BRENNAN IT

NEW DATA REGULATIONS: **IS YOUR BUSINESS COMPLIANT?**

What the new data regulations mean for your business, and how Brennan IT and Microsoft 365 can help.

THE REGULATIONS: **WHAT YOU NEED TO KNOW**

	Australia: Notifiable Data Breaches (NDB) scheme	Europe: General Data Protection Regulation (GDPR)	Draft Prudential Standard CPS 234 Information Security
Came into effect:	22 February 2018	25 May 2018	March 2018
Affects:	Any Australian business governed by *The Privacy Act 1988* that holds or processes customer data.	Australian businesses with an establishment in the EU, or that offer goods and services in the EU, or that monitor the behaviour of individuals in the EU.	All entities regulated by the Australian Prudential Regulation Authority (APRA), including authorised deposit-taking institutions, general insurers, life companies and private health insurers.
All regulations stipulate that businesses MUST:	• Develop transparent information handling practices and business accountability, to give individuals confidence that their privacy is being protected. • Implement measures to ensure compliance with a set of privacy principles • Take a privacy-by-design approach to compliance, or risk significant fines.		
Other key points:	• Organisations should embed a culture of privacy by appointing key roles and responsibilities for privacy management, including a senior member of staff with overall accountability. • A privacy impact assessment should be developed for many new projects or updated projects involving personal information. • Individuals must provide consent for their information being held, and this consent must be informed, voluntary, current, specific and fully understood.	• Businesses must appoint data protection officers to monitor and advise on compliance with the GDPR and with internal privacy policies and procedures. • Business must undertake a compulsory data protection impact assessment prior to data processing, where a type of processing is likely to result in a high risk for the rights and freedoms of individuals. • Individuals must provide consent for their information being held, and this consent must be freely given, specific, informed and an unambiguous indication of the data subject's wishes.	• Businesses must take measures to be resilient against information security incidents (including cyber-attacks) by maintaining an information security capability that is commensurate with information security vulnerabilities and threats. • Businesses must also develop transparent information handling practices and business accountability, to give individuals confidence that their privacy is being protected.
If a data breach occurs:	Organisations are required to notify the Australian Information Commissioner in addition to notifying individuals affected by a data breach that is likely to result in serious harm.	Data controllers *must* advise the relevant supervisory authority of a data breach within 72 hours of becoming aware of the breach unless the breach is unlikely to impact the rights and freedoms of individuals.	The business must notify APRA of material information security incidents.
Failure to comply:	Fines up to $2.1 million.	Fines of up to €20 million or 4% of annual worldwide turnover, whichever is greater.	To be determined by APRA.

Source: Office of the Australian Information Commissioner [1]

1. https://www.oaic.gov.au/resources/engage-with-us/consultations/australian-businesses-and-the-eu-general-data-protection-regulation/consultation-draft-australian-businesses-and-the-eu-general-data-protection-regulation.pdf

WHAT IS **A DATA BREACH?**

A data breach occurs when personal information that an entity holds is subject to unauthorised access or disclosure, or is lost. A data breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems.

Examples of common data breaches

Loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information.[1]

Unauthorised access to personal information by an employee[1], where an internal employee intentionally accesses data without permission.

Inadvertent disclosure of personal information due to 'human error' for example an email sent to the wrong person.[1]

Disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.[1]

Hacking/computer Intrusion (includes phishing, ransomware/malware and skimming)[2]

Causes of common data breaches

Weak or stolen credentials leading to a password being hacked or revealed which can lead to compromised data, compromised systems, and people using an employee's account without his or her knowledge.

A development or test environment containing real data is compromised.

Leaving computer open or unlocked when unattended.

A computer is infected with a virus, malware or remote-access Trojan.

Insecure storage or transmission of sensitive information, or a lack of encryption controls and policies.

Missing patches and updates which enable adversaries to take advantage of vulnerabilities in operating systems and applications – putting all of the data on those systems and other connected systems at risk.

Insecure disposal and re-use or devices, or a lack of secure destruction controls and policies.

Application vulnerabilities and mis-configuration that can be exploited.

Source: Office of the Australian Information Commissioner [2]

1. https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response 2. https://chiefexecutive.net/understanding-seven-types-data-breach/

DO YOU NEED A **SECURITY AUDIT AND RISK ASSESSMENT?**

	Security Audit	Risk Assessment
What is it?	Our expert team will assess your business' security policies, processes and practices to determine their level of effectiveness and compliance.	Our expert team will help you identify and help you manage any risks within your organisation, with a focus on those related to cybersecurity.
Our approach:	We conduct our audit against ISO 27001:2013 security standard – an international standard for implementing information security in organisations. This standard brings numerous benefits. It provides a structured approach to addressing security incidents, helps keep confidential information secure; provides customers and stakeholders with confidence in how you manage risk; helps you to comply with the regulations outlined in this document, and more.	We start by reviewing any existing Risk Management Policy and if such a policy exists, we align our own risk assessment methodology to either update the Risk Register with your existing policy, or create a new Risk Register which aligns with your management standards. In determining your exposure, we classify risks into "high", "medium" and "low" depending on the likelihood and consequence of a risk materialising.
How we do it:	We conduct interviews with key stakeholders from operationally crucial departments. We also conduct: • a documentation review including policies, procedures, processes and practices • a physical inspection of your offices and data centres within scope • a review of technical configurations from selected systems.	We conduct risk assessment workshops with key stakeholders from operationally crucial departments. We also: • Prepare and present scenarios of security risks and understand the current risk mitigation controls • Finalise the security risks and discuss the acceptable risk remediation controls • Identify risk ownership and timelines for risk remediation for each identified risk.
Outcome:	We provide a **Security Audit Report,** which provides a structured approach for meeting ISO 27001 security requirements and minimising security gaps. Aligning the business to ISO 27001 helps ensure you are complying with data regulations and also helps you reduce your cybersecurity insurance premiums.	We provide a **Risk Register Report**, which outlines: • Overall vulnerability • Level of risk (description, appetite and root cause) • Impact of the risk on the confidentiality, integrity and availability • Inherent likelihood, consequence and risk rating • Current security controls • ISO 27001 reference • Residual likelihood, consequence and risk rating • Risk treatment actions • Remediation action type • Risk resolution target date and risk ownership

REINFORCE YOUR SECURITY
AND AVOID DATA BREACHES WITH MICROSOFT 365

With Microsoft 365, you can reinforce your business' security against data breaches, and ensure you have the tools and processes in place to ensure compliance with these rigorous new regulations.

Microsoft 365 Business

- Advanced Threat Protection, including Safe Links and Safe Attachments
- Data loss prevention
- Classification and labelling
- Multi-factor authentication
- Message encryption and rights management
- Mobile device and application management
- Secure Store for benchmarking controls
- Compliance manager for visibility

Microsoft 365 Enterprise

- Conditional access (user, device, app, locations)
- Self-service password reset for on-premise identities
- Tracking, reporting and revolving privileges
- Advanced Threat Analytics
- Windows Enterprise: Device Guard, Credential Guard, App Locker, Enterprise Data Protection
- Automatically classify, protect and preserve sensitive data
- Shadow IT detection with cloud app security
- Real time risk-based access to corporate network
- Anomalous attack detection and reporting
- Additional customer access controls
- Endpoint protection with Windows Defender Advanced Threat Protection

HOW BRENNAN IT **CAN HELP**

By engaging Brennan IT as your Microsoft 365 partner, you can more effectively assess and manage compliance risk, protect your personal data and streamline your compliance and security processes.

Our dedicated team will work with you to understand your needs and compliance requirements, and secure the Microsoft 365 licenses that are right for your business.

As well as configuring and implementing a solution that's ideally matched to your needs, we can provide direct support to you and your end users through our managed services capability – empowering your people to work securely from anywhere, and from any device. We also provide you with a single point of contact for any potential issues, a 24/7 service desk, and ongoing advice and support from our expert team.

BRENNAN IT

brennanit.com.au | marketing@brennanit.com.au | 1300 500 000