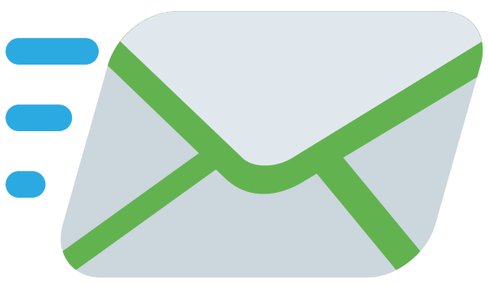
How to avoid five common breach scenarios

A **personal data breach** is likely if there is '*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*'.

Local entities who experience a breach are **legally obliged to report it to the ODPA** if the breach is **likely to pose a significant risk** to the person (or people) whose data has been affected: **odpa.gg/breach-reporting**.

Breach scenario: inappropriate action
A lack of staff training led to an employee **accessing and printing** clients' personal data without authority.
It may have been accidental and not malicious, but it is still a breach.

How to avoid this
Educating staff about what they **are and are not authorised** to do with the data they have access to should avoid this happening again.



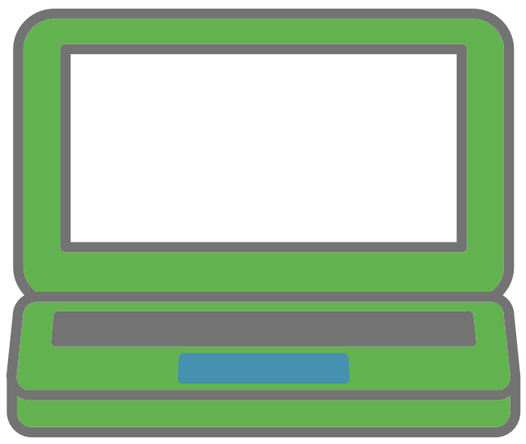
Breach scenario: email error
When replying to an email with several recipients, an **additional person was accidentally included** in the chain and received a number of messages and associated personal data that they were not authorised to have.
This was probably down to human error, possibly a typing mistake leading to an unintended recipient.

How to avoid this
Reminding staff to **slow down, double check recipients, and consider the consequences** of their actions before hitting the 'send' button should prevent this breach being repeated.

Breach scenario: mislaid data
An organisation posted out a client's **original** documents, containing personal data. They were **lost in the post and were never received** by the intended recipient.

In a large jurisdiction like the UK this information would be unlikely to be found by someone that knows the client. However, in the Bailiwick it is much more likely that personal data lost here could be found by someone that knows the person concerned. Once this kind of data is lost it may be impossible to recover and it is also not possible to be sure of the identity of and how many people, might have viewed it.

How to avoid this
When sending out any of this kind of personal data, the organisation should carry out a **risk assessment** to identify all the potential areas of risk. Appropriate measures could be put in place to prevent the loss of data in the post. The use of couriers or recorded delivery may be necessary. It may also be prudent to **keep copies of data if authorised to do so**.



Breach scenario: unsecured special category data
An organisation holding special category data (eg. data relating to a person's race/religion/sex life/health etc.) stored it in **an unsecured area of the IT system** that meant that all members of staff had access to it with or without permission or the correct training to do so.

How to avoid this
An **audit** of the IT systems would identify what areas are freely accessible to all staff and ascertain what data needs to be more securely stored. The **correct training and policies and procedures** need to be put in place to facilitate staff awareness regarding the use of special category data and the importance of keeping it secure and confidential.

Breach scenario: phishing attack
An employee within an organisation received a phishing email that **appeared to be from a reputable and known client**. Unwittingly the individual replied to the email which allowed the scammer access to the organisation's systems and data stored within them.

How to avoid this
Training on the **importance of data security** and how to verify the sources of emails would help reduce the risk of this re-occurring. It may also be possible to **install systems** that identifies these kinds of scams or suspicious correspondence and flag them up. It's also vital that staff know the **correct response and action** if this does happen. There needs to be an agreed action plan in place to reduce the harm caused by the attack and to **ensure all the correct reporting is carried out afterwards**.

odpa.gg

THE OFFICE OF THE
Data Protection Authority