Top 10 common pitfalls

when handling people's data, and practical steps to mitigate

THE OFFICE OF THE
Data Protection Authority

THE OFFICE OF THE
Data Protection
Authority

1. Storing personal data

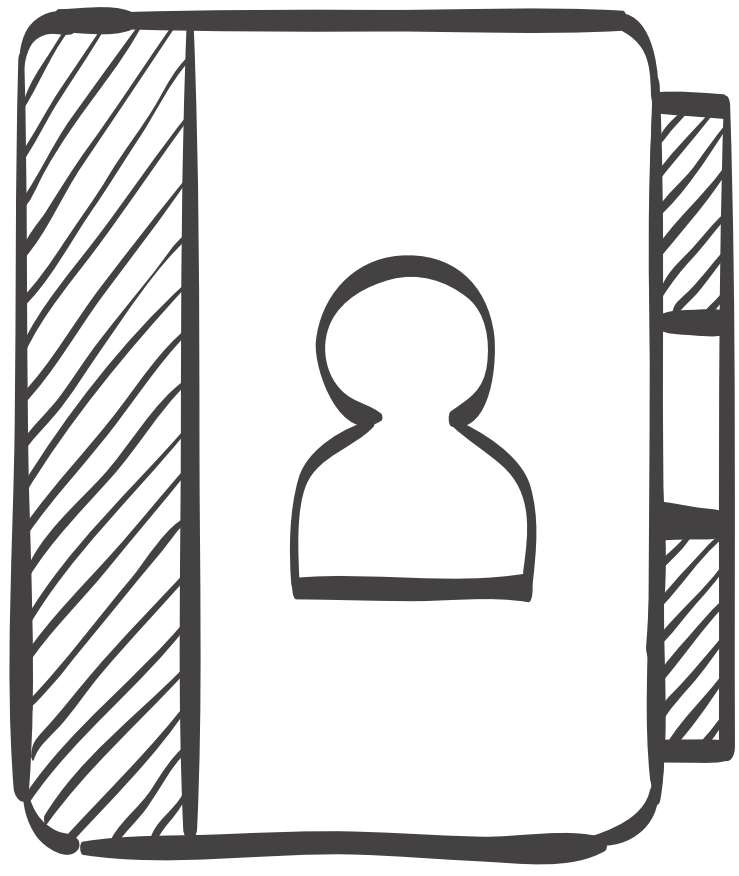
You have to keep personal data safe and make sure no one has access to it **without your authorisation**. Simple security measures could include storing paperwork in a locked cabinet and putting strong passwords on all your devices. If you've got sensitive personal information, you must take **extra steps** to protect it from getting lost, damaged or stolen. You also must make sure no-one accesses or alters it **without permission**.

Staff shouldn't store paperwork on their desk or in their workspace. It's useful to make a **policy** about this to help reduce the risk of sensitive information being left unattended.

2. Remote working

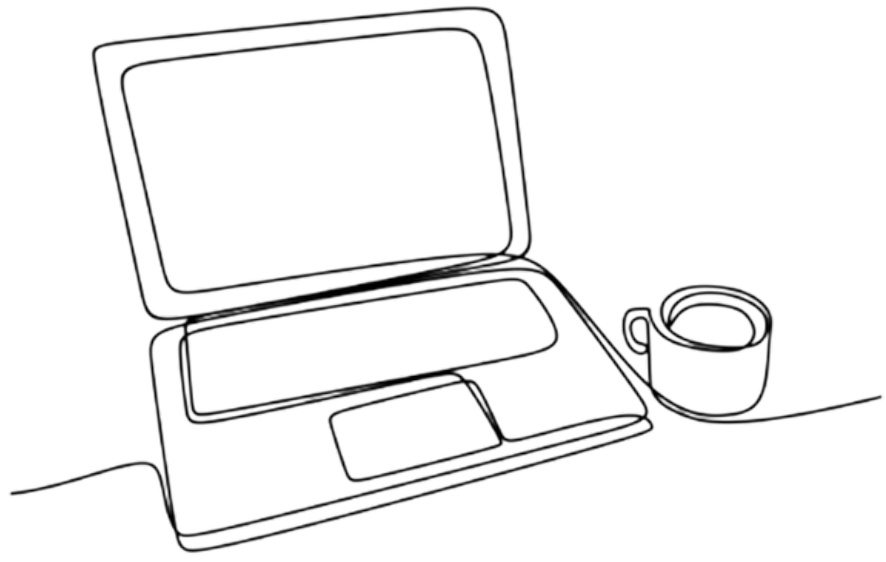
Staff should understand how they should handle personal data if they work off-site. If you use mobile devices, put **technical measures** in place to secure them, such as two-factor authentication. If staff use their own devices, have a **security policy** in place that addresses that.

3. Out of date address book



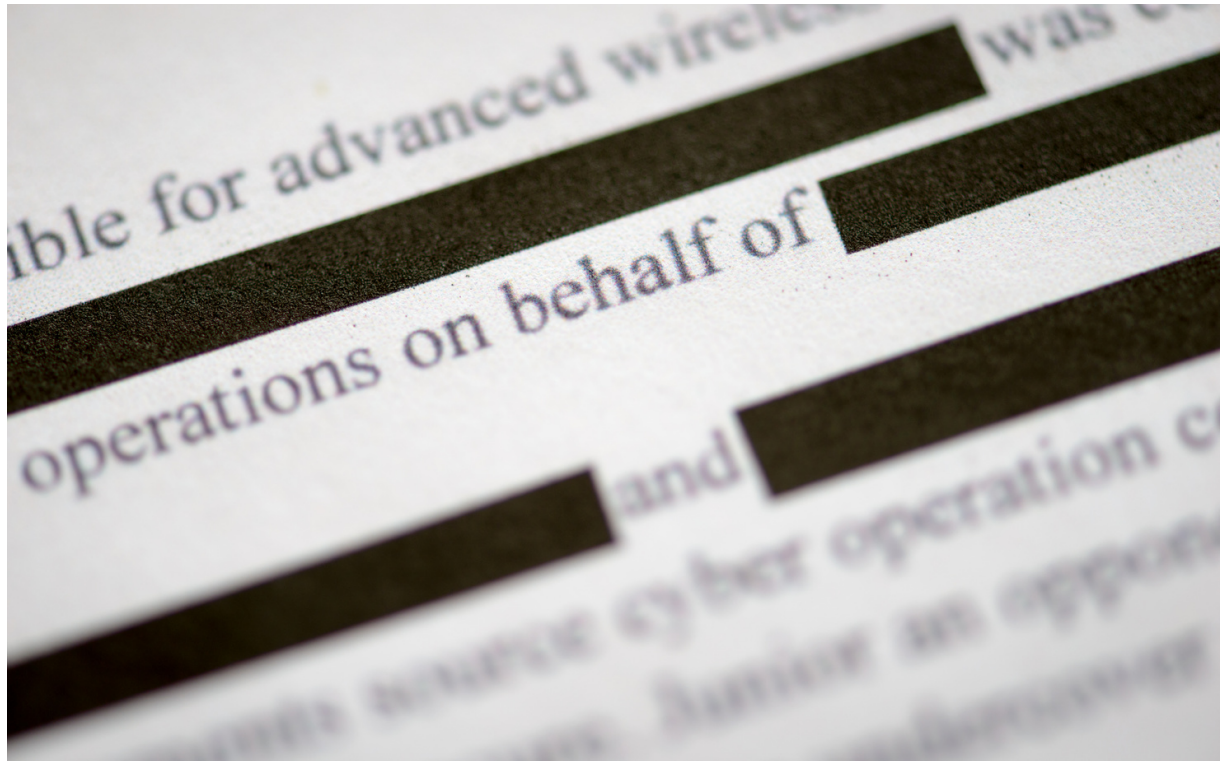
Ask your customers, clients or members regularly, **to let you know** if they change their address or other contact details. This helps to reduce the risk that an address you have on file for them is incorrect.

4. Unclear and inconsistent naming of documents



If you name your documents using the **same format** every time, it makes it easier to find the right one. It’s also less likely that someone will attach the wrong document to an email.

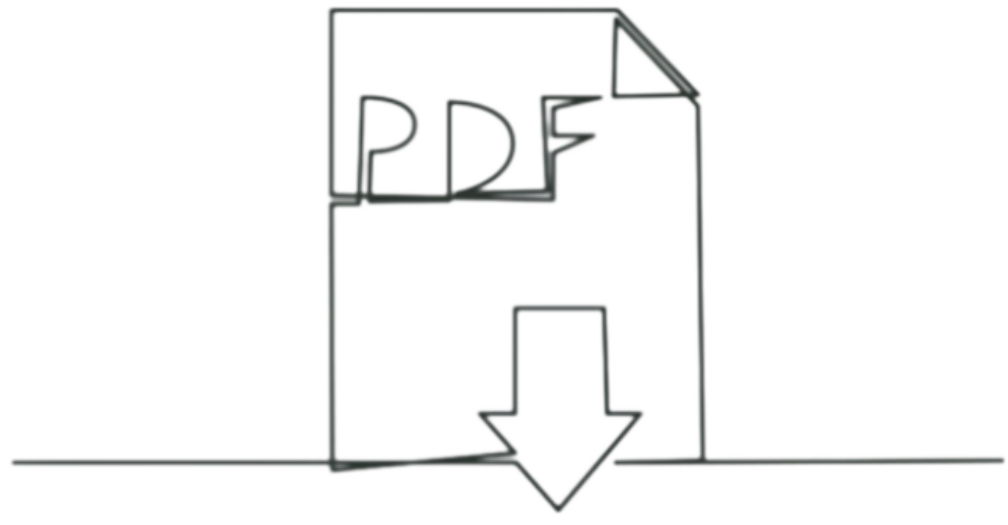
5. Redacting data



When responding to a subject access request, you will often need to send people copies of their data. This may mean needing to remove or redact information about **other** people. When doing this, **be thorough and check** the information can't still be seen.

Note: be careful when redacting data in Microsoft Word as we have seen instances where blocking text on Microsoft Word can be reversed even when converted to a PDF document. The safest method is to **remove the data** and **replace** with the word 'redacted' or similar.

6.Templates



If you use template documents, make sure you create a **new copy of it every time** and avoid overwriting a previous document.

Blank templates should be **stored separately** from pre-populated ones to avoid someone seeing this information by mistake.

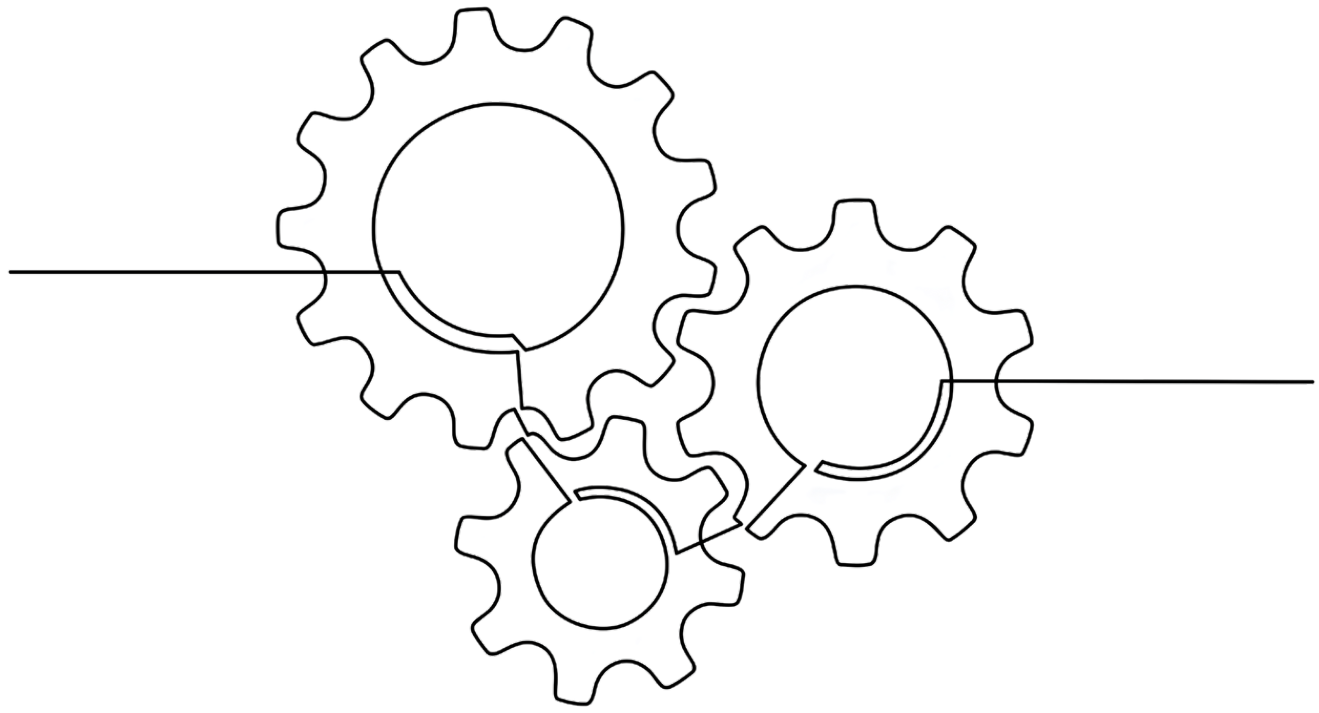
7. Access controls

Not everyone needs access to everything, so think about whether you can tighten your access controls so that staff **only have access to the personal data they need** to carry out their role.

8. Training of staff

Human error is still the most common cause of personal data breaches. Data protection is everyone’s responsibility, so make sure you give your staff the **training, support and resources** they need to get it right.

9. Disposal

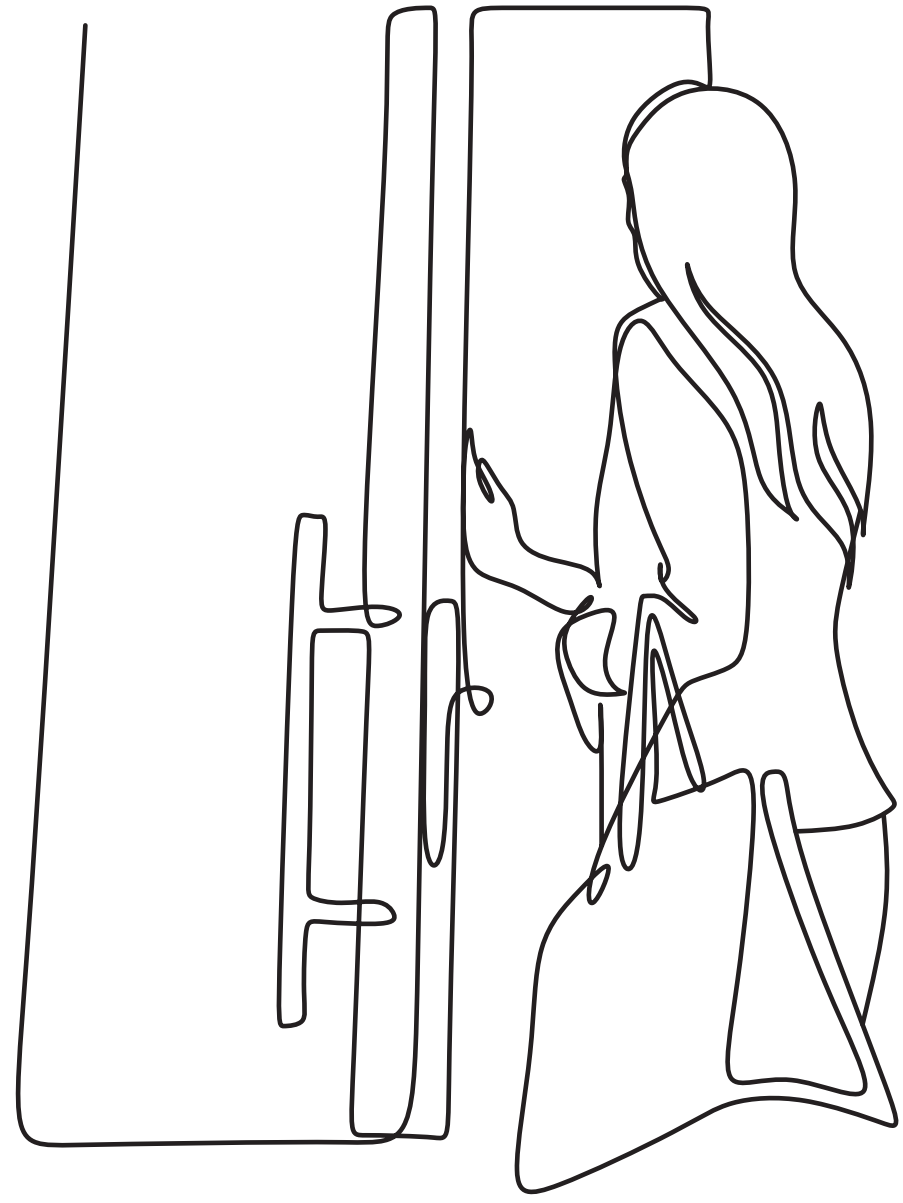


Before you dispose of anything that may have personal information on it, make sure it is **properly** destroyed.

For example, shred paper files and make sure you use software designed to **permanently** wipe data off devices.

Simply deleting the files does not fully erase data.

10. Ex-employees

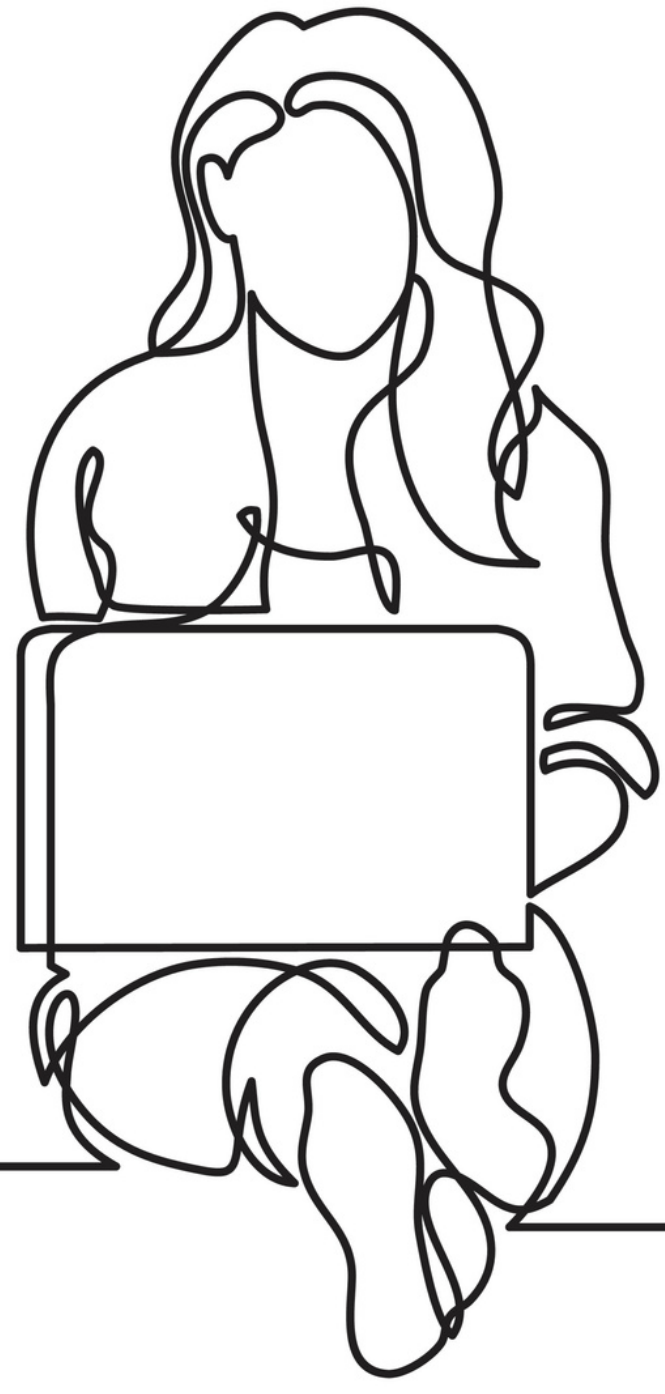


Ex-employees taking data with them is a common type of personal data breach.

You can use **clauses in employment contracts** to help stop ex-employees from soliciting customers whose information they had access to while employed by your business.

THE OFFICE OF THE

Data Protection Authority



visit odpa.gg for more