Conference on "Security of e-Government"
European Parliament, Brussels, 19 February 2013

"The role of data protection legislation"

Peter Hustinx
European Data Protection Supervisor

As the invitation for this conference rightly states, *"e-Government is at the forefront of current public sector reform policies across the world where the use of information and communication technologies aims to digitize transactions, deliver public service and leverage public sector innovation"*. It also mentions some of the challenges: *"how to ensure a proper security level, and how to safeguard citizen's privacy?"*

This introductory note will focus on the privacy challenges, more particularly in view of current and very likely future data protection legislation. Not in any way intended as a "show stopper", but as a contribution to overcoming some of the challenges and to finding the best way forward.

For this purpose, the note first briefly highlights some of the relevant characteristics of what is commonly referred to as "e-Government" (1), and how security and privacy relate to each other (2). It subsequently looks at some key privacy or data protection[1] challenges (3), and how they are affected by the review of the EU legal framework for data protection (4). This leads to a few main messages and conclusions (5).

1. E-Government

The term "e-Government" covers (much) more than only the - systematic - use of ICT for the delivery of public services. If that would have been the case, the emphasis of this conference would have been on efficiency or economy of scale. Instead, *current public sector reform* covers a number of other dimensions, which are interlinked and may be summarised as follows:

- re-allocation of public tasks: availability of ICT not only allows, but also often requires re-design of public tasks and services, potentially involving different government departments, different government levels and inclusion of private actors in different roles (in front or back office);

[1] Privacy and data protection are closely related, but different legal concepts, which in EU law are both recognised as fundamental rights, mentioned separately in the Charter of Fundamental Rights: the right to respect for private and family life (Article 7) and the right to the protection of personal data (Article 8). The latter is also mentioned in Article 16 of the Treaty on the Functioning of the European Union together with a general legal basis for adoption of rules on data protection, both for the EU institutions and bodies, and for the Member States, when they are acting within the scope of Union law. Article 16 TFEU is the main basis for the current review of the EU legal framework for data protection.

- common infrastructure: re-design of public tasks and services often results in common infrastructures for multifunctional use or shared service delivery;
- online delivery of services: new infrastructures not only allow delivery of services online, but also across public services and entities, thus creating more or less independent interfaces with citizens (users, clients etc).

Most current public sector reform has a *national focus*, although experience is shared with similar projects in other countries. The number of cross-border systems (such as the Internal Market Information System) is still very limited.

2. Security and privacy

There is no doubt that an ICT infrastructure for e-Government services requires a very high and robust level of security to ensure its availability, integrity and confidentiality on a permanent basis. This is even more so, if one considers the risk and potential impact of cyber attacks. Therefore, a multi-level infrastructure may well be required to provide adequate security in this context.

However, 'security' and 'privacy' should not be confused, nor should 'privacy and data protection' be treated as a subcategory of security.[2] These concepts should rather be regarded as distinct and only partly overlapping. Briefly put: good security does not necessarily provide good privacy and data protection, but good privacy and data protection would always require good security.[3]

This can also be formulated in another way: if security measures are needed to protect against '*unauthorized* disclosure or access' or 'all other *unlawful* forms of processing'[4], privacy and data protection are more about whether a certain disclosure or access of other form of processing should be *authorized* or *lawful* or not. They also provide for certain rights for data subjects and for certain arrangements of institutional oversight.[5]

3. Privacy and data protection challenges

A brief overview of current data protection legislation, as it applies to e-Government, should highlight the following main areas.

Scope

The national laws implementing Directive 95/46/EC apply to processing of 'personal data', i.e. *"any information relating to an identified or identifiable natural person"* in the private or public sector.[6] Although these laws follow the same basic concepts and principles, in

[2] The term 'data protection' has been used since the 1980's after the German 'Datenschutz'. However, it does not aim at the protection of data as such, but at the protection of the individuals concerned against the inappropriate collection and use of their personal data. See Article 1 of the current data protection Directive 95/46/EC: *"... Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."*

[3] Articles 16 and 17 of Directive 95/46/EC deal with 'confidentiality' and 'security of processing'.

[4] Article 17.1 of Directive 95/46/EC: *"Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. (....)"*

[5] Article 8 of the Charter of Fundamental Rights provides:
1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.

[6] Articles 2(a) and 3 of Directive 95/46/EC

conformity with the Directive, they tend to be slightly different in many relevant details. Each national law should apply to all processing *"in the context of the activities of an establishment of the controller"* on the territory of that Member State.[7] In principle, this means that e-Government in a particular Member State is covered by the laws of that Member State. This is usually the general Data Protection Act of that state, either or not in conjunction with any specific law that may be applicable.

Responsibility

The responsibility for compliance with data protection requirements is imposed on the 'controller', i.e. *"the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data"*. [8] In the public sector, this is normally the public body that is legally competent for the delivery of the service. However, in e-Government, increasingly other public or private actors may be involved as well. This may lead to different arrangements for joint control. The nature and scope of these arrangements may be problematic.

The controller should be carefully distinguished from the 'processor', i.e. *"a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller"*. [9] Processors have specific obligations, notably as to confidentiality and security of processing, but the main focus is on the controller. This terminology does not exclude different processors and sub-processors. However, the need to ensure the overall responsibility of the controller remains.

Lawful processing

The substantive principles of data protection contain a number of key requirements for lawful processing. Key requirements for data quality[10] are that personal data must be:

(a) processed fairly and lawfully;
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (...);
(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
(d) accurate and, where necessary, kept up to date (...);
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. (...).

Key requirements for legitimacy[11] most relevant in this context are that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or
(b) (.....)
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) (.....)
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
(f) (.....).

[7] Article 4 of Directive 95/46/EC
[8] Article 2(d) of Directive 95/46/EC
[9] Article 2(e) of Directive 95/46/EC
[10] Article 6(1) of Directive 95/46/EC
[11] Article 7 of Directive 95/46/EC

Compliance with these conditions requires a careful and timely analysis of all relevant details, notably as to *purpose specification, compatible use, and the need for personal data* at the different stages of the processing of personal data to which they will apply. It will be for the controller to ensure that these conditions are complied with.[12]

It is interesting to note that the provisions on security of processing referred to before require *"appropriate technical and organizational measures to protect personal data against (...) all (...) unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be processed"*.[13] This sets a high standard for most relevant e-Government projects.

Data subject's rights

The controller will also need to provide for the exercise of certain specific rights of the data subjects. Apart from adequate information to be given to data subjects when their data are collected - in order to ensure transparent processing - this involves rights of access, rectification and erasure, and to object to the processing, subject only to a few fairly strict exceptions.[14]

Supervision

The development of e-Government is not only subject to supervision and possible enforcement by independent supervisory authorities in all Member States, but there may also be prior involvement in relevant projects at different stages. This may also include prior consultation on specific legislation introducing certain e-Government measures.[15]

4. Review of EU legal framework

In January 2012 the European Commission presented a proposal for a General Data Protection Regulation[16] to replace Directive 95/46/EC, which is now under discussion in the European Parliament and the Council. The following aspects seem to be most relevant for e-Government.

Scope

The proposed Regulation will be directly applicable in all Member States and replace current national laws, except where some flexibility is left for national specificities. The degree of flexibility in the public sector is an important point for discussion, particularly in the Council. However, in principle, the Regulation would provide one single set of rules applicable in all Member States. Its scope would also include actors established in third countries, when active on the European market.[17] This would have a relevant impact on the provision of cloud services.

Responsibility

The proposed Regulation provides for enhanced responsibilities for controllers and some new obligations for processors.[18] In general, controllers must take appropriate measures to ensure - and be able to demonstrate - compliance with the Regulation. This also includes a number of

[12] Article 5(2) of Directive 95/46/EC
[13] Article 17(1) of Directive 95/46/EC
[14] Articles 10 to 14 of Directive 95/46/EC
[15] Articles 18 to 21 and 28 of Directive 95/46/EC
[16] COM (2012) 11 final
[17] Article 3 of the proposed Regulation
[18] Articles 22 to 34 of the proposed Regulation

specific obligations, such as the implementation of appropriate measures for "data protection by design" and "by default", and the need to undertake "data protection impact assessments", both of which seem to be relevant for e-Government. This underscores the need for a clear identification of the controller and very strong arrangements for shared control where relevant.

Lawful processing

The key requirements for lawful processing will continue to exist as they are now, possibly subject to some flexibility on the need for compatible use.[19] However, as this is a key element of data protection, also highlighted in the EU Charter of Fundamental Rights, the degree of flexibility will be limited.

Data subject's rights

Requirements for transparency have been enhanced and all existing rights have been reinforced,[20] including new elements such as the "right to be forgotten" and the "right to data portability" which may to some extent also be relevant in the public sector. The responsibility of the controller will also entail the need to provide for mechanisms and procedures for the exercise of data subject's rights. This will therefore become an integral part of e-Government development.

Supervision

The powers of supervisory authorities will be much stronger[21] and include the power to impose heavy financial penalties for breaches of the proposed Regulation and powers to impose specific measures where general obligations have not been complied with. There will also be measures to ensure cooperation and consistency in outcomes across the EU.[22]

5. Conclusions

The review of the EU legal framework aims to reinforce data protection rules, make them much more effective in practice and ensure greater consistency across the EU. A single set of rules will facilitate cross-border projects, but will also raise the stakes for e-Government.

Responsibility for the delivery of e-Government services will require a very clear allocation of responsibilities and strong arrangements for transparency and accountability, including data protection by design, impact assessment, and regular monitoring of performance in practice.

[19] Articles 5 and 6 of the proposed Regulation
[20] Articles 11 to 21 of the proposed Regulation
[21] Articles 46 to 54 and 79 of the proposed Regulation
[22] Articles 55 to 63 of the proposed Regulation