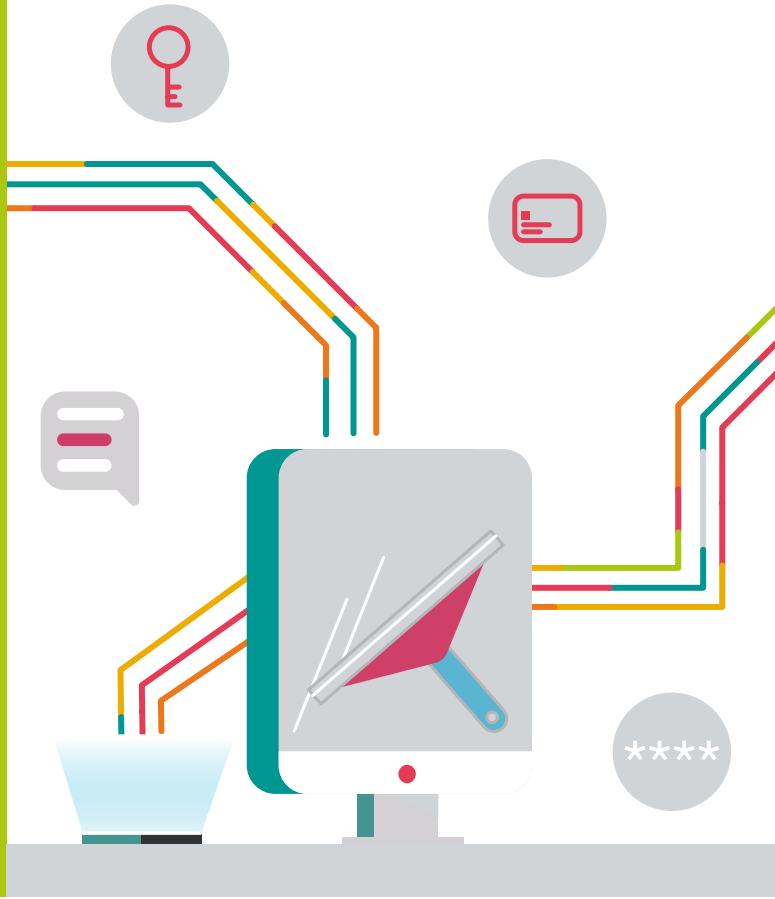
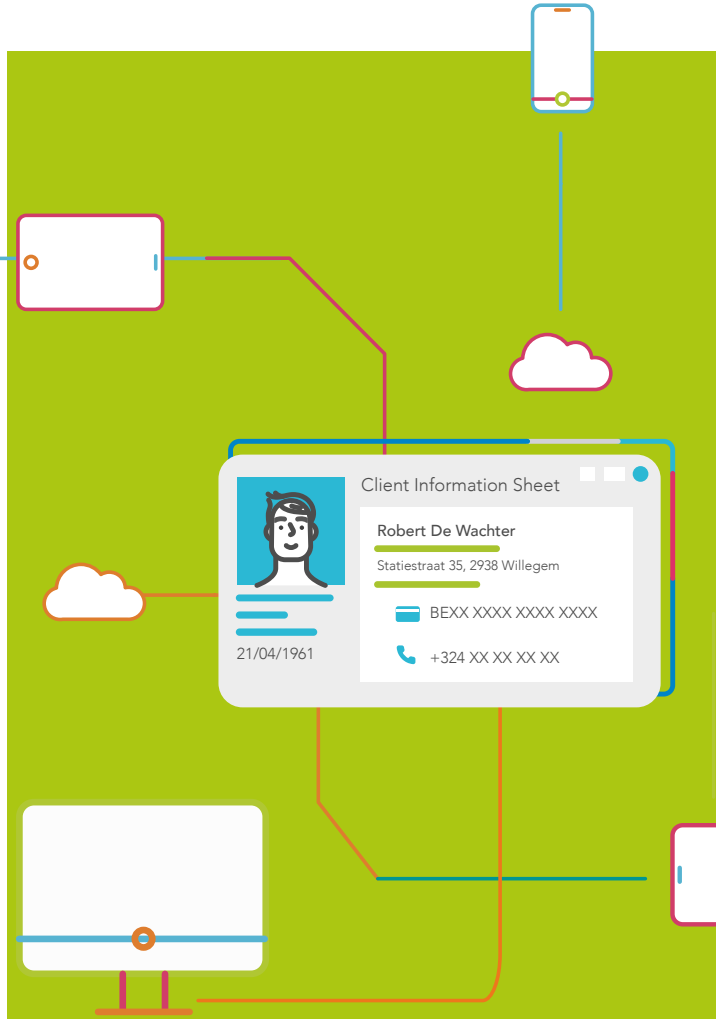
GDPR
DATA CLEAN-UP

DATA PROTECTION IS
ALSO YOUR JOB.
TIME FOR A CLEAN-UP!



CYBER SECURITY
COALITION.be



In this brochure, we will explain how to clean up personal data that you save - on your laptop, mobile phone or in the cloud - when performing your job.

Why is a clean-up so important?

Personal data are everywhere

You would be surprised how many personal data you keep on different devices and in various apps (for example on your laptop, smartphone or tablet for professional use, and on USB sticks and external hard drives) as part of your work. We send and save personal data in our mailboxes, on apps, in the cloud, etc. every day.

A genuine and significant risk

Just like other data, personal data are vulnerable to loss, theft or a violation of the confidentiality requirement. If an organization loses personal data or they are stolen, this can have very serious consequences. A data breach has consequences for the persons concerned (violation of privacy) as well as for the company (reputational damage, fines, loss of customers). Moreover, the law requires to delete personal data when the objective of the processing is achieved.

Everyone is involved

Data protection is the responsibility of your company or organization. However, you can also make a significant contribution as an employee. By correctly dealing with personal data, you protect others and help your organization preserve its good reputation. Treat the personal data of others as you would want your own data to be treated.

Data protection: a brief introduction

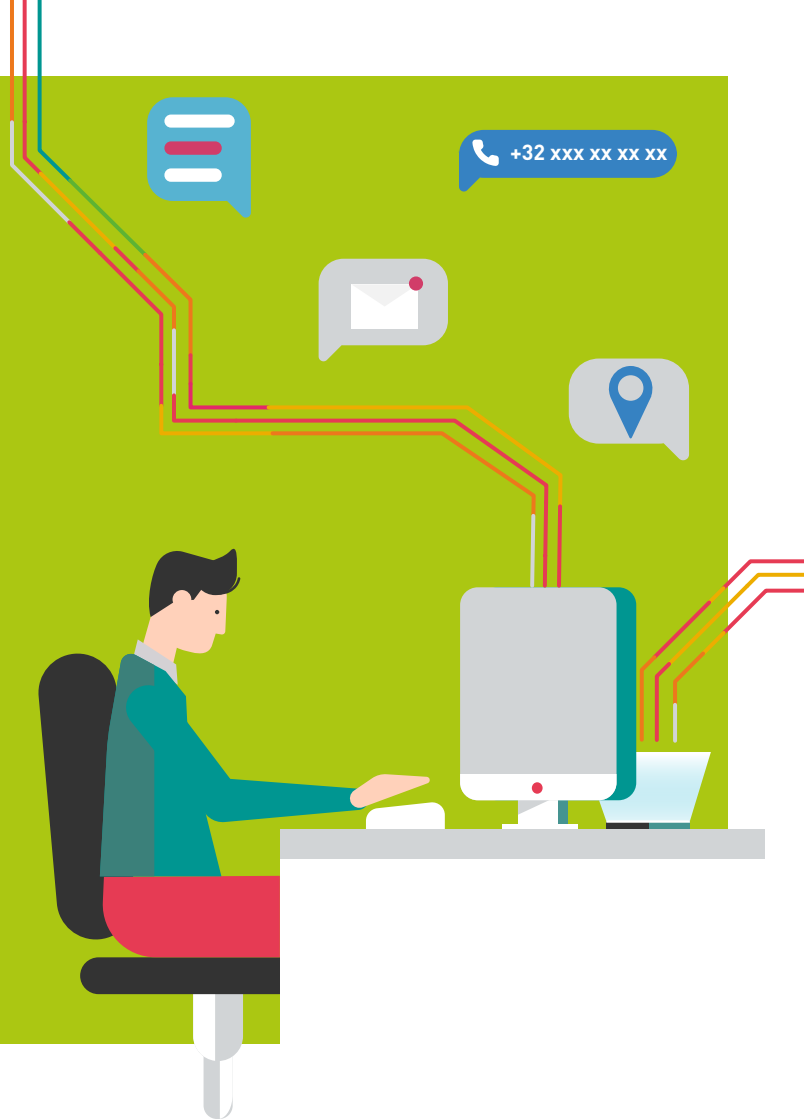
GDPR
The GDPR (General Data Protection Regulation) has been in force since 25 May 2018. This European legislation requires that all enterprises and organizations take the necessary measures to protect personal data.

Basic principles
The GDPR determines how we collect, process and store personal data lawfully and safely. A few of the basic principles are that personal data can only be collected for specific, legitimate objectives and that we cannot store the data for longer than necessary. We must also ensure that personal data are processed safely.

What do we mean by personal data?
These are data that identify a person or may be used to identify a person either directly or indirectly. Names, telephone numbers and e-mail addresses are obvious examples, but personal data also include payment information, photographs, evaluations and location data.

There is also a specific category of sensitive data that requires special attention. This concerns medical details, political opinions, religious convictions, etc.

Whom does it concern?
The GDPR is applicable to all personal data that is collected, processed and stored within your organization. It may concern details in relation to customers, prospective customers, employees and suppliers.



How does one start?

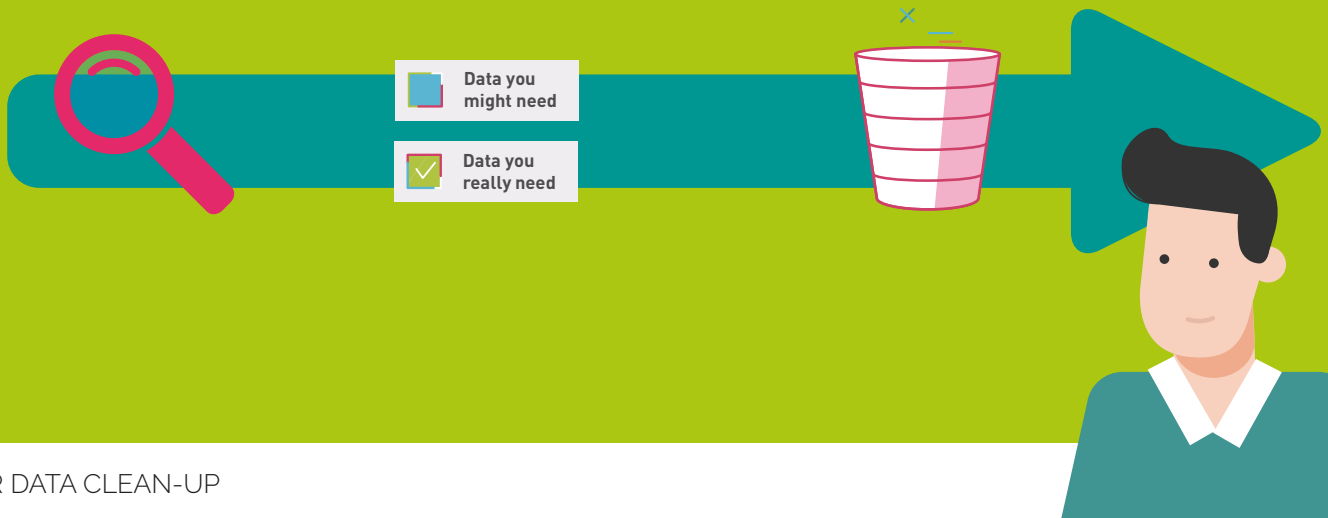
Are you ready to clean up your personal data?

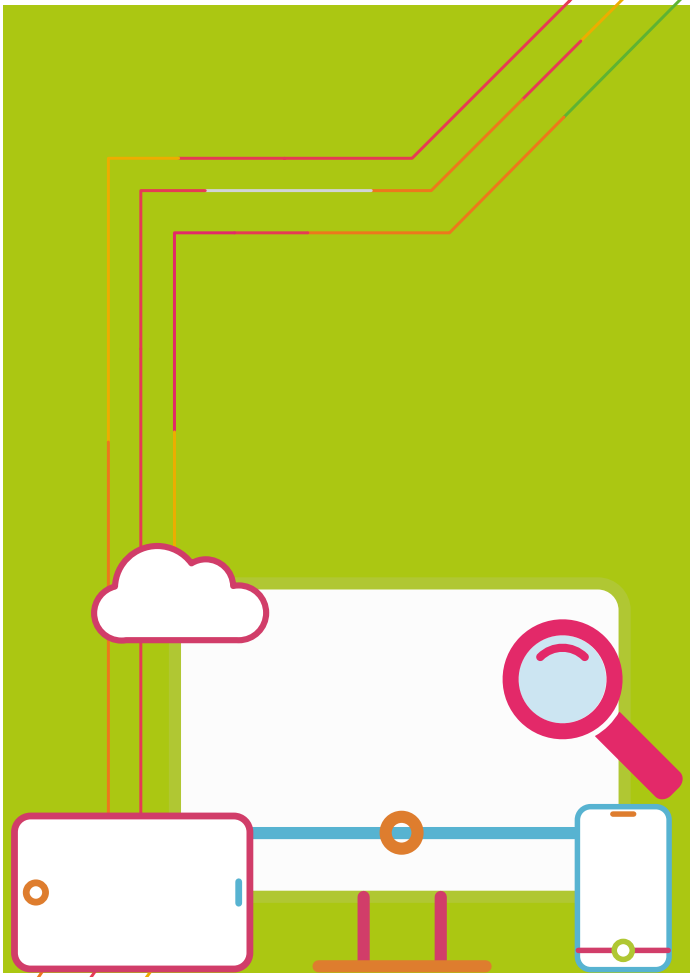
You can get started right away with our step-by-step guide!

Step 1
identify and localize

Step 2
familiarize yourself with the retention periods

Step 3
take action





Step 1: identify and localize

Before you can start the clean-up, it is essential to think about which personal data you store when performing your job and where you save it.

- **Identify the personal data** that you store. This could be data from customers, suppliers, colleagues, job applicants, etc. Think of obvious personal data like names, e-mail addresses and phone numbers, but do not forget that photographs, IP addresses, etc. are also considered as personal data. Depending on the sector that your organization is active in, you might also store sensitive data like medical information.

  – Your organization's **processing register** can serve as a tool. It contains an inventory of all activities related to data processing within your organization. This document is required for organizations with more than 250 employees or with high risk processing.

- **Find out where you store the personal data.** Most organizations use storage systems that are hosted **locally or in the cloud**, e.g., the central disk space, a CRM system, an intranet, wiki or other online collaboration platforms, etc. Do not forget your professional mailbox and reflect on other apps that you use for your job. Perhaps you store personal data **locally on your professional devices**, such as your laptop, smartphone, a USB stick or external hard drive.

- Check whether you store personal data on **other systems or devices**. Do you occasionally export documents from an app or make copies of documents that contain personal data? Where and how do you store back-ups?

! Avoid duplicating personal data.
This increases the risk of incidents, including unauthorized access by others.

- Check which rules your organization follows regarding duplicating personal data (data retention policy, Bring Your Own Device policy, ...)
- Data that are duplicated for convenience must be deleted immediately after use, since the retention period only applies to the original file.

  – Example: An employee exports customer e-mail addresses from the central CRM system to an Excel file and then uploads this list to an e-mail marketing program. As soon as this action is complete, the employee must delete the exported list.

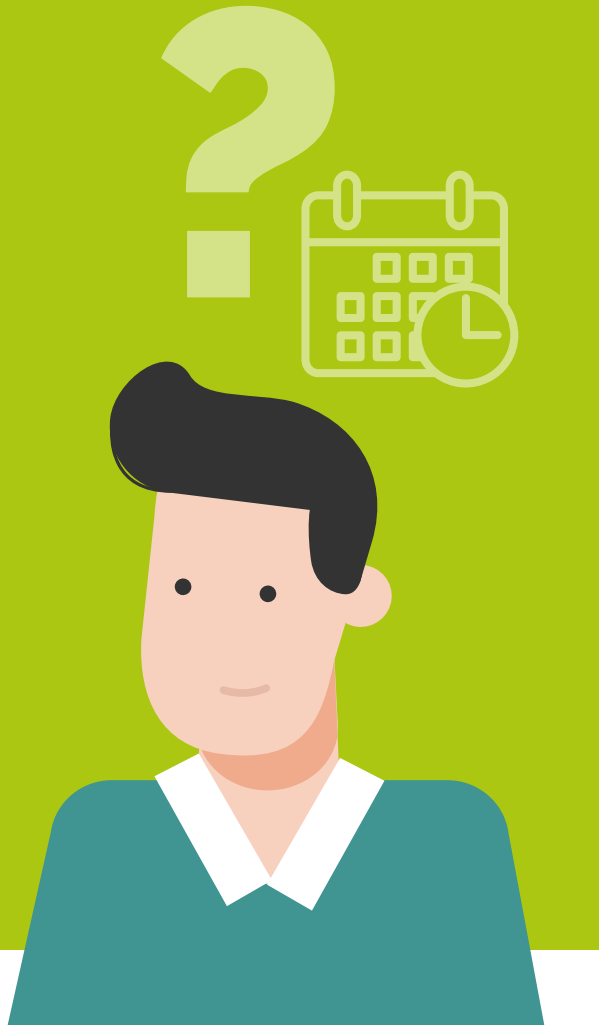
- Check whether you store personal data for professional use on your **own devices authorized for professional use**. You must also perform a data clean-up on these devices!

Step 2: familiarize yourself with the retention periods

Now that you have mapped the personal data that you store, it is important to know whether you can still keep it. As a basic rule, you can only store personal data as long as this is strictly necessary. But how long is that? Some retention periods are stipulated by law; others are determined by your organization. Once you know the applicable retention periods, you know which personal data you can delete in the next phase.

Retention periods within your organization or company
Gather information relating to the retention periods that your organization has established for every personal data processing operation.

- Every processing operation has an identified duration, or must as a minimum, satisfy criteria that determine when the objective is reached.
- Organizations must revise their retention periods regularly. The end of a retention period can be triggered by certain events.
  - Example: An organization must delete the personal data of a job applicant as soon as it is clear that this person will not be hired. If the organization wishes to store the CV of the job applicant, for example, to establish a shortlist, then that organization must let the job applicant know and give him the right to object.



- Some retention periods are based on legal obligations and have been established in **Belgian law**.

Where can I find this information?
Information relating to the retention periods that your organization has established, can be found in the **privacy policy or in the personal data protection guidelines of your organization**. For more information, contact the controller or Data Protection Officer (DPO) in your organization.

Remember!
- If you do not have a legal obligation, **only store the personal data that are needed to do your work** and ensure that the task falls within the permitted uses. When in doubt, ask for advice from your organization's controller or DPO.
- Do not keep unnecessary copies of personal data.

Step 3: take action

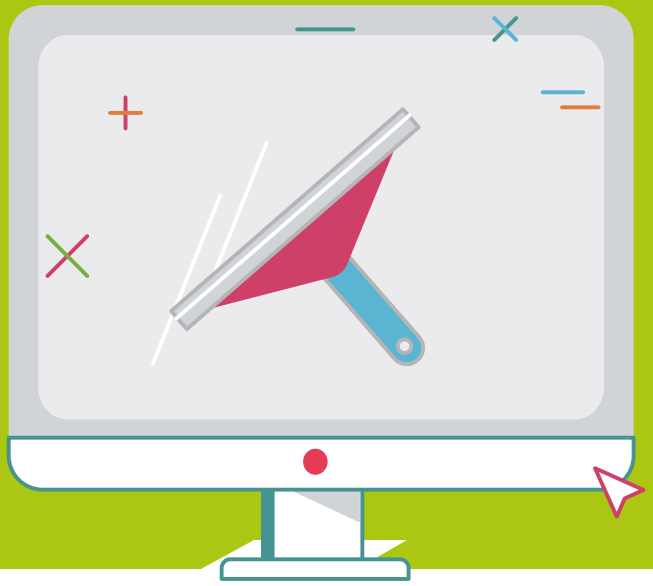
Now that you know the retention periods, you can get to work. In this step, you delete the personal data or store it safely.

Delete all personal data the retention period of which has expired or that are no longer needed for your job.

- If your organization has central IT systems, your IT department may have already implemented **automatic storage or deletion** to satisfy the retention periods.

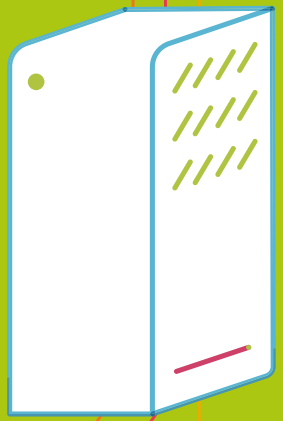
  – Example: video images can be kept for a maximum of one month. The system automatically recognizes dates and deletes images older than one month.

- If the systems that you use do not allow an automatic removal process, check whether there is a **manual procedure** that you can use regularly.
- Make sure that **duplicated personal data** are deleted unless they serve as a back-up for the organization.
- Do not forget to delete personal data stored on your **personal devices**.



You can archive personal data in specific cases..

- In some cases, you must store certain personal data, even if you no longer need them to perform your job. For example, data that could be necessary for a claim (legal procedure) or accounting justification. Make sure that you **archive these personal data safely and restrict access to them**. When in doubt, ask for advice from your organization's DPO.



Encrypted server

Safely store personal data that are still necessary.

- First and foremost, **access to personal data must be limited** to people who need the data for their work.
  - Example: only make employment contracts accessible to the HR department, by storing them in a specific, restricted location.
- To prevent unauthorized people from gaining access to your devices or tools in the event of loss or theft, you must limit the access to your devices or tools. You can do this by using a **strong password**.
- If you want to keep these data beyond the necessary retention period, for example for statistical or test purposes, it is necessary to **anonymize** them.

Practical tips

Cleaning up personal data requires time and effort. Here are a few more handy tips:

- **Work systematically and regularly.** Follow the three-step plan and allow sufficient time to perform each step.
- **Work together with your colleagues.** If you work in a large company, then you can organize the data clean-up with colleagues in your department.
- **Start with one device or tool.** For example, start by cleaning up your professional mailbox.
- **Clean up your personal devices too.** If you use your personal smartphone for business purposes, delete old professional photos and personal data that you shared in messaging apps, etc.
- **Use strong passwords.** Protect the personal data that you still need with strong passwords.
- **Avoid using USB sticks or external hard drives for storing personal data.** If you do use them, make sure that you always encrypt the data.
- **If there are private files on your professional devices,** you must perform the data clean-up yourself; this is in your own interest. Look in "My documents" or "My photos" if you store sensitive data in these folders.

List of interesting websites

dataprotectionauthority.be

edpb.europa.eu

Safeonweb.be

CYBER SECURITY
COALITION.be

www.cybersecuritycoalition.be

This brochure has been realized thanks to the cooperation of Belnet, MIVB/STIB, Hoge Raad voor de Zelfstandigen en de KMO/ Conseil Supérieur des Indépendants et des PME and AG Insurance.