Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Securing Customer Personal Data for Small to Medium Businesses

Content Complexity
MODERATE ● ● ○

cyber.gov.au

For more cyber security advice

For more information on how to improve your cyber security, see our other guides at cyber.gov.au

Small Business Cyber Security Guide.

Small Business Cloud Security Guide.

Protect Yourself: Data Security

Personal Cyber Security

Contents

Introduction

This guide is focused specifically on the protection of customers' personal data. Guidance on general cyber security for businesses can be found in the Small Business Cyber Security Guide and the Strategies to Mitigate Cyber Security Incidents published by the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC). Please note: this guide is not exhaustive and should be used in conjunction with guidance from the Office of the Australian Information Commissioner (OAIC).

Data breaches against Australian businesses and their customers are increasing in complexity, scale and impact. In a country that is increasingly conducting business online, businesses have a responsibility to keep the personal data they collect from customers secure from unauthorised access, unauthorised disclosure, corruption and loss. As such, businesses should take appropriate steps to secure any personal information or data they hold.

In order to implement the below advice effectively, Australian organisations should first have a good understanding of their data and cyber security practices. In order to assist with this, ASD's ACSC recommends that businesses use the free Exercise in a Box tool to self-assess their data and cyber security practices and identify any relevant areas of strength or weakness.

Personal data

For the purpose of this guide, personal data includes a broad range of information that could identify an individual. Personal information may include an individual's:

- Name
- Date of birth
- Address
- Medical records
- Racial/ethnic origin
- Political opinion
- Religious beliefs
- Gender
- Sexual orientation
- Criminal record
- Payment details
- Email address
- Password
- Licence
- Photo
- Video
- Phone number
- Passport
- Employment information
- Biometrics

Often, personal data is greater than the sum of its parts, as when seemingly innocuous data is aggregated or combined it can be used to form a more complete picture about an individual. The OAIC has further information available on personal information.

Legislative requirements for protection of personal data

The Privacy Act 1988 sets out how organisations must handle personal information. It applies to organisations with an annual turnover of more than $3 million and some small business operators. ASD's ACSC recommends businesses visit the OAIC website to understand if and how the Privacy Act applies to them.

This guidance does not cover specific obligations small and medium businesses may have under the Privacy Act. For guidance on Privacy Act obligations, see the OAIC website or obtain independent legal advice.

Key data security practices

For businesses to be confident they are employing appropriate data security practices, ASD'S ACSC has a number of key recommendations that businesses should consider implementing. These key recommendations are:

- ✓ Create a register of personal data
- ✓ Limit personal data collected
- ✓ Delete unused personal data
- ✓ Consolidate personal data repositories
- ✓ Control access to personal data
- ✓ Encrypt personal data
- ✓ Backup personal data
- ✓ Log and monitor access to personal data
- ✓ Implement secure Bring Your Own Device practices
- ✓ Report a data breach involving personal data

Create a register of personal data

Businesses need to have a thorough understanding of customers' personal data they collect and retain in order to effectively protect such data. As such, businesses should create a register of the types of personal data from customers they hold and where it is located. For example, businesses may consider creating a register of databases and data assets depending on their needs. Any register should be updated and verified on a regular basis to ensure new sources and storage locations for customers' personal data have been captured. These registers should use a standardised template to ensure that all necessary data is captured. The National Archives of Australia has further information on designing and maintaining an information asset register.

Limit personal data collected

Businesses should only collect personal data from customers that they need to operate effectively, and outline clearly and accurately why they need to collect such data and what purpose it will be used for. Additional personal data should not be collected from customers 'just in case' or on the basis that it might be useful at a later date, unless there is a clear understanding of what this data may be used for later. The more personal data from customers that businesses hold the more personal data that could be at risk if a data breach occurs.

Delete unused personal data

Businesses should develop and employ policies stipulating how long customers' personal data should be stored before it is deleted. These policies should outline the timeframes or criteria for data retention, and the processes once customers' personal data has been held for the required retention timeframe. The maximum time businesses should hold customers' personal data for before deletion should be based on the use case or risk profile of each business, and the type of personal data that is collected from customers. Businesses should endeavour to implement a stricter program with shortened timeframes where practical, with customers' personal data being deleted immediately after it is no longer required, to minimise occurrences of customers' personal data being retained unnecessarily – thereby avoiding customers being exposed to unnecessary risk.

In deleting customers' personal data, businesses should have an effective data sanitisation or data removal program that contributes to the reduction of impact in the event of a data breach involving customers' personal data. If businesses continue to retain customers' personal data that does not contribute to their operations, it creates unnecessary risk for both themselves and their customers. Businesses should also consider when and where customers' personal data is unnecessarily duplicated. If there is no identified business need to keep multiple copies of customers' personal data, businesses should remove all unnecessary duplication.

Consolidate personal data repositories

Consolidating customers' personal data into centralised locations or databases allows businesses to focus on key data repositories and apply enhanced security practices. In doing so, storing customers' personal data in fewer locations can also reduce the complexity of managing it and frees up resources to apply stronger data security measures. Businesses that are utilising both local and cloud-based databases will need to ensure that appropriate security measures are in place for both.

Control access to personal data

The implementation of strong and effective access controls can be used to ensure that employees only have access to customers' personal data that they require to complete their job, and that they only have the ability to perform actions on such data that they need to. Implementing strong access controls provides an additional level of security even when access to businesses' systems have been gained through stolen credentials or by a malicious insider.

As a first step in implementing access controls, businesses should consider what actions (and associated privileges) employees need to complete their job, and consider restricting them from performing any other actions. Employees with privileged access to systems, such as administrators, should have sufficient restrictions placed on their privileged access to limit damage in the event of a potential account compromise, as a compromised privileged user can have a significant impact on a businesses' ability to operate. Strong consideration should also be given to which users have privileges to access and alter backups, as any impact or tampering with these can seriously impact an organisation's ability to recover data in case of an incident. Businesses should also consider obtaining addition security training for privileged users.

Encrypt personal data

Full disk encryption should be applied to businesses' devices, such as servers, mobile phones and laptops, that access or store customers' personal data to provide protection against customers' personal data being accessed by unauthorised parties, such as when devices are sold, lost or stolen. Additionally, businesses may choose to implement file-based encryption to add an extra layer of protection in the event that systems are compromised as part of a cyber attack. Finally, customers' personal data should be protected by encryption when communicated between different devices, such as between businesses and customers over the internet. While the encryption of customers' personal data can reduce the immediate consequence of access by a cybercriminal, businesses should be aware that encryption is not guaranteed to prevent data breaches as not all encryption offers the same security and cybercriminals can still identify ways to exploit encrypted data.

Backup personal data

Backups are an essential measure to ensure an organisation can recover important business data, including customer personal data, if it is damaged, lost or destroyed. Backups are also critical in protecting customers' personal data from common incidents such as ransomware attacks or physical damage to devices. Notably, ransomware attacks encrypt businesses' data and shut down or severely limit their operations. If businesses are the victim of a ransomware attack, restoring customers' personal data from a recent and uncorrupted backup is one of the best ways to recover as businesses should not pay ransoms to cybercriminals. Backups can also ensure customers' personal data is retained if devices are impacted by events such as fires, floods or earthquakes.

In conducting backups, businesses should ensure that software and configuration settings for systems are also backed up. In addition, backups of different data repositories should be synchronised to enable restoration to a common point in time. Furthermore, it is essential that all backups are retained in a secure and resilient manner and that the ability to restore customers' personal data from backups is regularly tested. Finally, where possible, backups should be segregated or disconnected from businesses' systems when not in active use to ensure that should a system fall victim to a ransomware attack, or other form of destructive attack, backups (and the data they contain) will not be corrupted or lost. ASD's ACSC has further information regarding backups in its How to backup your files and devices guidance.

Log and monitor access to personal data

Implementing logging and monitoring practices can assist businesses in detecting unauthorised access to customers' personal data – either by cybercriminals or malicious insiders, such as employees viewing personal data of customers they shouldn't.

When implementing logging and monitoring, it is important to ensure that logs contain sufficient detail to be useful. In addition, a centralised event logging facility, if available, can be used to capture, protect and manage event logs from multiple sources in a coordinated manner. Finally, businesses should consider and evaluate what solutions can be utilised to enhance their logging and monitoring practices, including log management software, Endpoint Detection and Response (EDR) solutions or Security Information and Event Management (SIEM) tools.

Implement secure Bring Your Own Device practices

Businesses that employ Bring Your Own Device (BYOD) policies need to have appropriate protections in place to ensure that this is done securely and does not increasing the risk of data breaches involving customers' personal data. A BYOD policy allows employees to use their own personal devices, such as laptops and mobile phones, for work related purposes. Businesses that allow employees to access customers' personal data using their own personal devices without appropriate protections expose their customers' personal data to a number of risks that are unlikely to be present on devices owned and managed by their business.

In order to employ BYOD policies securely, businesses should have a considered strategy or risk management plan in place. This strategy should consider the types of personal devices that can be used, how customers' personal data is accessed from such devices, and what protections are in place to ensure appropriate separation between customers' personal data and the personal data of the device owner. Further information of what to consider when implementing a secure BYOD policy can be found in ASD's ACSC Risk Management of Enterprise Mobility Including Bring Your Own Device publication.

Report a data breach involving personal data

Businesses should ensure they are aware of their reporting obligations in case they are the victim of a data breach involving customers' personal data. For example, all cyber security incidents should be reported to ASD's ACSC through the ReportCyber portal, or by calling 1300 CYBER1 (1300 292 371), regardless of the scale or impact of the incident. Customers or users affected by data breach involving their personal data should also be made aware. Further information on how to respond to a data breach can be found in ASD's ACSC Data Spill Management Guide.

Businesses that are covered by the Privacy Act must report eligible data breaches to the OAIC. An eligible data breach occurs when:

- Personal information is accessed or disclosed without authorisation or is lost.
- This is likely to result in serious harm to any of the individuals whose information is impacted.
- The business has not been able to prevent the likely risk of serious harm with remedial action.

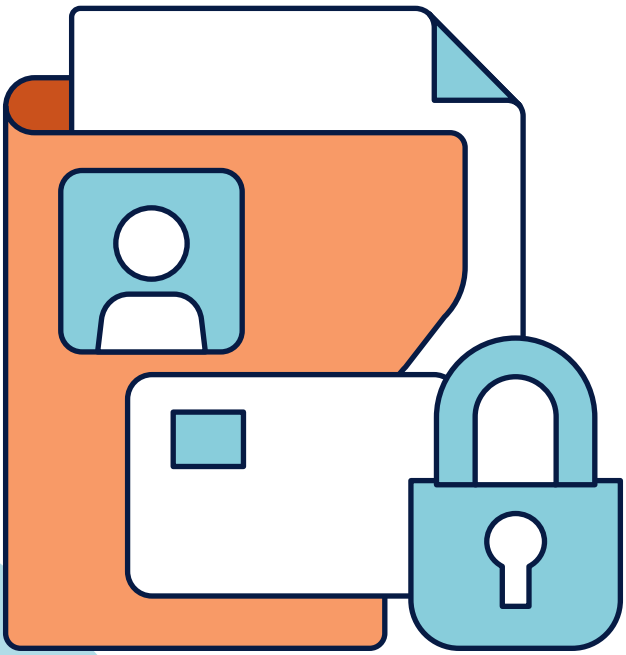
Further information can be found on the OAIC's Notifiable data breaches webpage.

Conclusion

Businesses cannot afford to forgo investing in their security, and risk compromising the security of their customers' personal data. The prevalence of data breaches and ransomware attacks underscores the importance of sound security practices. Businesses cannot afford to assume that they will not be targeted. Investing in security proactively can be far more cost effective than having to manage the repercussions and costs of a major data breach.

Australian organisations should strongly consider becoming part of the ASD Cyber Security Partnership Program in order to gain a better understanding of the cyber security landscape and the steps required to protect themselves from cyber security threats. Organisations should also consider joining the Cyber Wardens program, which is another initiative endorsed by ASD's ACSC and aims at bolstering the cyber capabilities of people who work in small businesses. Initiatives like these are critical in ensuring that an organisation's cyber and data security practices are up to date and evolving in line with current cyber security trends.

If any of the above information is unclear, or you have any inquiries please contact ASD's ACSC on 1300 CYBER1 (1300 292 371).



Notes

Notes

For more information, or to report a cyber security incident, contact us:
cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre