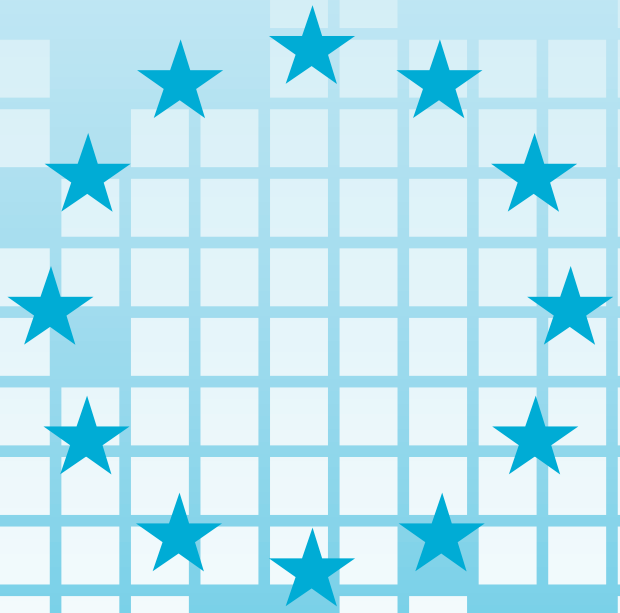
CPP
Commission for the protection of the privacy

GENERAL DATA PROTECTION REGULATION

BE PREPARED IN 13 STEPS



Version 2.0 (January 2018)

1. AWARENESS

You should make sure that decision makers and key people in your organisation are aware of the rules concerning data processing operations. They need to appreciate the impact this is likely to have.

2. RECORD OF PROCESSING ACTIVITIES

You should map what personal data you hold where it came from and who you share it with and set up a record of your processing activities. You may need to organise an information audit.

3. DATA PROTECTION OFFICER

You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

4. COMMUNICATING PRIVACY INFORMATION

You should review your current privacy notices and evaluate them in the light of the GDPR.

5. INDIVIDUALS' RIGHTS

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

6. ACCESS REQUESTS

You should update your procedures and plan how you will handle requests within the new GDPR timescales and provide any additional information.

7. LEGAL BASIS FOR PROCESSING PERSONAL DATA

Document the various types of data processing you carry out and identify the legal basis for each of them.

8. CONSENT

You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

GENERAL DATA PROTECTION REGULATION

BE PREPARED IN 13 STEPS

9. CHILDREN

You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

10. DATA BREACHES

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

11. DATA PROTECTION BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS

You should familiarise yourself now with the concepts of Data Protection by design and DPIAs and work out how and when to implement them in your organisation.

12. INTERNATIONAL

If your organisation operates internationally, you should determine which data protection supervisory authority you come under.

13. EXISTING CONTRACTS

You should review your current contracts especially with processors and subprocessors and make the necessary changes in time.

INTRO

INTRODUCTION

GENERAL DATA PROTECTION REGULATION

THE GENERAL DATA PROTECTION REGULATION (GDPR) BECOMES EFFECTIVE ON 25 MAY 2018. BE PREPARED IN 13 STEPS!

The GDPR is not completely new. Many of the GDPR's main concepts and principles are much the same as those in the Belgian Privacy Law, so if you already complied properly with the current law then you have a head start on the implementation of the GDPR. However, there are new elements and significant enhancements, so you will have to do some things for the first time and some things differently.

With the help of this checklist, and the additional information on the website of the Privacy Commission, you can establish an action plan. The Privacy Commission, with the input given by the sectors, provides guidelines and new tools in order to guide companies and organizations in their preparation. At European level, the Article 29 Data Protection Working Party also issued some guidelines. The European Data Protection Board continues the work.

Look around you – check if models exist for your sector or if codes of conduct have been developed by sector associations. Gain 'buy in' from key people in your organisation. You may need, for example, to put procedures in place to deal with the GDPR's new transparency and individuals' rights provisions. In a large or complex business this could have significant budgetary, IT, personnel, governance and communications implications.

One emphasis of the GDPR is placed on the documentation that data controllers must keep to demonstrate their accountability. This checklist helps companies and organizations to assess their current data protection policy and bring modifications to deal with the GDPR's provisions. One first step of this might be to review the contracts and other arrangements you have in place when sharing data.

Note that some parts of the GDPR will have more of an impact on some organisations than on others, for example the provisions relating to profiling or children's data. So it would be useful to map out which parts of the GDPR will have the greatest impact on your business model and give those areas due prominence in your planning process.

AWARENESS

You should make sure that decision makers and key people in your organisation are aware of the GDPR. They need to appreciate the impact this is likely to have and identify areas that could cause compliance problems under the GDPR. It would be useful to start by looking at your organisation's risk register, if you have one.

Implementing the GDPR could have significant resource implications, especially for larger and more complex organisations. Check whether models exist for your sector or if codes of conduct have been developed by sector associations.

RECORD OF PROCESSING ACTIVITIES

You should map what personal data you hold, where it came from and who you share it with and set up a record of your processing activities. You may need to organise an information audit across the organisation, or within particular business areas.

The GDPR assigns rights to data subjects. For example, if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own data. Doing this will also help you to comply with the GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles.

The Privacy Commission proposes on its website a template for the record of processing activities with a guide thereto.

READ MORE

- Recommendation 06/2017 *(only in Dutch and French)*
- Template record processing activities *(only in Dutch and French)*

DATA PROTECTION OFFICER

You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance. Assess where this role sits within your organisation's structure and governance arrangements.

The GDPR will require some organisations to designate a Data Protection Officer (DPO), for example public authorities or ones whose core activities involve the regular and systematic monitoring on a large scale of data subjects or a large-scale processing of sensitive data. The important thing is to make sure that someone in your organisation, or an external data protection advisor, takes proper responsibility for your data protection compliance and has the knowledge, support and authority to do so

READ MORE

- Recommendation 04/2017 *(only in Dutch and French)*
- Guidelines on the DPO (WP243)

effectively. Therefore you should consider now whether you will be required to designate a DPO and, if so, to assess whether your current approach to data protection compliance will meet the GDPR's requirements.

COMMUNICATING PRIVACY INFORMATION

You should review your current privacy notices and evaluate them in the light of the GDPR. When your company or organization collects personal data, you have to give people certain information, such as your identity and how you intend to use their information.

The GDPR sets requirements for the content of this privacy notice. For example, you will need to explain your legal basis for processing the data, your data retention periods, whether you transfer personal data outside of the EU and that individuals have a right to complain to the supervisory authority if they think there is a problem with the way you are handling their data. Note that the GDPR requires the information to be provided in concise, easy to understand and clear language.

READ MORE

- Guidelines on transparency (WP260)

INDIVIDUALS' RIGHTS

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

The main rights for individuals under the GDPR will be:

- ***subject access,***
- ***to have inaccuracies corrected,***
- ***to have information erased,***
- ***to prevent direct marketing,***
- ***to prevent automated decision-making and profiling, and***
- ***data portability.***

Plan roadmaps that detail how you will work when a data subject wants to exercise his/her right. Who will make the decisions? Would your systems help you to deal this? More attention should be paid to the right to data portability. This is an enhanced form of subject access where data subjects have the right to obtain the data related to him/her electronically and in a structured and commonly used format. Many organisations already provided the data in this way, but be aware that paper print-outs or an unusual electronic format are not sufficient under the GDPR.

Do you use automated individual decision-making? Then you must know the specific rules that apply thereto under the GDPR.

READ MORE

- Guidelines on data portability (WP242)
- Guidelines on automated individual decision-making (WP251)

ACCESS REQUESTS

Think on how you will handle requests within the timescales of the GDPR and plan eventually an update of your current access procedures.

The GDPR defines the rules for dealing with access requests. In most cases you cannot charge for complying with a request and you have a month to comply. Manifestly unfounded or excessive requests can be charged for or refused. If you want to refuse an access request, you need to have a policy and appropriate procedures in place to demonstrate why the request meets these criteria.

You also need to provide some additional information to the person making requests, such as your data retention periods and the right to have inaccurate data corrected. A roadmap is crucial, if your organisation handles a large number of access requests. The impact of the changes could be considerable so the logistical implications of having to deal with requests more quickly and provide additional information will need thinking through carefully.

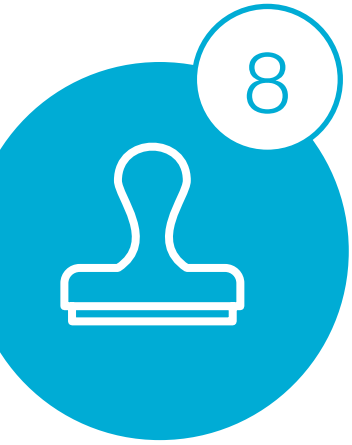
It could ultimately save your organisation a great deal of administrative cost if you can develop systems that allow people to access their information easily online. Companies and organizations should consider conducting a cost/benefit analysis of providing online access.

LEGAL BASIS FOR PROCESSING PERSONAL DATA

You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it. You must choose a legal basis from the list in the GDPR, but pay attention on the difference between “normal” and “special” data.

Under the GDPR some individuals’ rights can be modified depending on your legal basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your legal basis for processing.

You also have to explain your legal basis for processing personal data in your privacy notice and when you answer a subject access request. Look at the various types of data processing you carry out and identify your legal basis and document this in order to help you comply with the GDPR’s ‘accountability’ requirements.



CONSENT

You should review how you are seeking, obtaining and recording consent. The GDPR has references to both 'consent' and 'explicit consent'. The difference between the two do not have to be determined, since both forms of consent have to be freely given, specific, informed and unambiguous. Consent also has to be a positive indication of agreement to personal data being processed – it cannot be inferred from silence, preticked boxes or inactivity. If you rely on individuals' consent to process their data, make sure it meets the standards required by the GDPR. Note that consent has to be verifiable and that individuals generally have stronger rights where you rely on consent to process their data.

The GDPR is clear that controllers must be able to demonstrate that consent was given. You should therefore review your systems for recording consent to ensure you have an effective audit trail.

READ MORE

- Guidelines on consent (WP259)

CHILDREN

The GDPR allows in one specific context children under the age of 16 to give their consent for processing operations, particularly in the context of commercial internet services offered directly to children.

Remark – The Belgian legislator can grant the same privilege to the group of 13-16 years – keep an eye on the website of the Privacy Commission. Note that children who have given their consent themselves may require the erasure of their data at any time, including after attaining majority!

Check if you process data of minor children and if you need to verify individuals' ages. Determine how you can contact the parent(s) or guardian(s), for example to obtain consent or to subscribe a contract.

If your organisation collects information about children, consider the role of their parents or guardians! Remember that consent has to be verifiable and that when collecting children's data your privacy notice must be written in language that children will understand.

DATA BREACHES

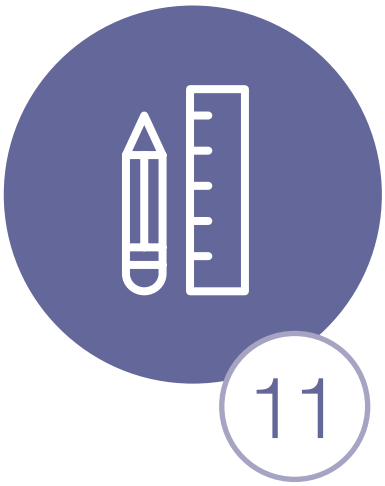
You should make sure you have the right procedures in place to detect, report and investigate a personal data breach. Assess the types of data you hold and document which ones would fall within the notification requirement if there was a breach. In some cases you will have to notify the individuals whose data has been subject to the breach directly, for example where the breach might leave them open to financial loss. Larger organisations will need to develop policies and procedures for managing data breaches – whether at a central or local level.

Not all breaches have to be notified to the supervisory authority, only ones where the individual is likely to suffer some form of damage, such as through identity theft or a confidentiality breach. Note that a failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

READ MORE

- Guidelines on data breach notification (WP250)

DATA PROTECTION BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)



You should familiarise yourself with the concepts of Data protection by Design and Data Protection Impact Assessment (DPIA) and work out how to implement them in your organisation. DPIAs can be linked to other organisational processes such as risk management and project management. You should assess the situations where it is necessary to conduct a DPIA. Who will do it? Who else needs to be involved? Will the process be run centrally or locally? It has always been good practice to adopt a privacy by design approach and to carry out a privacy impact assessment as part of this. However, the GDPR makes this an express legal requirement.

Note that you do not always have to carry out a DPIA – a DPIA is required in high-risk situations, for example where a new technology is being deployed or where a profiling operation is likely to significantly affect individuals. Note that where a DPIA indicates high risk data processing and this despite the measures taken to minimize the “high risk” (in other words, there is a “high residual risk”) , you will be required to consult the supervisory authority to seek its opinion as to whether the processing operation complies with the GDPR.

READ MORE

- Own-initative recommendation 01/2018 *(only in Dutch and French)*
- Guidelines on the DPIA (WP248)

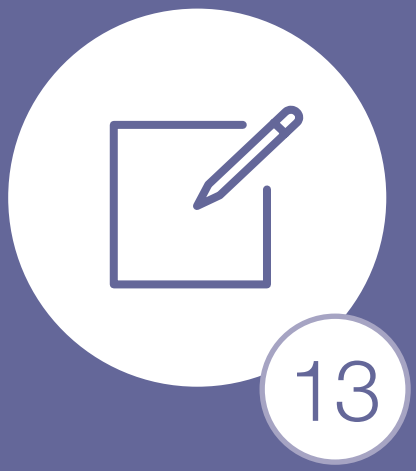
INTERNATIONAL

If your organisation operates internationally, you should determine which data protection supervisory authority you come under. The GDPR contains quite complex arrangements for working out which data protection supervisory authority takes the lead when investigating a complaint with an international aspect, for example where a data processing operation affects people in a number of Member States. Put simply, the lead authority is determined according to where your company or organisation has its main administration or where decisions about data processing are made. In a traditional headquarters (branches model), this is easy to determine. It is more difficult for complex, multi-site companies where decisions about different processing activities are taken in different places.

In case of uncertainty over which supervisory authority is the lead for your company or organisation, it would be helpful for you to map out where your organisation makes its most significant decisions about data processing. This will help to determine your 'main establishment' and therefore your lead supervisory authority.

READ MORE

- Guidelines on the lead supervisory authority (WP244)



EXISTING CONTRACTS

You should review your current contracts especially with processors and sub-processors in order to make changes if necessary. The GDPR creates a well-designed system to cover the relationship between controllers and processors. It goes even further by determining the conditions applicable to sub-processing activities. In order to make sure that you encounter those conditions, you should review the existing contracts and make the necessary changes.

The GDPR emphases as well the importance of the security measures applicable to the databases. If you have outsourced that part, it is important to assess whether the security measures that you have foreseen in the existing contracts are still sufficient and meet the requirements of the GDPR.

MORE INFORMATION ON THE GENERAL DATA PROTECTION REGULATION CAN BE FOUND ON OUR WEBSITE: WWW.PRIVACYCOMMISSION.BE

Commission for the protection of privacy

Rue de la Presse 35 | B-1000 Bruxelles | T+32 (0)2 274 48 00
E-mail: commission@privacycommission.be
Website: https://www.privacycommission.be

Responsible editor
W. Debeuckelaere
Printing
Printing office of the House of Representatives
Design
The Reference

This document is also available in French and Dutch.
Il exste aussi une version française de ce plan par étapes.
Er bestaat ook een Nederlandse versie van dit stappenplan.
This document can be downloaded on the website of the Privacy Commission.