Seven steps for businesses to get ready for the General Data Protection Regulation
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.

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.

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

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

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.

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.

The technical and organisational security measures that you need to put in place 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. Their decision to impose a fine must be proportionate and based on an assessment of all the circumstances of the individual case.

If you do not designate a Data Protection Officer (DPO), however, you don’t need to provide a special function for that purpose. Or it could be an external consultant; the same way many organisations use external accountants.

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.

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.

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.

They will also take your attitude and intentions into account. Their decision to impose a fine must be proportionate and based on an assessment of all the circumstances of the individual case.
If you wish to obtain more information:

1. Visit the European Commission’s online guidance on data protection reform – available in all EU languages:
   europa.eu/dataprotection

2. Consult your national Data Protection Authority:
   edpb.europa.eu/about-edpb/board/members_en

**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 following information.

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.