Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Securing customer personal data

For small to medium businesses: Quick reference guide

As a business, you have a responsibility to keep the personal data of your customers secure.

Data breaches and ransomware attacks are common, highlighting the need for robust data security. Without this, your business may be at risk of severe financial and reputational damage.

Knowing the best ways to protect this data can often be confusing. You can follow this checklist to improve your data security practices and refer to the full guide on cyber.gov.au

What is personal data?

Personal data includes any information that could identify an individual. This may include details such as their name, address, payment details or medical records.

Cybercriminals can exploit this data to create a full profile of an individual for identity theft and fraud.

Steps for securing customer personal data

- ☐ **Create a register of personal data:** Know what data you collect from your customers and where you store it. Use a standardised template to collect data and always keep your register up to date.
- ☐ **Limit personal data collected:** Only collect what data is necessary for your business. Be clear and accurate about why you need that data and how you will use it.
- ☐ **Delete unused personal data:** Develop policies about when, why and how you should delete customer data. Keep data only for as long as you need and remove unnecessary duplication.
- ☐ **Consolidate personal data repositories:** Store customer data in centralised locations with stronger security. If you use local and cloud databases, make sure both are secure.
- ☐ **Control access to personal data:** Only give your staff access to the data they need to perform their role. Limit admin access, including to backups, and only give users the privileges they need.
- ☐ **Encrypt personal data:** Turn on encryption for devices that access or store customer data. Encrypt files and any data you transfer online for extra security.
- ☐ **Back up personal data:** Back up customer data, software and configuration settings. Store backups outside of business systems when not in use. If you have separate data repositories, sync all backups to a common time.
- ☐ **Log and monitor access to personal data:** Use event logs to track unauthorised access to data and make sure they capture enough detail. Consider using centralised logging software to manage event logs.
- ☐ **Implement secure Bring Your Own Device practices:** Create a policy on whether staff can use their personal devices for work. Have a plan to manage risks, including approved device types and secure ways to access data.
- ☐ **Report a data breach involving personal data:** Be aware of your reporting duties. Notify all customers affected, and report the incident at cyber.gov.au/report or call 1300 CYBER1 (1300 292 371). You may also need to report eligible data breaches to the OAIC.

More information

For cyber security advice and resources, visit cyber.gov.au/smallbusiness

For more small business resources, visit cosboa.org.au

For advice on data breaches and your legal obligations, visit oaic.gov.au