FROST & SULLIVAN

AUSTRALIA

Data Security & Breach Notification Acts

Understanding the GDPR and Data Breach Reporting Laws: Perception Versus Reality

A Frost & Sullivan Growth Insight
commissioned by LogRhythm

LogRhythm™
The Security Intelligence Company

Contents

1. Local Data Privacy Regulations Act As GDPR Catalysts In Australia 4

    a. An Overview Of Australia's Readiness For Changing Customer Data Processes 4

2. Letting The Research Talk: Myths Versus Findings 6

    a. Myth 1: My Business Does Not Need To Prepare For The GDPR; It Doesn't Impact Us 6

    b. Myth 2: We Already Have A Data Protection Programme In Place, We Won't Be Penalised Under The GDPR 7

3. Not Just An I.T. Job: GDPR As An Organisation-wide Effort 8

    a. Get Your 'People' Awareness Right – Is The C-level Willing To Take Responsibility? 8

    b. Fine Tune Your Incident Response Plan – Is Your 'Process' Ready For A Breach? 10

    c. Measure Your 'Technological' Barometer – How Quickly Can You Detect The Leak? 11

4. The Last Word 12

    a. Phase 1: Investing In The Tech 12

    b. Phase 2: Adapting To The Era Of The Consumer 13

    c. Phase 3: Crossing Off The Gdpr Checklist 13

5. In Conclusion: What's In It For The Organisation? 15

6. About Logrhythm 16

1. Local Data Privacy Regulations Act as GDPR Catalysts in Australia

Why is everyone talking about the GDPR?

After Net Neutrality, the next big thing in the 21st century is data security and privacy. The GDPR is a new privacy regulation from the EU Parliament which etches out strict guidelines for businesses to handle user data. Businesses that do not comply with these guidelines will be fined.

How hefty are these fines?
GDPR fines can go up to EURO 20 million or 4% of a business' annual global turnover, whichever is higher. These are the maximum fines – exact or actual fines would depend on the severity of non-compliance.

If this is an EU regulation, why does it affect non-EU countries?
It is expected that as companies leverage the GDPR as a business opportunity to develop trust with customers and partners, more organisations will eventually apply GDPR guidelines to all their data.

This whitepaper takes a comprehensive look at where businesses in Australia stand in terms of the GDPR readiness, understanding, and awareness. Australia has already undertaken a thorough due diligence process to set the stage for the GDPR with the Australian Data Privacy Regulation.

In broad terms, Australia's Data Privacy Regulation applies more granular definitions to the same core aspects of the GDPR: breach notifications and timeframes, business size applications, and reporting requirements.

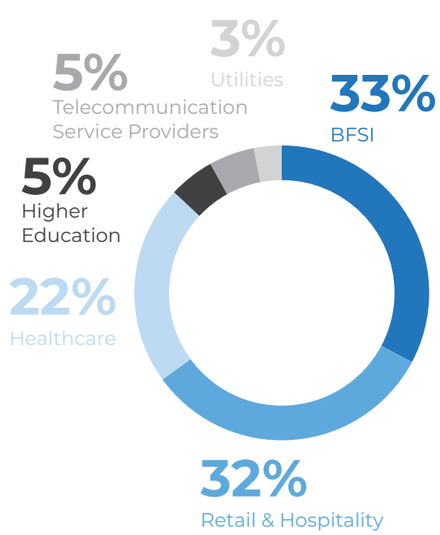
There are two key differences between the GDPR and the Australian Data Privacy Regulation. The first is how they both define "real risk of serious harm" – while the GDPR does not explicitly define what this risk constitutes, the Office of the Australian Information Commissioner (OAIC) defines this as "may include serious physical, psychological, emotional, financial, or reputational harm". In contrast, the GDPR, with its broader definition, leaves companies to determine the likelihood of risk instead. The second key difference between the GDPR and the Australian Data Privacy Regulation is the fact that the latter is only applied to businesses with "an annual turnover of more than $3 million", while the GDPR is applied to any company or government agency that controls or processes personal identifiable information.

While Australia lies oceans away from the European Union, it is still at the forefront of trade, technology, and innovation. With Australian organisations ramping up their GDPR know-how, this report aims to capture key findings and insights on the readiness of Australia for the EU GDPR.

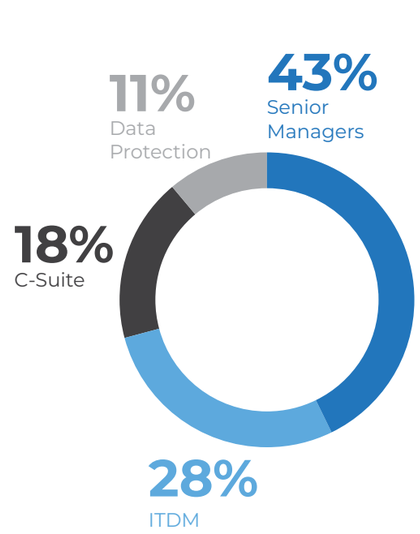
By asking companies to enforce better data protection policies, GDPR can change how Australian consumer data is handled.

Respondent profile:
Frost and Sullivan conducted a Market Insights study in January 2018 and surveyed 100 respondents from multinational companies in Australia. These companies span industries such as financial services, retail and hospitality, healthcare, higher education, telecommunications, and utilities.

Sector Breakdown



Designation Breakdown



2. Letting The Research Talk: Myths Versus Findings

a. Myth 1: My business does not need to prepare for the GDPR; it doesn't impact us

In reality, the GDPR is not limited by actual geographical scope or whether a business permanently stores data:

- Does a business collect or process personal data from residents in the EU? Does a business have employees who reside in the EU? If either answer is Yes, then the business in question would be under the GDPR jurisdiction.

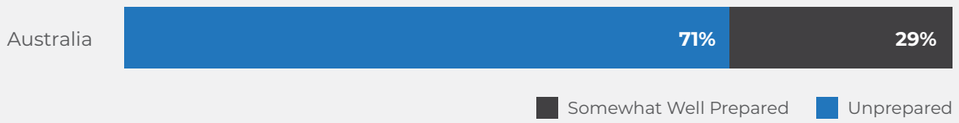
For example, an Australian company selling furniture to EU residents from its website is still subject to the GDPR.

- "But our business doesn't actually keep customer data, we just analyse it." The GDPR also applies if a business is just monitoring the behaviour of individuals in the EU, such as a research firm, even if the data is not permanently stored.

Our Findings: Frost and Sullivan's 2018 survey found that 53% of organisations in Australia qualify as businesses that would have to comply with GDPR guidelines as they actively collect or process personal data of EU residents.

However, only 29% of respondents have taken steps to comply with the GDPR.

Exhibit 2: Respondents' Views on Preparedness for GDPR



The graph above indicates that organisations in Australia are still lagging in their awareness of the GDPR and are not taking the required measures to be fully compliant. With the GDPR having just come into force this year, global business are on an even learning curve; however, as time goes by, non-compliance could mean losing a global competitive edge.

As a result, Australian companies need to quickly assess whether they are subject to the GDPR and comply with their new obligations. Inaction may land businesses on the growing list of companies that have already fallen short of these regulations, becoming subject to extremely heavy fines.

b. Myth 2: We already have a data protection programme in place, we won't be penalised under the GDPR

While Australia's local data protection programmes have set a foundation of sorts for GDPR-readiness, local organisations still face a significant gap in relearning the fundamentals of a broader, more exhausting policy like the GDPR. Compliance with local data protection acts like Australia's Notifiable Data Breaches scheme from the Privacy Amendment (Notifiable Data Breaches) Act 2017, Australian organisations may also not be as robust as hoped, with only 28% showing knowledge of the types of organisations affected.

Further insights into local knowledge of Australia's Notifiable Data Breaches scheme's notification requirements reveal that only 2% of local organisations showed correct knowledge of the right course of action following a suspected data breach.

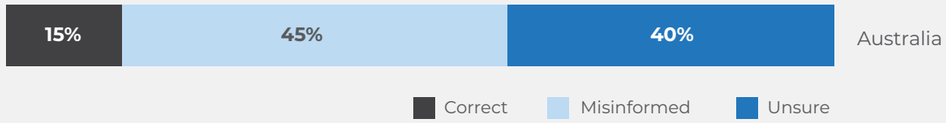
The GDPR also demands much more from organisations in terms of accountability for their use of personal data, with fines being significantly heavy. Under the GDPR, organisations that fail to comply could be subject to fines of up to 4% of annual global revenue or EURO 20 million, whichever is higher.

Our Findings: 70% of Australian organisations remain unprepared for Australia's Notifiable Data Breaches scheme. In evaluating awareness of data breach penalties,

only 4% have correct knowledge, 52% were misinformed and answered incorrectly, while 44% were unsure. This shows a worrying lack of awareness and understanding in Australia.

Exhibit 3: Respondents' Knowledge of Maximum Penalty for Failure to Report a Data Breach

Exhibit 4: Respondents' Awareness of Proposed Penalty for Failure to Report a Data Breach under Local



In comparison, organisations in Australia showed slightly higher levels of awareness of local data breach regulations where 15% had correct knowledge of penalties most likely due to it being a local, older

regulation. However, awareness levels are still fairly low and calls for increased education on both local and global privacy regulations.

The GDPR isn't only about fines and fees; it centres on putting the consumer first. Being fined is not the only punishment for non-compliance – companies face greater implications with damages to their reputation and consumer confidence.

3. Not Just An I.T. Job: Addressing The GDPR Is An Organisation-wide Effort

a. Get your 'people' awareness right – Is the C-level willing to take responsibility?

The GDPR requires businesses to change the way they operate, which is a huge mindset shift and not just an IT department responsibility. This would span across:

Marketing – demonstrating value and transparency to customers for collecting data;

HR – protecting employee data and using it for the purposes it was handed over;

Finance – while financial firms are no strangers to regulation, it will be imperative to have clear visibility over how data is accessed by different people at different stages;

Procurement – The GDPR requires the organisation to demonstrate compliance both internally and within their supply chains, so appropriate due diligence of suppliers and monitoring of their GDPR compliance will have to be taken on, and lastly;

The Board – For the first time, the GDPR requires that the board become active drivers of better data protection processes, where cybersecurity is a top-of-mind issue and responsibility of board members including external directors.

More importantly, the GDPR calls for firms in Australia to designate a Data Protection Officer (DPO) to oversee data protection management. The majority of appointed DPOs were trained (77%) and resource-ready (80%). However, less than half of organisations had an appointed DPO present on staff in preparation for the breach notification acts. As Australia's cause-effect relationship with the GDPR changes through the year, it would be essential to centralise this knowledge and responsibility into a dedicated function, responsible for creating cross-department compliance.

Our Findings also showed that while 57% of legal departments have made preparations to respond to the breach, only 24% perceive their staff to be well prepared to respond to a cybersecurity threat.

Exhibit 5: Respondents' Views on Senior Management Involvement in GDPR Compliance Plans

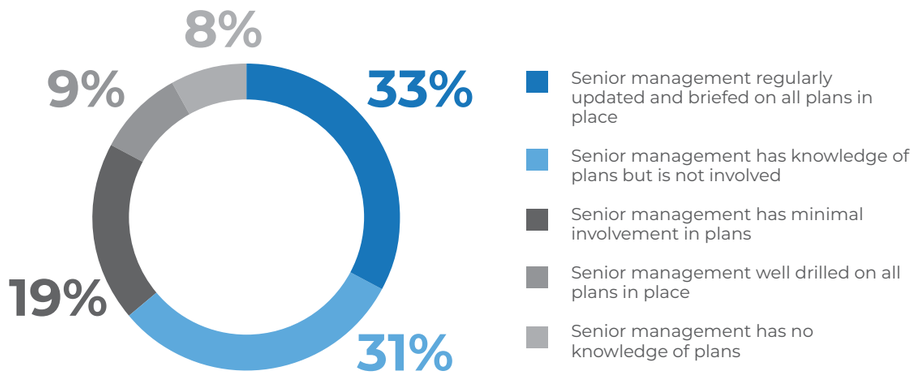
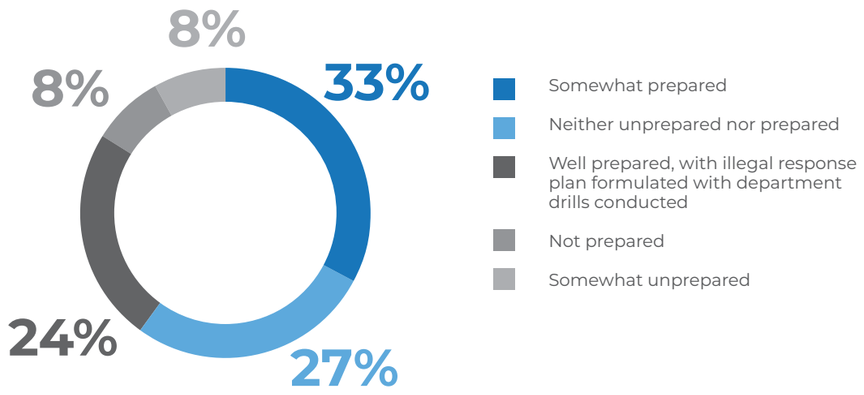


Exhibit 6: Respondents' Views on Preparedness of Organisations' Legal Departments for GDPR

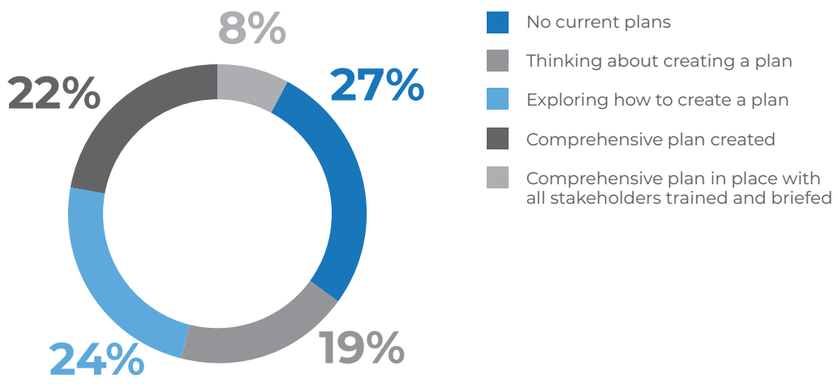


b. Fine tune your incident response plan – Is your ‘process’ ready for a breach?

A key component of the GDPR readiness is the need to have a breach notification plan in place. Only 8% of organisations have a comprehensive incident response plan in place with all stakeholders trained and briefed, with another 22% of respondents stating that they have comprehensive plans. Meanwhile, less than half of senior management are regularly updated and briefed on all plans in place.

This paints the current landscape as one where most Australian organisations have not formulated comprehensive plans or adopted industry-recognised security frameworks. This indicates a high level of risk to possible security incidents and their ability to detect and remediate without business disruption.

Exhibit 7: Respondents’ Level of Preparedness in Having a Breach Notification Plan

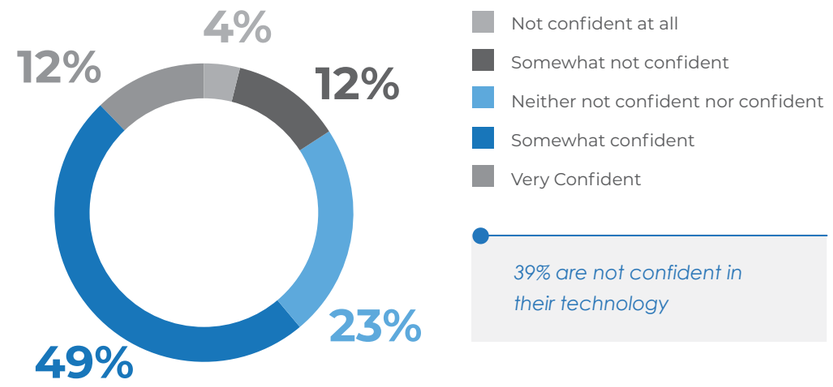


c. Measure your ‘technological’ barometer – How quickly can you detect the leak?

In terms of IT security solutions, 39% of the respondents are not confident that their current IT security solutions would detect and provide visibility of a breach.

More concerning is the fact that 71% of organisations would expect to take more than an hour to detect an incident.

Exhibit 8: Respondents’ Confidence Level in Their Companies’ Existing IT Security Solutions to Provide Detection and Visibility in the Event of a Security Breach



39% are not confident in their technology

Ensure a proper balance between people, process, and technology to achieve GDPR readiness. Each element will play a critical role in the GDPR journey.

4. The Last Word

a. Phase 1: Investing in the Tech

When asked about future investments in IT security, only 3% of survey respondents plan to invest an additional 10% of their IT budget; 34% plan to spend an additional 2%–5%; while a whole 33% intend to invest only an additional 1% of their IT allocation.

Exhibit 9: Past IT spending vs spending increase to prepare for EU GDPR

Australia	No	Yes: up to additional 1% of IT budget	Yes: up to additional 2% - 5% of IT budget	Yes: up to additional 6% - 10% of IT budget	Yes: more than 10% of IT budget
More than 20% of IT budget	0%	0%	0%	3%	1%
16% - 20% of IT budget	3%	0%	5%	1%	1%
11% - 15% of IT budget	2%	4%	14%	1%	1%
6% - 10% of IT budget	9%	12%	14%	2%	0%
1% - 5% of IT budget	19%	17%	1%	0%	0%

Readiness for the GDPR is also aimed at finally severing IT ties to old, monolithic technology pieces. Innovative technology like cloud gives organisations the flexibility and dynamism they need to grow compliantly in the GDPR environment – a domain where personal data will be needed at the touch of a button so that business decisions can be made in real time as well as to quickly identify and respond to a customer regarding their data record. Breaking away from complex and expensive legacy systems, the cloud would offer scalable solutions that fully integrate with organisational applications. CIOs (Chief Information Officer) and CISOs (Chief Information Security Officer) are turning to encryption technologies, along with newer innovations such as big data analytics, Internet of things (IoT), and blockchain. These are just the in-house obligations; CIOs must also ensure that their cloud vendors and other third-party partners are following GDPR specifications.

b. Phase 2: Adapting to the era of The Consumer

Amid the media coverage, information and organisational awareness efforts, it is easy to overlook GDPR's focus on customer privacy. Despite the organisational overhaul it demands, GDPR is not meant to prohibit business processes but to drive transparency and foster good data management. Although complex, GDPR compliance allows companies to come out on top by using this as an opportunity to master the customer experience:

- Better Big Data: One of the failures of 'big data' is that it encouraged harvesting as much data as possible without necessarily asking why this data was needed and how it was going to be used. The GDPR will break this cycle, turning big data into smart data. Going forward, it will be simpler for businesses to ensure they are looking at customer engagement across the entire life cycle and not just as a marketing exercise.

- Data Value Management: Organisations can start seeing data as a corporate asset by improving how they measure the effectiveness of their data strategy better, and in turn, use data more efficiently to improve customer journey.

c. Phase 3: Crossing off the GDPR Checklist

There is ample room for improvement in increasing the awareness of the GDPR and its implications, given that only 30% of Australian organisations consider themselves somewhat or well prepared for the regulation. When we look at a snapshot view of Australia's organisational GDPR state:

Awareness and readiness for data breach notification acts	53% of Australian organisations collect or process personal data of EU residents. 30% of Australian organisations consider themselves somewhat or well prepared for the GDPR. Only 4% know that fines can be up to 4% of annual global revenue or EURO 20 million, whichever is higher.
Plan for the GDPR	30% of Australian organisations have a comprehensive plan; only 35% have an incident response plan; while 34% have adopted an information security framework. 58% of senior management is minimally involved in compliance plans.
Action for the GDPR	34% of respondents plan to increase spending by 2%–5% of revenue, while only 3% of respondents aim to increase by more than 10% of their revenue.

With this snapshot, Australia's businesses are in the prime spot to begin aggressively focusing efforts on GDPR compliance. There are two key steps organisations can use to start asking themselves "Have we crossed this off the list?"

1. Reporting data breaches

The GDPR defines a personal data breach as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed” (Article 4, definition 12).

- Data breaches must be reported within 72 hours of being detected.
- Data processors are liable for any breaches.
- Penalties are determined at a maximum of EURO 20 million or 4% of annual revenue—whichever is greater.

The checklist below is a good head start for organisations to cover their bases with their data breach processes:

Checklist: Reporting Data Breaches

The GDPR will require companies to develop or update internal breach notification procedures to meet the 72-hour reporting requirement.

- ☐ Timely detection of breaches
- ☐ Reporting and alarms
- ☐ Mitigation through automation
- ☐ Investigation capabilities (e.g. case management and forensics)

2. Data protection by design

Under the GDPR, data protection and processing safeguards must become part of the DNA of all systems and processes. Data protection by design is based on 7 foundational principles:

- Proactive not reactive; preventative not remedial
- Privacy as the ‘default’ setting
- Privacy embedded into design
- Full functionality: Positive sum, not zero sum
- End-to-end security: Full lifecycle protection
- Visibility and transparency: Keep it open
- Respect for user privacy: Keep it user-centric

Checklist: Compliance and Data Protection by Design

The GDPR will require companies to rethink how data protection and privacy are met and managed by the organisation.

- ☐ Analyse the gap between current and mandated position
- ☐ Assign required budget and resources
- ☐ Assign a data protection officer if the criteria are met
- ☐ Align with best-practice mandates
- ☐ Review and update data handling procedures
- ☐ Develop a workplace education program

5. In Conclusion: What’s in it for the Organisation?

Beyond of the checklists and the audits, the GDPR is a big picture solution to some very important privacy concerns of today. In its ideal form, the goal of the GDPR is to increase transparency, and greater transparency fosters trust.

People are wary of sharing personal details with companies in fear of where their data will end up. Transparency creates a better understanding and this means companies will need to communicate more openly and provide value to prospects. From the organisation’s standpoint, GDPR should be seen as a huge opportunity to get data storage and handling processes in order. Operations will become more streamlined, efficient, secure, and – most importantly – compliant, so that companies lead a united effort to ensure data privacy for the global good.

Organisations that use this as a competitive tool will be able to cultivate stronger, more trustworthy customer relationships.

We Accelerate Growth

WWW.FROST.COM

Auckland	Colombo	London	Paris	Singapore
Bahrain	Detroit	Manhattan	Pune	Sophia Antipolis
Bangkok	Dubai	Mexico City	Rockville Centre	Sydney
Beijing	Frankfurt	Miami	San Antonio	Taipei
Bengaluru	Iskandar, Johor Bahru	Milan	Sao Paulo	Tel Aviv
Bogota	Istanbul	Mumbai	Seoul	Tokyo
Buenos Aires	Jakarta	Moscow	Shanghai	Toronto
Cape Town	Kolkata	New Delhi	Shenzhen	Warsaw
Chennai	Kuala Lumpur	Oxford	Silicon Valley	Washington D.C.

ABOUT FROST & SULLIVAN

Frost & Sullivan is a growth partnership company focused on helping our clients achieve transformational growth as they are impacted by an economic environment dominated by accelerating change, driven by disruptive technologies, mega trends, and new business models. The research practice conducts monitoring and analyzing technical, economic, mega trends, competitive, customer, best practices and emerging markets research into one system which supports the entire "growth cycle", which enables clients to have a complete picture of their industry, as well as how all other industries are impacted by these factors.

Contact us: Start the discussion

To join our Growth Partnership, please visit www.frost.com

ABOUT LOGRHYTHM

LogRhythm is a world leader in NextGen SIEM, empowering organisations on six continents to successfully reduce risk by rapidly detecting, responding to, and neutralizing damaging cyberthreats. The LogRhythm platform combines user and entity behaviour analytics (UEBA), network traffic and behaviour analytics (NTBA), and security automation and orchestration (SAO) in a single end-to-end solution. LogRhythm's Threat Lifecycle Management (TLM) workflow serves as the foundation for the AI-enabled security operations center (SOC), helping customers measurably secure their cloud, physical, and virtual infrastructures for both IT and OT environments. Built for security professionals by security professionals, the LogRhythm platform has won many accolades, including the 2017 Frost & Sullivan awards for Global SIEM Enabling Tech Leadership and Asia-Pacific Enterprise Security Product Line Strategy Leadership.