (6) provides that the controller or processor should ensure that any other professional duties of the data protection officer are compatible with that person's tasks and duties as data protection officer and do not result in a conflict of interests. Is this not primarily a responsibility of the data protection officer himself? And how does this relate to the provisions of the draft Article 36 (3)? Here it is pro-

[1] COM(2012)11.
[2] COM(2012)10.

posed that the data protection officer should have staff, premises, equipment and any other resources necessary to carry out his duties and tasks properly. This gives the impression that it is more than a full-time post. In other words, how do these provisions relate to one another? And what criteria should be applied when determining whether an organisation is a public authority or body? Do these terms also include private institutions that have a public function, semi-public bodies and autonomous administrative authorities?

3. The existing duty of notification is abolished under this proposal and the duty to provide information is greatly expanded in the draft Article 14, as are the rights of access, rectification and erasure. The controller must now inform the data subject not only of the purpose of the processing and of his own identity but also of such matters as the identity of the controller's representative and of the data protection officer, the period for which the personal data will be stored, the existence of the right to request access to and rectification or erasure of the personal data, the right to lodge a complaint to the supervisory authority (in the Netherlands the Dutch Data Protection Authority / CPB), the recipients or categories of recipients of the personal data, where applicable any intention on the part of the controller to transfer the personal data to a third country or international organisation and the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission and any further information necessary to guarantee a fair process in respect of the data subject. On the face of it, it seems a good thing that the duty of notification is to be abolished since this would greatly reduce bureaucracy. However, in view of the expansion of the duty to provide information and the increase in the rights of the data subject the controller will have to keep records of almost exactly the same data. The only difference is that instead of having to record them in a notification form to be sent to the national supervisory authority, the controller will in future have to notify them directly to the data subjects in a detailed letter. What is the European Commission's view on this? Was this indeed the Commission's intention? And do not these obligations impose an unnecessarily great administrative burden?

4. The duty to maintain documentation as set out in Article 28 does not apply to an enterprise or organisation employing fewer than 250 persons that processes personal data only as an activity ancillary to its main activities. The criterion of 250 persons seems rather arbitrary. The decisive factor should be not the size of the organisation but the purposes of the data processing, the nature and amount of the personal data and the recipients of the personal data. Moreover, complying with the duty to maintain documentation is hardly onerous in view of the obligations of Articles 11 to 15. The committees therefore request the European Commission to drop the exemption contained in Article 28 (4)(b).

5. Under Article 23 controllers are obliged to apply the principles of data protection by design and data protection by default to data processing. Paragraph 2 of this article provides that the controller must implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, in terms of both the amount of the data and the time of their storage. In particular, those mechanisms must ensure that by default personal data are not made accessible to an indefinite number of individuals. This last sentence refers to the establishment of authorisation measures and mechanisms designed to safeguard confidentiality. These mechanisms do not therefore in themselves

ensure that the data processing takes place only where it is necessary for these purposes and that the data are not stored for longer than is strictly necessary for such purposes. It is unclear whether the European Commission also wishes to make the mechanisms compulsory in order to provide a system for enforcing the principles of purpose limitation and proportionality. Is the European Commission able to shed any light on this?

6. Article 24 of the draft Personal Data Protection Directive obliges the Member States to ensure that records are kept of at least the following processing operations: collection, alteration, consultation, disclosure, combination and erasure of personal data. The records of consultation and disclosure should show, in particular, the purpose, date and time of such operations and as far as possible the identity of the person who consulted or disclosed personal data. Why is this provision included in the draft Directive but not in the draft General Data Protection Regulation?

7. Article 51 (2) provides that the supervisory authority of the main establishment of the controller is competent to supervise the processing activities of the controller in all Member States. In practice, however, it is not always clear what establishment constitutes the main establishment. This means that the criteria for deciding which supervisory authority is competent and how decision-making is allocated between the different Member States must be formulated more clearly. For example, it could be provided that if it is not possible to establish where the main establishment is located, the European supervisory authority – i.e. the European Data Protection Board – should have the power to determine which national supervisory authority is to take the lead and how the responsibilities should be divided up with the other national supervisory authorities. What is the European Commission's view on this?

8. The committees take a positive view of the introduction of a duty to notify personal data breaches. A controller must give notice without undue delay and, where feasible, not later than 24 hours after becoming aware of a breach. A processor is obliged to alert and inform the controller immediately after establishing that there has been a personal data breach. Is it correct that this duty of notification goes beyond the obligation to report data leaks and that every breach of technical and organisational measures designed to ensure a suitable protection level must be notified? And is the requirement in Article 31 (3) that the processor should immediately notify the matters referred to in points (a) to (e) feasible in practice? Would it not be more logical for the processor to have a duty to give immediate notice of the breach, but merely to inform the controller as quickly as possible of the other matters?

Questions about the specific Personal Data Protection Directive in criminal matters

1. The draft Personal Data Protection Directive is applicable to all processing activities by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The term 'prevention' of criminal offences is a broad and elastic concept. Could the European Commission indicate how this term should be interpreted?

2. The term 'competent authorities' is defined in Article 3 (14) of the draft Personal Data Protection Directive as 'any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties'. Public authorities compe-

tent for the prevention of criminal offences can constitute an especially broad category. Is the European Commission at least able to give examples of such authorities? Authorities responsible for preventing criminal offences are generally subject to very different competence criteria, and their powers do not generally have a statutory basis. Why is this distinction not reflected in the rights and obligations which competent authorities obtain on the basis of this proposal?

3. How should the relationship between the draft Personal Data Protection Directive in criminal matters and the draft General Data Protection Regulation be viewed? If data are processed by groupings established to combat crime, does the draft Directive or the draft Regulation apply? Where data are processed by groupings the present position in the Netherlands is that such processing is governed by the general Personal Data Protection Act and not by the Police Data Act, which applies only to specific sectors. This is because bodies such as municipalities, which are not covered by the Police Data Act, may participate in these groupings. What will be the position once the General Data Protection Regulation is in force and the Personal Data Protection Directive in relation to criminal matters has been transposed into national legislation and taken effect?

4. Under Article 4 (a) of the draft Personal Data Protection Directive the Member States must provide for personal data to be processed fairly and lawfully. What is meant by 'fairly'?

5. Under Article 4 (f) the Member States must provide for personal data to be processed under the responsibility and liability of the controller. What is the meaning of 'liability' in this connection? The controllers will generally be police and criminal justice authorities. Do not such authorities – as is the case in the Netherlands – enjoy immunity from liability? How, therefore, should the term 'liability' be interpreted in this context?

6. Article 19 is headed 'data protection by design and by default'. It is not clear from the text of Article 19 what is meant by the term 'data protection by default'. Does it mean that the ICT systems used for processing personal data must at all times be designed and configured in such a way that the protection of personal data can be enforced by means of these systems? Could the European Commission clarify and explain this?

7. Finally, the committees request the European Commission to improve coherence between the general Regulation and the specific Directive. This could be done by including general principles and definitions in both proposals and putting them on equal footing. Greater coherence could also be achieved if the same obligations were made applicable to the controller and the processor, for example the obligation to carry out data protection impact assessments and to apply data protection by design.

Reminder

Finally, the committees would like to take the opportunity to point out to the European Commission that two letters sent by the Senate of the States General have not yet been answered by the European Commission and that the 3-month period for reply set by the European Commission itself has already expired. These are the following letters:

- letter of 8 November 2011 concerning the proposal for a Regulation to provide for common rules on the temporary reintroduction of border control at internal borders in exceptional circumstances (COM(2011)560), reference 149443.01u;
- letter of 11 November 2011 concerning the proposal for a Directive on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011)32), reference 147341.06u.

The committees would kindly request you to answer these letters as quickly as possible. They look forward with interest to receiving your reply to this letter.

Yours sincerely,

P.L. Meurs
Chair of the standing committee for Immigration & Asylum / Justice and Home Affairs Council

A. Broekers-Knol
Chair of the standing committee for Security and Justice