PrivacyPerfect White Paper series (3)

How to make a data map

(art. 30 GDPR)

Article 30 of the General Data Protection Regulation (GDPR) requires organisations with 250 or more employees and organisations for which data processing is an important part of their business to provide an overview of their processing activities.

However, all organisations are obliged to provide information on processing activities on requests of the supervisory authorities and data subjects. Consequently, your organisation needs a clear overview of its processing activities, even if article 30 does not apply directly to your organisation. Such a clear overview can be reached through a data map.

This 'how to' White Paper helps you carry out a data mapping exercise for your own organisation. Data mapping is an activity that might require many disciplines to work together: people aware of the organisation, security specialists, privacy officers and lawyers.

PrivacyPerfect helps to keep track of the data mapping exercise, collaborate with your colleagues and facilitates the selection of legal grounds, and other things important to get the result of the data mapping exercise properly registered.

1. Establish the scope and phasing

First, you have to determine whether you want to do data mapping for the entire organisation, or just for one or more organisation entities. Phasing data mapping and planning the scope for each phase will help to get the work done. If your organisation has an HR department and a customer profiling business unit, the latter might attract more attention from a supervisory authority.

2. Determine the organisation structure

In the course of the data mapping exercise, you will have to inventory which organisation entities have which roles, e.g. which entity is the controller and which entity is the processor. For each organisation entity that will have a legal role, you should also add contact details.

PrivacyPerfect allows hierarchical organisation mapping. For instance, for each organisation entity, you can choose between the qualification 'legal entity' or 'department'.

3. Inventory all applications and services in the organisation

Although a processing activity is not necessarily bound to a single 'system' or software application, in general it is good practice to have a list of all software in use – both local application software and web applications. If they are in use, the odds are quite high that personal data is being processed with them. Once you have the list, you can add them into PrivacyPerfect in order to have them available during the processing inventories.

PrivacyPerfect helps you with a bulk import into the system if the list of applications is long.

4. Determine which processing activities are executed where

A typical processing activity has a thematic 'coherence' that sets it apart from other processing activities. For instance, in an HR department, a salary administration is a processing activity. So is an employee performance programme. In a marketing department, a repetitive e-mail marketing campaign is probably a single processing activity in your data map. However, if you start a big data analysis for e-mail marketing, that will probably constitute a processing activity on itself.

5. Ask your colleagues to fill in the article 30 form for each processing activity

PrivacyPerfect has a form to enter all information needed for an article 30 GDPR compliant processing activities register. You can use it to ask other colleagues in your organisation to contribute to the inventory.

We have tried to make the form as user-friendly as possible, but users might need clarification of the different form fields from time to time. Therefore, we provide information that helps people without specific personal data protection knowledge to fill in the form.

Upon request, we can provide a comprehensive explanation of all the form fields.

6. Double check the information in the form

Once your colleagues have filled in the forms for the different processing activities, you have to determine if the descriptions are valid. Additional questions for verification you might have to ask are:

- Check if the interpretation of the stakeholder roles has been correctly done and thus if the legal roles are assigned to the right organisation entities.
- Are you sure all personal data items used in the processing activity have been identified?
- Are data sources properly identified and all relevant characteristics set?
- Have the correct legal grounds been selected? Do they match the personal data types processed and the jurisdictions involved? You can use the risk view in order to identify such problems as well.

It is generally good to take a critical view of the inputs of business users, as the subject matter is complex and it is easy to forget things or make the legally incorrect decisions in classifying activities.

7. Is everything complete?

It is not easy to assess whether the inventories are complete, but you can use a number of rules of thumb to investigate:

- Check for any gaps in the privacy records. There may be a good reason not to fill in a certain field, but it might also be oversight or a lack of knowledge.
- Check, on the basis of the various departments and roles in your organisation, if obvious processing activities might have been forgotten during the inventory. For instance, salary administration, pension, and employee monitoring are obvious candidates for an HR department.
- Check whether all the software applications from step 3 are actually in the processing records. If not, it might be that the application does not process personal data, but it might also be the case that someone forgot to mention that it is being used.
- Are the processing purposes explicit, specific and legitimate?
- Be critical about the match between purpose, legal grounds and the personal data actually processed. Are the personal data used really necessary for the specified purpose?

Do a regular check on of the existing inventories in order to assess whether they are still up to date. Once or twice a year might be a good frequency to ask the various organisation entities to give input on their ‘own’ processing records. If you start with a new processing activity, make sure to add this to your registration immediately.

PrivacyPerfect is here to help your organisation to become compliant with the GDPR. Please feel free to contact us for more information, we are more than happy if you want to join our webinars and learn more about our tool!

- Created and hosted in Europe
- Software as a Service (SaaS)
- Advanced visualisations
- Easy-to-use templates
- Multi-lingual software
- Transparent pricing
- Security by design
- Flexible reporting

Transparency **Compliance** **Accountability**

Watch our Video

Ask for a webinar

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

Please be aware that this White Paper may not be considered as legal advice and that, although we have done the utmost to check the correctness of our texts, we cannot be held responsible in any way for possible mistakes or errors. This White Paper is meant for informational purposes only and not for the purpose of providing legal advice. Please contact an attorney or a legal consultant to obtain advice with respect to any particular issue or problem related to the subject matter of this White Paper. Although PrivacyPerfect takes the utmost care in producing all its information leaflets, including this White Paper, PrivacyPerfect cannot guarantee their correctness. PrivacyPerfect does not accept any liability on actions taken on the basis of such materials, including this White Paper.