GDPR: A PRAGMATIC APPROACH

AUTHOR: KOEN CLAESSENS
PARTNER - BDO RISK & ASSURANCE SERVICES

INTRODUCTION

Numerous information sessions have been held and publications issued about the whys and wherefores of General Data Protection Regulation (GDPR), often from a legal perspective. So, everyone has become aware of the importance of GDPR.

However, many (maybe even the majority) are still unclear as to how they will effectively ensure that their organisation is GDPR-compliant by 25 May 2018. In other words: the WHAT has become clear for everybody, but many questions remain about the HOW.

In this white paper, we propose a pragmatic approach to implementing GDPR, based on our own experience, with limited overhead within the organisation.

GDPR MEASURES

Although GDPR legislation is, of course, a legal given, its implementation has organisational and IT elements as well as legal ones. We distinguish **a total of 8 measures** that are to be implemented:

1. DATA PRIVACY POLICY & AWARENESS PROGRAM

2. MAINTAINING A DATA REGISTER OF PERSONAL DATA

3. PRIVACY IMPACT ASSESSMENTS (PIAs) FOR SENSITIVE PERSONAL DATA

4. IMPLEMENTING SECURITY MEASURES

5. ADAPTING THE AGREEMENTS BETWEEN CONTROLLERS AND PROCESSORS (SUPPLIERS)

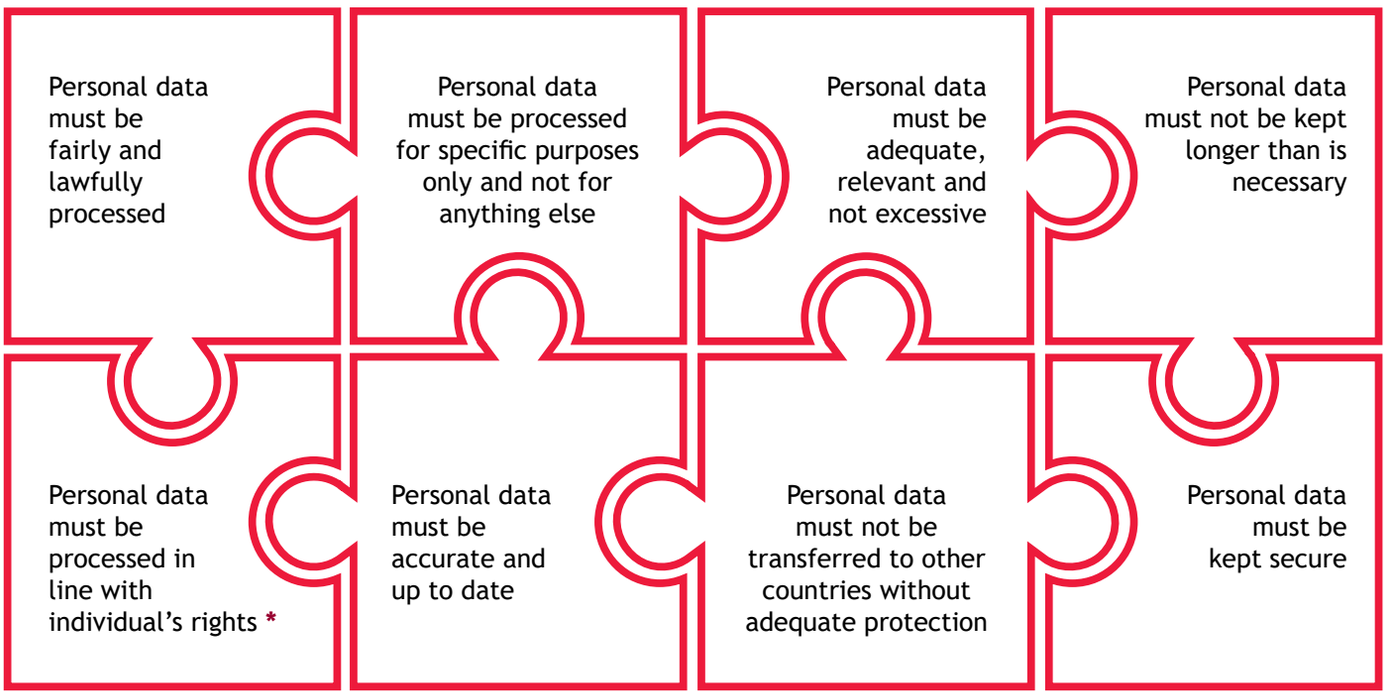
6. ADJUSTING COMMUNICATION TO THE 'DATA SUBJECTS' THROUGH 'PRIVACY NOTICES'

7. DATA BREACH NOTIFICATION

8. APPOINTMENT OF A DATA PROTECTION OFFICER (DPO)

1. DATA PRIVACY POLICY & AWARENESS PROGRAM

Organisations must have a data privacy policy that describes how they collect, use and manage personal data. **The 8 well-known GDPR principles** are the starting point for this:



*** right to access their data, right to get data deleted, right to be forgotten, right to object data distribution, opt out of direct marketing, claim compensation for damages**

In addition, the actual meaning of data privacy for the organisation and its specific activities are indicated, as well as which personal data are recorded in that context. The data privacy policy also provides clear guidelines to the organisation's staff in order to protect personal data.

Once the guidelines are set out, they must be communicated to management and the staff who handle personal data. This can be done through videos, e-learning, awareness sessions, etc. These are often combined with tips & techniques regarding cyber-security. Later, the Data Protection Officer (see below) will have to verify whether the guidelines are actually being followed.

2. MAINTAINING A DATA REGISTER OF PERSONAL DATA

Setting up the data register constitutes the basis of GDPR and provides a first view of the amount of personal data within the organisation. The data register must be set up and maintained for all categories of personal data processing activities that are performed by the organisation. Important elements that are registered for the identified personal data are usually:

- Nature and purpose of processing
- Categories of those involved (data subjects)
- Where (on which systems) and how the data are recorded
- Who collects the data and keeps them up-to-date
- Details and purpose of data transfers
- Data retention periods

After drawing up the data register, the following questions are asked to ascertain whether the 8 data privacy principles are being fulfilled for the identified personal data:

- What is the reason for data processing, and is it justified?
- Have we obtained permission from the data subject and have we been transparent about the way in which we are going to use the data?
- Do we actually need all the data, and do we only keep the data that we need for our purposes?
- How do we ensure that the data are accurate and up-to-date?
- How long do we retain data, and is this necessary?

3. PRIVACY IMPACT ASSESSMENTS (PIAs) FOR SENSITIVE PERSONAL DATA

Privacy Impact Assessments (PIAs) must be made for the most sensitive personal data: analysing and documenting risks on the one hand, and the measures taken to protect the data on the other.

In this context, the sensitivity of the personal data is initially determined through objective criteria, such as the potential impact and possible abuse of data, amount of data, etc.

In addition, the protection measures that are in place to protect the data are mapped out, typically on multiple levels:

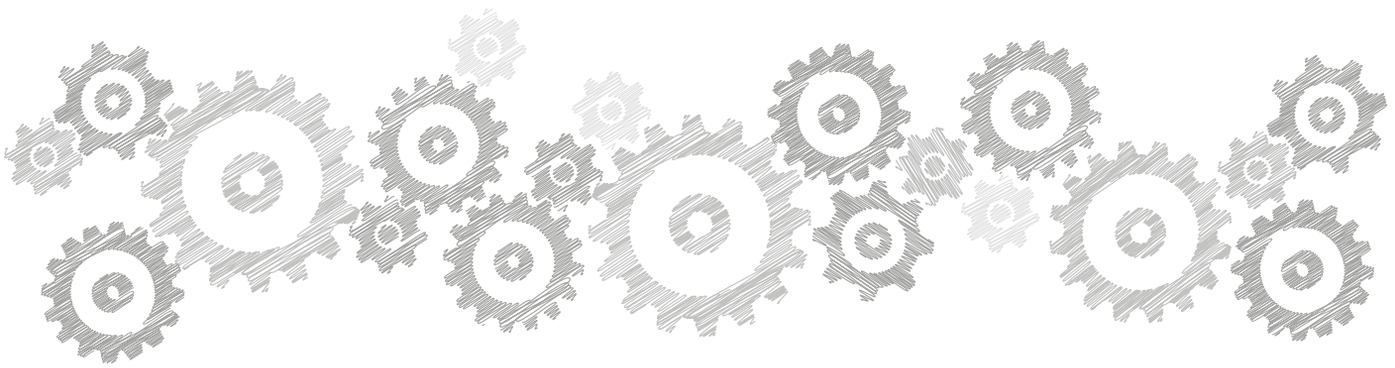
- Security policies and procedures
- Application security and Active Directory
- IT infrastructure security
- Physical security

4. IMPLEMENTING SECURITY MEASURES

Thus, the PIAs examine whether the measures taken to secure data are proportionate to the sensitivity of those data. If the measures taken do not suffice, additional security measures must be implemented according to a ‘suitable’ security level, in line with the PIAs.

That is what GDPR legislation states, but of course a ‘suitable’ security level is subjective. Parties will have to define this by themselves and document what measures this involves. This will certainly be important in the case of a future data breach, and the measures taken will need to be proven (e.g. to the Data Privacy Commission).

The security measures themselves are typically a combination of organisational and IT measures. Examples are implementing procedures, passwords, roles, badges, etc.



5. ADAPTING AGREEMENTS BETWEEN CONTROLLERS AND THE PROCESSORS

GDPR distinguishes between **'controllers'** (who determine the purpose and the resources for processing) and **'processors'** (suppliers who process data upon the controller's request). An example is a social secretariat that processes personal data (payroll) as a processor upon the request of its clients, the controllers of the personal data.

GDPR requires **the controller** and **the processor** (who works upon the controller's request) to enter into a written agreement. GDPR has stipulated the content of this written agreement, and roles and responsibilities regarding data privacy are clearly defined.

The liability of the processors for the correct processing of personal data increases under GDPR – so processors will also be subject to fines and damage claims. In the case of data leaks at processors, they must notify the controllers (the clients hit by the leak) as soon as possible.

It will become increasingly important for suppliers to demonstrate their reliability regarding data privacy to clients and potential clients. This can be done through GDPR certification, which enables suppliers to show that they are GDPR-compliant and meet all GDPR requirements.

6. PRIVACY NOTICES

An important data privacy principle is that we must be transparent towards those involved (employees, clients, etc.) about which data we collect and how we use them. In some cases, permission must be requested, which is done through so-called 'privacy notices'.

Organisations will be required to inform those involved (data subjects), the most important elements are: what data is processed, the basis of the processing (e.g. permission, justified importance, etc.), the purposes of processing, the retention period, sharing with third parties, and the rights of those involved

7. DATA BREACH NOTIFICATION

The Privacy Commission will need to be notified of data breaches regarding personal data. In the case of violations, compliance with GDPR will have to be proven, as well as the fact that suitable measures were taken to protect personal data sufficiently.

For this purpose, an incident procedure and register (system) will need to be implemented. Often, a similar system is already in use by the safety officer of the organisation – and, after a few small adjustments, this can probably be used for GDPR as well. Incidents must be registered and analysed in this system to identify which personal data and individuals are involved. The objective is to evaluate the sensitivity of the incident – and based on this, decisions will be made as to whether those involved and the Data Privacy Commission must be notified.

When notifying the Privacy Commission of data breaches, it will be necessary to indicate: (1) what has happened, (2) which error and weakness in the system caused it, and (3) which measures had been taken to avoid data breaches. Any fines will depend on the level of negligence. New responsibilities of the Privacy Commission will be to investigate data breaches and carry out inspections.

8. DATA PROTECTION OFFICER (DPO)

A new position has been created: the Data Protection Officer (DPO), who is responsible for GDPR compliance within the organisation. Organisations that employ over 250 employees, and organisations that process sensitive personal data, are required to appoint a DPO. For other organisations that do not meet these criteria, the appointment of a DPO is still recommended as a 'best practice'.

The DPO is seen as an extension of the Privacy Commission. He or she can be contacted by the Commission to provide information, and the DPO is to notify the Commission of any data breaches. In some sectors (the healthcare and public sectors, for example), the requirement for a 'security advisor' already exists – the DPO is regarded as an expansion of this function.

The DPO's responsibility is to ensure GDPR compliance by managing the data register, conducting PIAs, and following up on security measures, agreements with processors and privacy notices. In addition, he or she has a number of other 'continuous' tasks, such as organising 'Security awareness' sessions, investigating complaints and responding to questions regarding data privacy, conducting sample reviews regarding staff and third-party access, and checking safety logs. In addition, he or she will report to the Management about all of this.

Belgian companies will need an estimated 6,000 DPOs in total. Due to the specific requirements regarding competences, these profiles will be difficult to find. Therefore, many are expected to choose to outsource the function (DPO as a service). But the service providers are also likely to encounter shortages, which means that these profiles will be highly sought after. DPO is expected to become one of the leading job positions of the future.

These are the job trends of 2017

article: vacature.com

The arrival of the Internet and other digital technologies led to the creation of a lot of new jobs. About 20 years ago, functions such as web designer, millennial generation expert and social media manager did not exist. In 2017 as well, new jobs and/or trends will appear on the labour market.

NEW JOBS :

Data protection officer

"*The* job of 2017 is definitely 'data protection officer' or DPO. The European authorities will soon develop a new regulation about the protection of EU citizens' personal data. The General Data Protection Regulation (GDPR) will have consequences for all companies that handle personal data. A lot of companies are asking themselves questions about this new and far-reaching regulation."

The data protection officer (DPO) can answer these questions – and, in many cases, a DPO is even obliged to do so. This is the case, for example, for public authorities, companies that regularly handle data on a large scale, and companies that handle 'sensitive' data such as religion, political preferences, or sexual orientation.

Profile: understand legal texts and communicate clearly to staff, thorough IT knowledge.

FOR WHICH ORGANISATIONS IS GDPR IMPORTANT?

GDPR applies to all organisations that manage personal data. Since all organisations manage at least the personal data of their own employees, everybody is involved – but if this is the only issue, efforts will be limited. Most organisations manage a lot of other personal data these days: typical examples are contact details of clients in the CRM system and payment data of clients on the e-commerce website.

Some industries are more involved than others due to the specific sensitive personal data that they manage. The top 5 are:

HEALTHCARE
(MEDICAL DATA)

FINANCIAL INDUSTRY
(FINANCIAL DATA)

PUBLIC SECTOR
(CITIZENS' DATA)

ICT AND COMMUNICATION
(AS A PROCESSOR)

RETAIL
(CLIENT AND PAYMENT DATA)

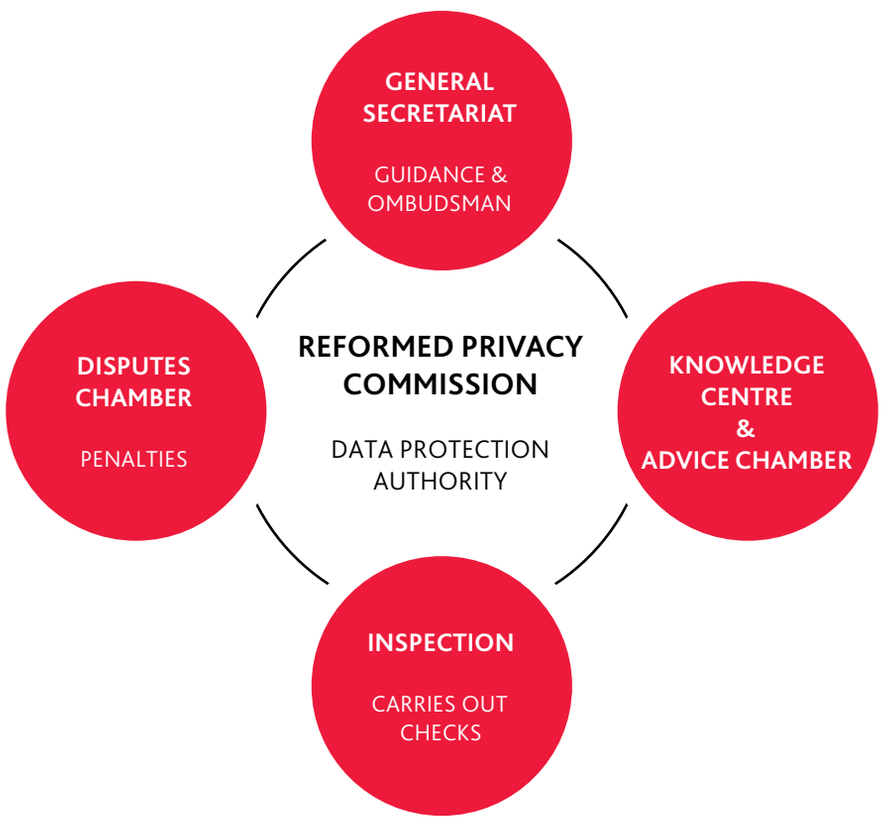
THE ‘NEW’ DATA PRIVACY COMMISSION: THE DATA PROTECTION AUTHORITY (DPA)

The introduction of GDPR will significantly change the protection of personal data in Belgium, and thus the Data Privacy Commission as we know it will undergo a metamorphosis. It will gain more responsibilities so that it can truly protect the rights of citizens and can call organisations to account if they do not respect those rights.

But because creating new rights and obligations alone are not sufficient to increase the level of protection, the GDPR requires Member States to implement a supervisory authority that has the responsibilities needed to ensure compliance. And this authority is the new Belgian Data Protection Authority (DPA), the new name for the former Data Privacy Commission.

The new, independent DPA will not only assume the advisory role of its predecessor, but it will also be able to perform extensive investigative actions and impose various sanctions. In this way, the DPA will gain the power needed to ensure compliance with GDPR.

In order for the DPA to perform this new role optimally, it will be further divided into 5 bodies:



CYBER-SECURITY AND GDPR

Cyber incidents are one of the main causes of data breaches: a hacker can steal sensitive personal data, and this is expected to become increasingly common.

Thus, good cyber protection will become an important component of GDPR compliance. Unfortunately, perfect protection does not exist, the techniques applied by hackers are becoming more and more sophisticated, and it is practically impossible to be prepared for anything that might happen. So, not only must preventive measures be taken, a plan must also be prepared in case security measures are circumvented by a hacker.

In any event, it is important to ensure that the 'basic' measures are in place, such as patch management, strong passwords, firewalls, encryption, etc. Then, a company will be able to demonstrate that it has acted with all due care. This 'demonstrability' in the event of data leaks breaches will be important, also when it comes to reputational damage.

Fortunately, not all cyber incidents lead to data breaches. The most recent 'Wannacry' ransomware attack was very troublesome to the organisations involved, but it did not lead to data breaches in which personal data left the organisation. However, chances are that this will happen in future attacks.

But, even if companies implement the most important security measures in an effort to act with all due care, a residual cyber-security risk will always remain. For that reason, more and more organisations are taking out cyber-security insurance policies. Just as all organisations these days have fire insurance and professional liability insurance, within the near future they will have cyber-security insurances as well.

Cyber-security insurances usually also cover GDPR-related risks and costs. Currently, the premiums for these insurance policies are still quite low, but they are expected to increase quickly in the future. Therefore, the advice is not to wait too long.

A PLAN TO BECOME GDPR-COMPLIANT BY 25 MAY 2018

Your organisation is not yet working on GDPR? No reason for panic, as a recent study showed this to be the case for 61% of organisations. But it does mean that it's time for action now.

It all starts with a GDPR assessment, in which the organisation's 'gap' regarding GDPR legislation is determined and an action plan is drawn up accordingly. An important part of this is creating an initial inventory of the personal data in your organisation to provide a clear picture of the effort required to become GDPR-compliant.

For a mid-sized organisation, 6 months are usually needed to carry out the action plan and the GDPR implementation itself. In order to become GDPR-compliant by 25 May 2018, it is best for an initial GDPR assessment to take place during or soon after the summer holiday period.

HOW CAN WE ASSIST YOU?

GDPR requires competences and resources in multiple domains: organisational, legal and IT. We offer a combined approach, in which these domains are covered by our BDO Risk & Assurance Services and BDO Legal departments.

We can assist you in carrying out the following tasks:

- **GDPR assessment:** this is usually the first step towards becoming GDPR-compliant. In a GDPR assessment, the current situation (AS-IS) is determined, as well as the 'gap' with regard to GDPR legislation. Based on this, specific measures are determined (TO-BE) and a pragmatic action plan is drawn up.
- **Assistance with GDPR implementation:** once the plan has been determined, the various elements of the plan must be carried out on the organisational, IT and legal levels. We can help you implement these elements, as well as take care of the project management involved.
- **Data Protection Officer (DPO):** this position is required for many organisations as of 25 May 2018. We can perform this role for you.
- **GDPR certification**: GDPR certification enables organisations to show clients, partners and monitoring bodies that they comply with GDPR legislation or certain elements thereof. This is primarily of interest to processors of personal data.

A pragmatic approach to the implementation of GDPR requirements is important. If this is not tackled efficiently, it may turn into a budget-consuming and overhead-creating monster. BDO assures you of a pragmatic and straightforward approach.