



How to get an overview of your company's personal data

On May 25, 2018, a new European privacy regulation called The General Data Protection Regulation (GDPR) will come into effect.

Companies that fail to comply with this new regulation could face fines of up to 20 million Euros or 4% of the global revenue, whichever is bigger.

As a part of becoming GDPR compliant, it's important to map where all the personal data in your entire business comes from, where and how this information is stored and document what you do with the data.

Personal data can comprise, for example, IP addresses, geographical locations, gender, income, interests and website visited.

Personal data checklist

Use this list of questions to help you analyze the personal data that you have stored in your systems.

A good way to collect this data is in an Excel spreadsheet, but, of course, there are numerous other ways you can collect the data.

What is most important is that you answer these 13 questions for every type of personal data that you collect.

- 1 What is the personal data that is being collected?**
Provide a description of the types of personal data being collected, for example, names, addresses, emails phone numbers. Remember to include more personal information such as date of birth, personal ID number and any other additional data that identifies a person.
- 2 What is the purpose for collecting the personal data?**
Explain why you are collecting this information. For example, if you really need the date of birth, you need to be able to explain why and what you need it for.
- 3 What is the legal basis?**
Explain the company's legal basis for collecting this information. Refer to Article §6.1A-F of the GDPR directive for more information.
- 4 What is the source of personal data?**
Provide information about how you are obtaining the personal data. Are you getting the data via web forms, business cards which are collected in different settings, integrations with other systems, etc.
- 5 What is the classification?**
Classifications of personal data can be confidential, anonymous, sensitive, etc. For example, sensitive data could be salary or bonus information. Note that all personal data which is sensitive and confidential will need to have extra security measures.



6 How long is the personal data stored?

Note down how long you will keep the personal data. The period of time you plan on keeping the personal data can be dependent on the purpose and the legal basis. For example, salary information can be kept as long as required by the Accounting and Archiving Act.

7 Who can access the personal data?

Note down who has access to the personal data. For example, payroll people can access the payroll system, HR people can access HR information, Sales people can access customer information.

8 Is the personal data being transferred to other countries?

Personal data should preferably stay in the EU. Otherwise, note if the personal data is being transferred and for what purpose.

9 What system are you storing the information in?

You will most likely have a separate system for payroll and for your customer information. You will need to note down the system used for personal data. You should also note if the system you are using is a cloud-based system.

10 Has explicit consent been given to use the data?

Explain if the person has voluntarily given you his personal data for marketing communications purposes. Explicit consent is particularly important when you are storing and processing personal data about persons you do not have an active customer relationship with.

11 Has the data subject been informed about data being collected?

This kind of information is usually provided in the customer contract, at a start-up meeting and/or in the privacy statement on your website.

12 Is this personal data shared with third parties and why?

Indicate what type of information is provided and which third parties are recipients, if the information is disclosed to others.

If you are using the personal data for marketing purposes, you will need to state whether or not the data is collected and shared with third parties in your privacy statement and contractual documents with customers.

13 How is the information secured?

Describe the security measures for protecting the personal data. This is especially important if you have sensitive data stored where you are the controller and responsible for keeping this data safe.

Next Steps

Once completed, this checklist will also help you determine what data you want to keep. You shouldn't keep more information than is necessary and you should get rid of data that isn't used.

If your business collects a lot of data without any relevant purpose or need, you won't be able to do this in a GDPR world.

Mapping your company's data and determining what data you need to keep are a few of the first important steps to becoming GDPR compliant.

You'll also need to put security measures in place to safeguard your data, and develop routines for accessing, deleting and archiving personal data.

If you have any questions for how SuperOffice CRM can support you on your GDPR journey, please contact us at info@superoffice.com

Disclaimer: The content in this guide is not to be considered legal advice and should be used for information purposes only.