European Commission

Seven steps for businesses

to get ready for the General Data Protection Regulation

Justice and Consumers

Who is this for?

This guide aims to help those companies that do not handle personal data as a core business activity, such as SMEs that mainly deal with personal data of their employees or have lists of clients and customers. This includes for instance traders or shops, such as a bakery or a butcher, or service providers like architects. This guide highlights the few steps that need to be taken to get ready for the GDPR.

Personal data is any information that relates to an actual living individual (not legal entities). This includes, for instance: name, surname, home address, e-mail address or location data from the map on your mobile. Typically, this would be the case of the data you might hold on your employees, your clients or your suppliers.

The less risk your activities pose to personal data, the less you have to do

Apply key principles:

- **collect personal data with clearly defined purpose, and don't use them for something else** (if you tell your clients to give you their email so they can get your new offers or promotions, you can't use this email for anything else or sell it to another business).
- **don't collect more data than you need** (if you do home delivery, you need e.g. an address, a name on the buzzer, but you don't need to know if this person is married or single) - simply be mindful of the personal data under your control.

STEP 1 — CHECK THE PERSONAL DATA YOU COLLECT AND PROCESS, THE PURPOSE FOR WHICH YOU DO IT AND ON WHICH LEGAL BASIS

You have **employees**; you are processing their personal data based on the employment contract and based on legal obligations (e.g. reporting to tax authorities / social system).

You can manage a list of **individual customers**, for instance to send them notice about special offers/adverts if you obtained consent from these customers.

You don't always need consent. There are cases when individuals will expect you to process their data. For instance, as a pizza merchant you can process the delivery address to advertise one of your new products. This is called a legitimate interest. You must inform individuals about your intended use and stop processing such data if they tell you to do so.

If you manage a list of **suppliers** or **business clients**, then you do it based on the contracts you have with them. The contracts are not necessarily in a written form.

STEP 2 — INFORM YOUR CUSTOMERS, EMPLOYEES AND OTHER INDIVIDUALS WHEN YOU COLLECT THEIR PERSONAL DATA

Individuals must know that you process their personal data and for which purpose.

But there is no need to inform individuals when they already have information on how you will use the data, for instance, when a customer asks you to do a home delivery.

You also have to inform individuals on request about the personal data you hold on them and give them access to their data. Keep your data in order, so when e.g. your employee asks you about what sort of personal data you have, you can provide it easily with no extra hassle.

STEP 3 — KEEP THE PERSONAL DATA FOR ONLY AS LONG AS NECESSARY

Data on your employees: as long as the employment relationship and related legal obligations.

Data on your customers: as long as the customer relationship lasts and related legal obligations (for instance for tax purposes).

Delete the data where it is no longer necessary for the purposes for which you collected it.

STEP 4 — SECURE THE PERSONAL DATA YOU ARE PROCESSING

If you store this data on an **IT system**, limit the access to the files containing the data, e.g. by a password. Regularly update the security settings of your system.

(Note: the GDPR does not prescribe the use of any specific IT system)

If you store physical documents with personal data, then ensure that they are not accessible by unauthorised persons; lock them in safe or a cupboard.

STEP 5 — KEEP DOCUMENTATION ON YOUR DATA PROCESSING ACTIVITIES

Prepare a short document explaining what personal data you hold and for what reasons. You might be required to make the documentation available to your national data protection authority when it requests it.

Such documents should include the information listed below.

INFORMATION	EXAMPLES
The purpose of data processing	Alerting customers about special offers / providing home delivery; paying suppliers; salary and social security cover for employees
The types of personal data	Contact details of customers; contact details of suppliers; employees' data
The categories of data subjects concerned	Employees; customers; suppliers
The categories of recipients	Labour authorities; tax authorities
The storage periods	Employees' personal data until the end of the employment contract (and related legal obligations); customers' personal data until the end of the client/contractual relationship
The technical and organisational security measures to protect the personal data	IT system solutions regularly updated; locked cupboard/safe
Whether personal data is transferred to recipients outside the EU	Use of a processor outside the EU (e.g. for storage in the cloud)

STEP 6 — MAKE SURE YOUR SUB-CONTRACTOR RESPECTS THE RULES

If you sub-contract processing of personal data to another company, use only a service provider who guarantees the processing in compliance with the requirements of the GDPR (for instance security measures). Before you sign a contract, check if they have already changed and adjusted to the GDPR. Put it in the contract.

STEP 7 — CHECK IF YOU ARE CONCERNED BY THE PROVISIONS BELOW

> To better protect personal data, organisations might have to appoint a Data Protection Officer (DPO). **However, you don't need to designate a Data Protection Officer** if processing of personal data isn't a core part of your business, is not a risky processing and your activity isn't at a large scale;

For example, if your business only collects data on your customers for home delivery, you do not need to appoint a DPO.

Even if you need to make use of a DPO, he/she could be an existing employee tasked with this function in addition to his/her other tasks. Or it could be an external consultant; the same way many organisations use external accountants.

> **You normally don't need to carry out a Data Protection Impact Assessment**

Such an impact assessment is reserved for those that pose more risk to personal data, for instance they do a large-scale monitoring of a publicly accessible area (e.g. video-surveillance).

If you are a small business managing employees' wages and a list of clients, you do not need to carry out a Data Protection Impact Assessment for those processing operations.

Fines

The data protection supervisory authorities are empowered to sanction infringements of the data protection rules. They can adopt corrective measures (such as an order or a temporary suspension of the processing) and/or impose a fine.

Their decision to impose a fine must be proportionate and based on an assessment of all the circumstances of the individual case.

If they decide to impose a fine, the amount of the fine will also depend on the circumstances of the case, including the gravity of the infringement or if the infringement was intentional or negligent. They will also take your attitude and intentions into account.

If you wish to obtain more information:

1. Visit the European Commission's online guidance on data protection reform – available in all EU languages:

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

2. Consult your national Data Protection Authority:

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080

IMPORTANT NOTICE

The information in this guide is intended to contribute to a better understanding of EU data protection rules.

This is intended purely as guidance – only the text of the General Data Protection Regulation (GDPR) has legal force. As a consequence, only the GDPR is liable to create rights and obligations for individuals. This guidance does not create any enforceable right or expectation.

The binding interpretation of EU legislation is the exclusive competence of the Court of Justice of the European Union. The views expressed in this guidance are without prejudice to the position that the Commission might take before the Court of Justice.

Neither the European Commission nor any person acting on behalf of the European Commission is responsible for the use which might be made of the information in this guide.

As this document reflects the state of the art at the time of its drafting, it should be regarded as a 'living tool' open for improvement and its content may be subject to modifications without notice.

Publications Office

Luxembourg: Publications Office of the European Union, 2018

Print	PDF
ISBN 978-92-79-85367-8	ISBN 978-92-79-85390-6
doi:10.2838/360	doi:10.2838/589038
DS-02-18-544-EN-C	DS-02-18-544-EN-N