

What is a data breach?

A data breach is the unauthorised access, disclosure, or loss of personal information. This can result from cyber incidents (such as ransomware or business email compromise), as well as human error or accidental disclosure (e.g. sending information to the wrong recipient). In Australia, organisations regulated under the [Privacy Act](#) must notify affected individuals and the [OAIC](#) where a breach is likely to result in serious harm.

How can I detect a breach of my information?

An organisation may notify you that your personal information has been compromised, though they might describe it using terms like "breach", "incident", "unauthorised access", or "data exposure".

You may also become aware of an incident through media reporting, particularly where organisations are unable to contact affected individuals directly.

You can use online tools to detect if you have been involved in a data breach. [HavelBeenPwned](#) is an excellent, free resource that you can use.

What to ask an organisation about a data breach

If you are notified about a data breach, the following questions can assist you to understand the event and what the impact is likely going to be.

- ☐ When did the breach happen and what information has been involved? (This will commonly be outlined in the notification letter)
- ☐ How did the breach occur?
- ☐ What have you as an organisation done to respond to the breach?

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Prevention

While it is not always possible to prevent being involved in a data breach - when you are making a determination on whether to provide an organisation with your information, you may like to follow the below steps to assess if there could be any risks if they handle your sensitive information.

- ☐ Take the time to understand why your information is being collected, how it will be secured, how long it will be stored, who it will be shared with. You should be able to find this information within the organisation's **privacy policy** on their website.
- ☐ Ask whether they have experienced a data breach or do some searching on the [Information Commissioner's website](#) (for Australia) or the [Privacy Commissioner's website](#) (for NZ). to see if they have a track record of breaches.
- ☐ Work out what's important to you and protect it. If they ask for photo ID, produce something other than a licence or passport if you can (these are high risk credentials).

Knowing your privacy rights

We all have rights in relation to the protection of personal information. Privacy legislation in Australia and New Zealand requires regulated entities to protect your information that identifies you. It is important to understand these rights, particularly when they are threatened by identity compromise and misuse, including data breach events. The Privacy Commissioner websites in Australia and New Zealand are the best sources of information on these rights. This Fact Sheet introduces the basics and provides some tips if your identity information is compromised.

For more information, please see our [Knowing Your Privacy Rights Fact Sheet](#).

For additional support or information, contact IDCARE:

Submit [Get Help Form](#) | 1800 595 160 (Aus) | 0800 121 068 (NZ)

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.