privacy perfect

The ultimate guide to become GDPR compliant

All you need to know in 7 easy steps

The GDPR is complex, yes, but desperation never helped anyone to get further in life.

Therefore, in this guide, we provide a seven step scheme to help you become GDPR compliant. We won't claim it's easy, but it's doable.

To provide you with more insight, we have drafted an infographic reflecting the internal and external stakeholders and sources needed for inventory purposes.

Make sure.

1

Get backing from C-level management

Wandering around in your organisation as a privacy professional without backing from management will probably be a disappointing exercise. But here are the four main reasons why C-level management should (and probably will) provide you with that backing:

- the ability to prove to your stakeholders that you take their privacy seriously
- the danger of reputation damage arising from non-compliance
- the risk of being fined substantially for non-compliance
- the importance of being 'in control' of your personal data handling

Obviously, once backed by C-level management, your project will become easier.

2

Get an overview of your organisation structure and assign 'privacy champions'

IIt might seem trivial at first, but in our experience many customers find difficulty in plotting their organisation structure. Still, this is crucial in terms of both inventorying processing activities and getting your governance in place. Moreover, by assigning people responsible for compliance in various parts of your organisation, you will be able to roll out a governance model.

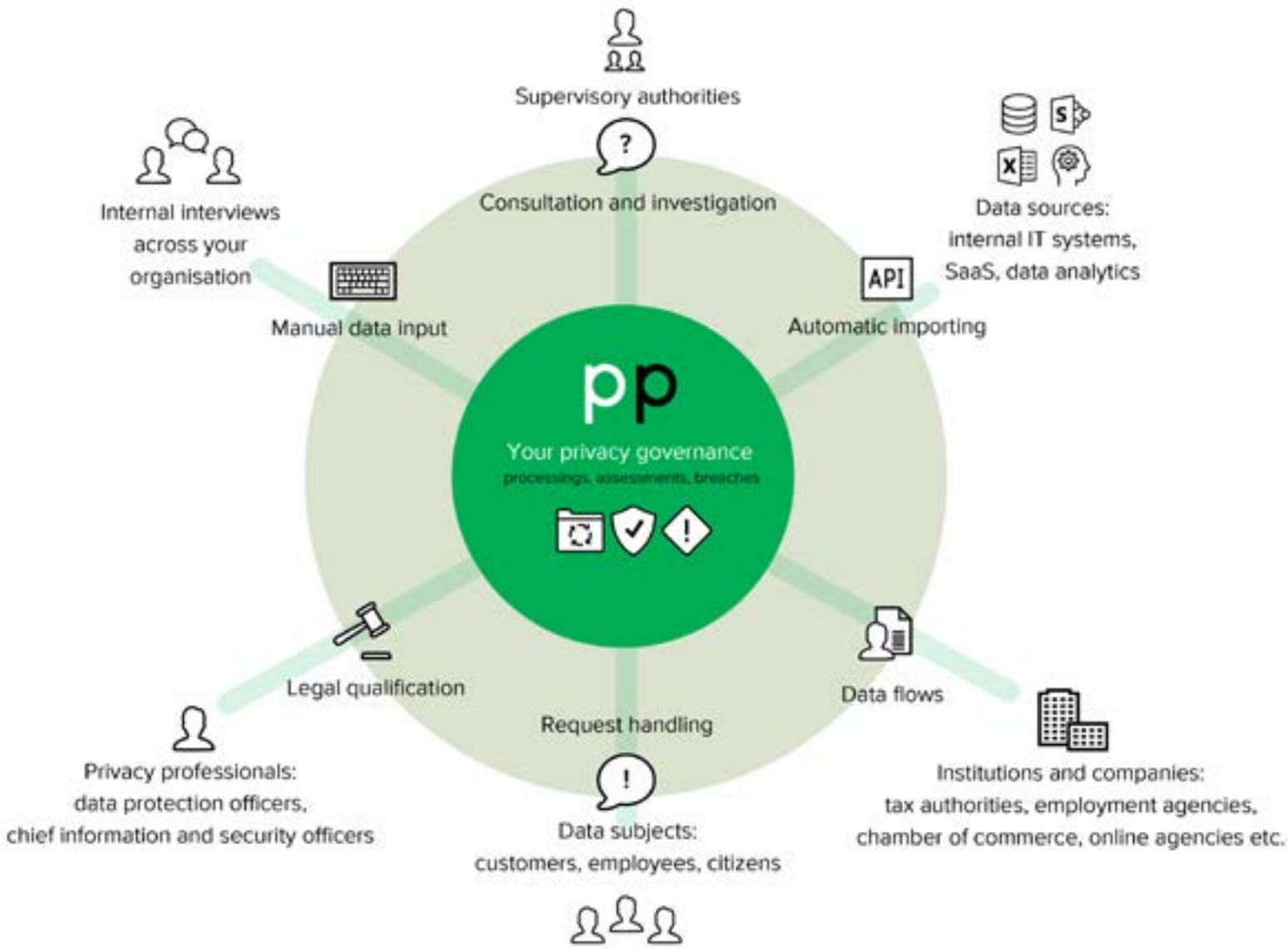
3

Inventory sources

This step is a mixed bag. Why? Because data processing is not only about IT, but also about people. In the infographic, you'll find the relevant sources of information for your inventory at 2, 4, 8 and 10 o'clock. These concern, respectively:

- Data sources: systems in use in the broadest sense, such as your local applications, your network, SaaS services, data analytics and big data services. You should have an idea where you can get the inventory from, and how you might be able to automate it (providing e.g. API connections for parts of the inventory).
- Data flows: external stakeholders in the broadest sense, such as tax authorities, employment agencies, chamber of commerce and online agencies. These are stakeholders with which you exchange personal data and therefore should be taken into account in your inventory.
- Privacy professionals: internal stakeholders, such as privacy officers, security officers, business analysts etc. who can help establishing the appropriate legal qualification of processing activities. A correct qualification is crucial for the legitimacy of your data processing activities.
- Internal interviews: internal staff or external consultants may help in inventorying data processing activities, but first you need to determine who has to be spoken to in order to make the inventory.

Make sure.


Supervisory authorities
Consultation and investigation
Internal interviews across your organisation
Data sources: internal IT systems, SaaS, data analytics
Manual data input
API
Automatic importing
pp
Your privacy governance
processings, assessments, breaches
Legal qualification
Data flows
Request handling
Privacy professionals: data protection officers, chief information and security officers
Institutions and companies: tax authorities, employment agencies, chamber of commerce, online agencies etc.
Data subjects: customers, employees, citizens

Make sure.

4 Inventory processing activities

A data mapping exercise requires an overview of all processing activities. After inventorying above sources, it should be possible to start making this overview. It is a project on its own, requiring a lot of information about each activity, such as its purpose, a legal processing ground, and the categories of data subjects and personal data involved. Such an overview is obligatory under art. 30 GDPR in most circumstances.

5 Implement privacy governance policies

Proper privacy governance requires putting in place procedures that improve the degree of privacy compliance. These can be manifold, but a few ones to keep an eye on are:

- A collection of technical and organisational security measures helps to mitigate privacy risks and is required by art. 32 GDPR
- A procedure for deciding whether a processing activity needs a data protection impact assessment is implicitly required by art. 35 GDPR
- A procedure for registering and notifying data breaches is implicitly required by art. 33 and 34 GDPR
- In some cases, a DPO has to be assigned. Their role should be properly be embedded in the organisation structure, and sufficient independence should be guaranteed

In addition, your organisation needs to be ready to communicate with external stakeholders:

- A procedure is needed for responding to the many data subject rights under the GDPR such as the right to access, rectification, erasure, restriction of processing and the right of data portability
- Assuming that your organisation works with other controllers and processors, procedures need to be in place to guarantee appropriate contracting and collaboration
- A procedure is needed to responding to supervisory authority questions and investigations

6 Test if it works

Like with fire alarms and a real fire, you don't want to wait until the supervisory authority knocks on your door to practice your organisation's response. So stage a data breach, test your procedures and convince your colleagues that next time it could be for real. You'll probably find white spots, faulty procedures and a lot of room for improvement. That's the idea: learn from practising.

7 Maintain and keep maintaining

Obviously, maintaining your privacy landscape and accompanying governance is not a project that's finished at some point in time. After the initial inventory, you need to update on a regular basis to reflect the changes in your environment: new stakeholders enter, old ones leave, and new processing activities are considered.

PrivacyPerfect is a software tool allowing you to inventory and maintain the three obligatory registers under the GDPR: those for assessments, processing activities and breaches. These registers allow you to properly align with all stakeholders and comply with data subject requests and to respond to supervisory authority investigations.

Click here to become GDPR compliant

Make sure.

Watch our Video

Ask for a webinar

Contact us
info@privacyperfect.com
+31 10 310 07 40