The impact of GDPR on the Public Sector

Rolling Sisyphus’ stone?
The General Data Protection Regulation (GDPR) will replace the current Data Protection Directive and take precedence on all national legislation that is in vigour. Although a number of excellent introductions to GDPR are freely available online, most tend to focus exclusively on the impact GDPR has on the private sector. While the consequences, obligations and the fines of up to 20 million dollars (or 4% of worldwide revenue) are keeping many private sector CIOs awake at night and have been widely discussed, GDPR’s far-reaching consequences for the public sector have rarely been highlighted.

This paper aims to rectify that situation, by clearly mapping the obligations of public sector organisations when processing personal data, and by listing the practical implications GDPR has for the public sector. We will argue that GDPR offers public sector organisations more leeway than private enterprises for processing data, but that in order to comply to all GDPR obligations by May 2018, the workload for the public sector is vast.

This paper will first zoom in on the processing of personal data by public sector organisations. Afterwards, the focus will be shifted to the practical obligations of the public sector in implementing GDPR. Finally, the main steps that need to be taken by public bodies to be GDPR-ready, will be listed.
Gimme Shelter: Basics of the regulation

GDPR aims to protect the “fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data”, while at the same time enabling the “free movement of personal data within the Union” (GDPR, Art. 1). To harmonize these seemingly diametrically opposed objectives, GDPR lays down a set of rules for private and public organisations “with regard to the processing of personal data and rules relating to the free movement of personal data”. (Very) Generally speaking, GDPR pushes accountability to the data controller, who needs to inform the data subject and needs a clearly defined form of authorisation for all data processing.

However, with respect to public authorities, not all personal data are the same, as will be explained below.

Fingerprint file

In principle, GDPR applies to all personal data - all information relating to an identified or identifiable natural person, including genetic and biometric data - intended to become part of a “filing system” of EU subjects, independent of the public or private nature of the receiver (GDPR, Art. 2).

However, for public sector organisations\(^1\), some major exceptions are foreseen where GDPR does not apply:

1. Public authorities that collect data in the framework of a particular investigation in accordance with a legal obligation for the exercise of their official mission are not seen as recipients and thus do not have to comply to GDPR. (GDPR, Art. 2, 9) The key word here is ‘particular’, indicating it is not a free pass for all public authorities, but only is valid in the context of an inquiry into a specific situation. GDPR mentions different examples, such as inquiries by tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities\(^2\). (GDPR, Rec. 31)

2. Competent authorities, mainly police and judicial services, are excluded “for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security”. (GDPR, Art. 2, 2 (d)) GDPR also provides a legal basis for “processing of personal data relating to criminal convictions and offences or related security measures […]”. Any comprehensive register of criminal convictions shall be kept only under the control of official authority”. (GDPR, Art. 10) In short, entire parts of police and judicial activities related to the prevention and prosecution of crimes don’t have to take GDPR into account.

3. Member states carrying out activities which fall within the scope of the EU Common Foreign and Security Policy. (GDPR, Art. 2, 2 (b)) This provision broadly shields data processing by services and departments related to ministries of Foreign Affairs. However, these services will have to demonstrate that the processing of personal data is based on the EU Common Foreign and Security Policy.

In conclusion, for specific areas of public sector activities, broadly related to oversight, crime detection and crime prevention, GDPR does not apply and existing legislation concerning lawful processing remains in vigour. This has to be clearly distinguished from the more common processing by public authorities, where GDPR fully applies.

\(^1\) For EU institutions and agencies, another regulation applies, namely (EC) No 45/2001.

\(^2\) “Public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients”. (GDPR, Art. 4, 9) “Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. (GDPR, (31)).
Lawful processing: You can’t always get what you want

The provisions above determine when GDPR does not apply to the activities of public authorities. Where GDPR does apply, it strictly describes what constitutes lawful processing of personal data by public authorities:

1. The ‘need for consent’ is mainly eliminated. This need for consent of the data subject to process personal data has major implications for private enterprises. Public authorities, however, don’t have to comply with this in so far “as 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” (GDPR, Art. 6, 1 (f)). Furthermore, the purpose of processing needs to be laid down in Union- or Member State law. This implies that consent is not required for data processing activities of public institutions if the institution can demonstrate that the processing is in the ‘public interest’ and falls within its legal competences. We emphasize that a ‘legitimate interest’ without a legal basis in EU or Member State legislation does not constitute sufficient basis for legal processing. It is therefore advisable for institutions to assess whether all collected data fall within this scope. For instance, one could argue that the collection of (e-mail) addresses for dissemination purposes by governmental agencies is not always strictly necessary for carrying out the tasks within its legal competences.

2. Processing for “archiving purposes in the public interest, scientific or historical research purposes or statistical purposes” is legal. (GDPR, Art. 89)

3. The notorious ‘Right to be forgotten’ does not apply if it impedes the performance of a task carried out in the public interest (and more specifically in the area of public health) or in the exercise of official authority vested in the controller. It also does not apply for data processing for archiving purposes in the public interest, and scientific, statistical or historical research purposes.

Finally, some types of personal data are considered off-limits for processing, namely ”personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation”. (GDPR, Art. 9, 1) Again, some exceptions are made, for instance:

1. In the framework of legal obligations of the data controller considering employment, social security and social protection law.

2. For courts acting in their judicial capacity.

3. For reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices. (GDPR, Art. 9 & recital 53)

Generally speaking, legal basis is the name of game for public institutions. GDPR provides various instruments for public authorities to claim a legal basis or an exception. Furthermore, while ‘consent’ and ‘the right to be forgotten’ are major topics for private sector organisations and entail a complete rethinking of data processing procedures, they generally do not apply to public sector organisations. In this regard, the impact of GDPR is clearly heavier on the private than on the public sector. Therefore, we can conclude that for public authorities working clearly within their legal competence, GDPR does not form an unsurpassable obstacle for the continuation of their normal operations.

---

Beast of burden

It is important to understand that while GDPR provides more leeway to public authorities compared to private enterprises, some obligations and rights need to be complied with all the same. We will argue that in some respects, the operational burden in implementing GDPR is much heavier for the public sector than for the private sector. The regulation leaves room for governments to add specific restrictions and also imposes a number of practical arrangements, such as establishing a supervisory authority.

Filling in the legal blanks

Although GDPR is a regulation and therefore does not need to be translated into national law, it does leave a few blank spaces where Member States can introduce more specific requirements. GDPR only describes the minimum requirements and Member States can further determine limitations or exceptions relating to situations where:

1. Processing is necessary for compliance with a legal obligation to which the controller is subject;
2. 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;
3. The processing of genetic data, biometric data or data concerning health is concerned. (GDPR, Art. 9, 4)
4. Profiling, i.e. automated decision-making on a data subject, such as direct marketing. Member States can explicitly allow certain types of profiling (GDPR, Art. 22, 2 (b)).

The specific requirements can include “the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures”. Furthermore – and not without controversy – specific provision can curtail the rights of data subjects if necessary for amongst others: (a) national security; (b) defence; (c) public security (Complete list: GDPR, Art. 23).

This legal workload will be complemented by a number of practical arrangements that need to be made, such as establishing a supervisory authority, appointing Data Protection Officers, informing data subjects and integrating Data Protection Impact Assessments. These will be discussed below.

Establishing and supporting a supervisory authority

Each country, and in federal states possibly each region, will be legally obliged to establish a supervisory authority. This independent supervisory authority will be responsible for monitoring and enforcing the application of the GDPR and will handle all complaints by data subjects. Furthermore, the supervisory authority will advise national or regional parliaments on legal issues concerning GDPR (Complete list of tasks under GDPR, Art. 57.). The Member States shall provide “the human, technical and financial resources, premises and infrastructure necessary”.

---

5 We stress that the principles of GDPR concerning data minimisation, anonymisation and proportionality are applicable to public authorities. For reasons of brevity, the impact of these principles will not be discussed here.
In many countries, these supervisory authorities will not be new institutions, but rebranded existing institutions that have similar objectives. However, because of the enlarged scope and more proactive assignment, the capacities, resources and capabilities of these institutions will need to be increased.

**Appointing Data Protection Officers**

All public authorities (except for courts acting in their judicial capacity) must designate a Data Protection Officer (DPO). A DPO consults data controllers and processors on following GDPR standards and thus helps to ensure compliance. Several institutions can designate a single DPO, taking into account their organisational structure and size, but the DPO must be ‘easily accessible’ for all of these institutions (GDPR, Art. 37-39). The data protection officer may be a staff member, or fulfil the tasks on the basis of a service contract.

**Informing data subjects**

Governmental institutions might have more freedom than private companies concerning data processing, they do need to provide the data subject with information about the legal basis for processing and with the contact details of the data protection officer and data controller. These contact data need to be communicated to the supervisory authority as well (GDPR, Art. 13).

**Get off My Cloud (?): Data Protection Impact Assessments**

Data Protection Impact Assessments (DPIA) is an analysis of the risk of non-compliance to GDPR and is to become standard procedure during the implementation of all processes “likely to result in a high risk to the rights and freedoms of natural person”, in particular using new technologies. A Data Protection Assessment contains a “systematic description of the processing and its purposes”, an “assessment of the necessity and proportionality of the processing”, an “assessment of the risks to the rights and freedoms of data subjects” and a risk mitigation plan. (GDPR, Art. 35) An audit of the technical aspects of data storage might be opportune, as unauthorised data storage outside of the EU can have grave implications.

The DPO is to be closely involved with the DPIA. For public authorities, excluding courts, which process lots of personal data, this entails a new way of preparing to implement almost any significant new technology or ICT project.

These general obligations translate to a whole series of practical measures that need to be taken by public authorities. Given the deadline of May 2018, the practical ramifications of GDPR implementation in the public sector are tremendous, as we will demonstrate by shedding some light on the tasks that lie ahead.
Down the road a piece

Public authorities, semi-public companies, public agencies, … will all need to come to terms with the new requirements and all procedures will need to be re-assessed from the GDPR perspective. As a pointer, we include the major tasks and challenges ahead for the public sector.

1. Get organised

• Set up a road map: the government as a whole and each individual organisation should have a GDPR strategy and a corresponding road map for implementation. A fine example is the roadmap the Belgian Crossroads Bank for Social Security has put online (Link in Dutch and in French).

• Appoint DPOs: DPOs can assist organisations throughout the implementation of GDPR. The earlier in the process they get involved, the better they can ensure a coordinated and smooth transition.

2. Do the legal work

• Determine what a public body is: as explained above, public and private organisation have sometimes divergent obligations under GDPR.

• Verify the legal basis for data processing and determine proportionality.

• Prepare legislation: as discussed above, there are some legal blanks that need to/can be filled in. An impact assessment of GDPR on other existing legislation is needed as well.

• Set up a Supervisory Authority and provide it with sufficient means.

• Encourage the establishment of data protection certification mechanisms and of data protection seals and marks. These will be elementary in providing guidance to the private sector.

3. Cultivate Privacy by Design

• Map the ‘As Is’ situation for all data processing and reassess if your legal basis is sufficient.

• Introduce tools and practices to register each act of personal data processing (the so-called internal register).

• Incorporate DPIA in standard procedures and project management methodology.

• Audit data processing suppliers to ensure they meet GDPR standards.

• Train your staff to ensure they understand what the new obligations of the data controller and the rights of data subjects are.

4. Tell that what you’re going to do, tell them what you’ve done

• Update all privacy notes, policies, terms & conditions to inform data subjects adequately.

• Prepare to communicate with data subjects, especially when data have been obtained by consent.

• Prepare for data breaches by putting a communication plan in place in case of breach.
Simon Nichelson is a public sector business analyst at DXC technology. He holds master degrees in European politics and policies, modern history and philosophy. You can follow him on LinkedIn.

The DXC Technology Public Sector team consists of highly specialised public sector experts, with a longstanding expertise in public administration reform, tax and revenue management and ICT implementations.

About the author:

Simon Nichelson is a public sector business analyst at DXC technology. He holds master degrees in European politics and policies, modern history and philosophy. You can follow him on LinkedIn.

The DXC Technology Public Sector team consists of highly specialised public sector experts, with a longstanding expertise in public administration reform, tax and revenue management and ICT implementations.