Data Breaches and Privacy

Preparing for the Australian Privacy Amendment (Notifiable Data Breaches) Act 2017

Government agencies and some private sector organisations, under an amendment to the Privacy Act 1988, will need to notify individuals and the Privacy Commissioner when data breaches of personal information occur. Similar legislation in other jurisdictions has increased the cost and risk associated with data breaches. This brief discusses how Oracle products and services can assist customers in complying with the new obligations.

ORACLE DATABASE

Privacy Amendment (Notifiable Data Breaches) Act 2017

On 13th February 2017 the Australian Parliament passed the Privacy Amendment (Notifiable Data Breaches) Act 2017. The Act introduces a mandatory breach notification scheme into the Privacy Act 1988. It applies to APP entities covered by the Australian Privacy Principles including federal government agencies and a significant number of private sector organisations.

The amendments are expected to commence within 12 months of the Act passing, giving organisations time to comply. In order to comply with the key obligations, an AAP entity will need processes and systems in place which enable it to:

- conduct a prompt assessment of whether an eligible data breach has occurred; and
- notify relevant individuals and the Privacy Commissioner of an eligible breach.

An "eligible data breach" occurs if there is unauthorised access to, unauthorised disclosure of, or loss of personal information, and the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

"$2.64 million is the average total cost of a data breach"

PONEMON INSTITUTE LLC
SURVEY QUOTED BY THE ACT'S EXPLANATORY MEMORANDUM

"There will always be a risk that data will be exposed: this could come from carelessness; a disgruntled employee wishing to cause harm; a malicious actor…"

SENATE ECONOMICS REFERENCES COMMITTEE (AUSTRALIA)
2016 CENSUS: ISSUES OF TRUST REPORT

The Inevitability of Data Breaches

Analysts and commentators point to the inevitability of data breaches, whether from accidental release or advanced cyber-attacks. Healthcare was the most cyber-attacked industry in 2015, with government in fourth place. Consider the potential notification costs of an incident like the United States Office of Personnel Management (OPM) release of the personal information on 22 million government employees.

Security measures can be applied to reduce the risk of breaches, promptly identify breaches when they do occur, and to mitigate the risk of serious harm from a breach.

"Have you considered whether you should employ encryption of databases used to store personal information?"

OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER
GUIDE TO SECURING PERSONAL INFORMATION

Apply Security Controls Where the Data Lives

Adoption of software as a service, infrastructure cloud services, a mobile workforce and multi-supplier outsourcing have blurred the network and geographic boundaries. Perimeter and network-centric security is less effective as a result. Organisations must identify their personal information holdings and *apply security controls where the data lives*. Administrative accounts are prime targets for intruders. Focusing on where the data resides also facilitates appropriate controls on administrative privileges.

DISCLAIMER
Security technologies form only part of a comprehensive people and policy response to security risks. The information in this document may not be construed or used as legal advice.

ORACLE

Database Encryption

The Act provides a list of considerations, including encryption, when determining whether there is a likely risk of serious harm to an individual from a breach, and importantly whether a breach is an eligible breach under the Act.

The Act's explanatory memorandum anticipates that "encryption is expected to be the most common security technology" used to determine whether a breach will cause serious harm, and therefore must be notified. If breached data is encrypted and encryption keys are secure, no harm may be caused by the breach. The memorandum references surveys that indicate similar legislation in Europe (the General Data Protection Regulation or GDPR) has driven significant adoption of encryption.

Full disk encryption, the common solution for securing laptops and mobile devices, has limitations for servers hosting databases. Database encryption has a number of advantages over full disk encryption. Database encryption provides:

- **separation of duties** – operating system administrators and compromised "superuser" system accounts cannot access data and this extends to backup copies. User and administrative access can also be granted to selective data sets rather than globally;
- **resilience to cyber attack** - database administrator credentials must be compromised in addition to gaining operating system access (in keeping with the '*defence in depth*' strategy recommended by the Australian Signals Directorate);
- **ease of implementation** - database encryption is installed by default with the Oracle database and can be implemented without an outage, in hours not days; and
- **cost** – in many scenarios database encryption will be more cost effective, requiring no new hardware, and providing the flexibility to selectively encrypt only sensitive data.

KEY BENEFITS

- Personal data is encrypted and protected from accidental loss
- Database encryption makes it harder for cyber-attackers to access personal information
- In the event of a breach, loss of encrypted data may not be notifiable
- The cost of data breach notification is managed

Masking and Sub-setting

Many organisations report that they have no way of knowing if the data in non-production environments has been compromised and what data may have been breached. Ensuring personal information does not reside in non-production environments, including cloud environments, is another key risk mitigation.

Oracle offers an automated and repeatable process for sanitising copies of production data for testing and development. Replacing personal information with dummy but realistic values facilitates testing without compromising security.

Sub-setting allows a consistent portion of production data to be reproduced in non-production environments, or shared with 3rd parties for production or non-production.

Production Dev/Test

KEY BENEFITS

- Personal information obfuscated
- Reduce costs through automated, repeatable processes
- Improves compliance (e.g. ASD Information Security Manual)

Prepare for Data Breach Notification with Oracle

Whether your data is onsite or in the cloud, Oracle has comprehensive capability to discover personal data, audit and notify data access, encrypt data, mask and subset data for non-production environments, to protect databases with "SQL smart" firewalls, for encryption key management, for patch automation, for restricting administrative privileges and for fined grained access control.

Oracle offers consulting services to assess Oracle database security, help migrate to Oracle, and to improve information security posture from the inside out.

For more information, contact your local Oracle sales representative.

CONNECT WITH US

blogs.oracle.com/securityinsideout
facebook.com/oracle
twitter.com/oraclesecurity
oracle.com/security

FOR MORE INFORMATION

Contact: 1300 366 386 (Australia)

ORACLE

Integrated Cloud Applications & Platform Services