Protecting your EU customers

EU General Data Protection Regulation (EU GDPR)
1. **Introduction**

2. **EU GDPR: What is it?**

3. **Potential impact to Australian organisations?**
   - Territorial scope of the EU GDPR
   - Obligation to appoint a Data Protection Officer
   - Privacy governance
   - Risk analysis and Data Protection Impact Assessments (DPIA)
   - Data breach notification
   - Consent
   - Sensitive Information
   - The right to ‘Erasure’
   - Cross border data transfers
   - Data notification
   - Enforcement

4. **Are you prepared?**

5. **Contacts**
Privacy is no longer just a legal, compliance or security issue; it has become a strategic topic at boardroom level and even more so since the proposed EU General Data Protection Regulation (“EU GDPR”) was announced.

For organisations in Australia, understanding the new requirements that the EU GDPR introduces for organisations will be paramount to managing risk exposure.

Our Privacy and Data Protection team will keep you posted of the developments affecting the regulatory framework of privacy and personal data protection in Australia, and can be reached for further information on how best to get prepared in a pragmatic way.

We acknowledge the assistance of Deloitte Belgium in the preparation of this material for Australian organisations.
EU GDPR: What is it?

The EU GDPR are is a set of new data protection requirements that will be enforced from 25 May 2018, replacing existing legislation.

The EU GDPR will potentially move privacy and data protection from organisations having local to global risk exposure.

Organisations will need to shift from just thinking globally, to acting globally.
How does the EU GDPR impact organisations in Australia?

The proposed changes will have a profound impact on the operational and control environment of organisations.

The new Regulation is expected not only to impact organisations within the EU, but also those organisations globally with:

- Operations in the EU
- Third parties operating in the EU
- EU data subjects as customers

Most organisations will be able to attest to the effort and project(s) which were undertaken to prepare for the implementation of the Australian Privacy Principles in March 2014.

Organisations should not underestimate the time it will take to comply with the changes the GDPR brings.
What Australian organisations may need to do

Organisations will need:

- To be more pro-active and have a risk based approach to privacy.
- A monitored approach towards finding out where and which data they are processing or sharing.
“Privacy is an international conversation, particularly as information flows have become more complex, traversing national borders and established regulatory jurisdictions.”

**Timothy Pilgrim,** *Australian Privacy Commissioner,* ‘Privacy directions’ (Speech delivered at the iappANZ Summit, Melbourne, 18 November 2015)
Potential risk exposure areas

Organisations in Australia may need to consider risk exposure across many elements of the proposed EU GDPR. The key elements are explained in the following slides.

Alignment to Australian Privacy Principles:

- New
- Partially similar
- Similar
Territorial Scope of the EU GDPR

The proposed Regulation covers:

• organisations who offer goods or services to individuals in the EU even if the organisations are based outside of the EU, such as Australia.

• non-EU based organisations, conducting monitoring activities in the EU which entail the processing of personal information.

Alignment to Australian Privacy Principles:
Obligation to appoint a Data Protection Officer (DPO)

The proposed Regulation now states that all public authorities will have to appoint a DPO.

In the private sector, companies that:

- Process personal data of more than 5,000 individuals within a year
- Are active in regular and systematic monitoring of individuals
- Process data which is sensitive, location, relating to children, or employee data.

will have the obligation to appoint a DPO. There is currently no such obligation under the Privacy Act 1988 (Cth) in Australia.
Companies should be able to clearly demonstrate that appropriate measures (privacy, security, compliance, and others) have been taken. This is similar to Australian Privacy Principle 1, as part of the Privacy Act 1988 (Cth).

Any general reporting that refers to the company’s activities, such as the issuance of annual reports by publicly traded companies, must contain a summary description of the policies and measures that are being taken to ensure compliance with the personal data requirements of the Regulation. It is currently unclear whether this will apply to organisations operating outside of the European Union.
Risk analysis and Data Protection Impact Assessments (DPIA)

There may now be an obligation to conduct a privacy risk analysis when setting up new business processes.

The personal data management lifecycle should be considered and focus on the controls that protect the accuracy, confidentiality, integrity, physical security and deletion of personal data.

Where the risk analysis indicates a high risk, organisations will be obligated to conduct a Data Protection Impact Assessment (DPIA).

While organisations are not required to perform Privacy Impact Assessments (PIA), it is suggested that a risk analysis or PIA is performed.

“…our focus over the next year, and beyond, will be on issues of governance, and on the integration of privacy in business processes, particularly as we all move to more and more technology-based solutions to everything from information storage to data aggregation.”

Timothy Pilgrim, Australian Privacy Commissioner, ‘Privacy directions’ (Speech delivered at the iappANZ Summit, Melbourne, 18 November 2015)
Data breach notifications

Organisations will have to:

- Notify the supervisory authority of a breach ‘without undue delay’.
- Notify the data subjects if the breach is likely to affect the privacy, rights or legitimate interests of an individual.
- Keep an internal register of the data breaches that have occurred in the organisation.

The obligation to notify individuals may, at the discretion of the regulator, be dropped, if the company can prove that it has taken appropriate means to prevent adverse effects on individuals.

Similarly, Australia has introduced mandatory data breach notification laws which will come into effect February 2018. Under this amendment, organisations will need to notify the regulator and potentially affected individual(s) of an eligible data breach.

Alignment to Australian Privacy Principles:
The requirements for consent remain largely unchanged. However, conditions regarding how consent should be used for processing personal information have been strengthened. Key considerations include:

- Organisations have the burden of proving genuine consent
- Purpose-limited consent
- Allow withdrawal of consent at anytime

It is expected these changes will mitigate the frequent misuse of consent for processing personal data.

Alignment to Australian Privacy Principles:
Sensitive Information

Sensitive personal data has been expanded to also include:

- Gender identity
- Trade union activities
- Administrative or criminal sanctions
- Genetic or biometric data

Alignment to Australian Privacy Principles:
The right to ‘Erasure’

Individuals will have the right to obtain the erasure of their personal data in a limited number of cases. For example, if:

- The data are no longer needed to achieve the purpose of collection
- The individual's consent has been withdrawn
- The data in question have been obtained through unlawful processing

An individual’s right to data erasure may be restricted, for example due to particular legal obligations of an organisation.

There is no similar concept in Australia.

Alignment to Australian Privacy Principles:
Cross border data transfers

The following have been introduced in legislation as appropriate controls to ensure the adequate protection of personal data and do not require a specific Data Protection Authority (DPA) authorisation:

- Model contracts
- Binding Corporate Rules
- European Data Protection Seals (certification)

Where disclosure of personal information is required to non-EU judicial or administrative authorities, the local or “lead” DPA must provide authorisation prior to any disclosure.

In Australia, cross border transfer obligations are outlined in Australian Privacy Principle (APP) 8.

“*If an organisation fails to ensure the protection of personal information disclosed overseas, they can be held accountable.*”

Timothy Pilgrim, Australian Privacy Commissioner, ‘Privacy directions’ (Speech delivered at the iappANZ Summit, Melbourne, 18 November 2015)
“Information flows no longer acknowledge national borders, and can therefore no longer be effectively dealt with by one authority.”

Timothy Pilgrim, Australian Privacy Commissioner, ‘Privacy directions’ (Speech delivered at the iappANZ Summit, Melbourne, 18 November 2015)
Enforcement

Whenever a case relates to multiple jurisdictions or countries, the Data Protection Authority (DPA) of the organisation’s headquarters will assume the lead, coordinate with all other authorities, and endeavour to reach a consensus.

However, the local DPA will remain the sole enforcement authority in its own jurisdiction. In Australia, this would be the OAIC.

Persons who have suffered damage, including non-monetary damage, will have the right to claim compensation from an organisation for the damage.

International enforcement

- Develop international co-operation mechanisms.
- Provide international mutual assistance in the enforcement of legislation.
- Promote the exchange and documentation of personal data protection legislation and practice.

In the event of data protection violations, supervisory authorities will be able to issue a written (public) warning against the infringers, subject them to regular audits, and/or impose fines of up to 4% of their annual worldwide turnover (whichever is greater).

Alignment to Australian Privacy Principles:
The proposed Regulation implies the use of forms and text formats that make sure privacy notices are visible, easy to understand, and communicated in a user-friendly way. For example, the use of a layered privacy statement and the use of standardised icons is encouraged.

In Australia, this is similar to the Data Collections notice required by Australian Privacy Principle 5.
Are you prepared?

- Do we have a process for managing and specifically logging data breaches?
- Is there a process for responding to any global regulatory changes?
- Can we provide access to the information an individual requests?
- Do we have a process to perform a risk analysis or privacy impact assessment for all new or changing business processes?
- Will we be able to erase data when requested?
- Does our privacy policy or data notification contain the required elements under the EU GDPR?
- Do we understand how data flows and where data resides?
- What metrics do we want to report on to measure compliance?
- How much are breaches costing the organisation?
- How much is compliance with the EU GDPR costing us?
- Do we have a role that can fulfil the responsibilities of a Data Protection Officer?
- Have we assessed the risk exposure of the EU GDPR to our organisations?
- How will we ensure all new business processes undergo a risk analysis and/or PIA?
- Do we understand the purposes for which individuals which interact with our organisation provide consent?

Governance

1. Assess
   - Does our privacy policy or data notification contain the required elements under the EU GDPR?
   - Do we understand the purposes for which individuals which interact with our organisation provide consent?
   - Do we understand how data flows and where data resides?

2. Protect
   - Do we have a process to perform a risk analysis or privacy impact assessment for all new or changing business processes?
   - Will we be able to erase data when requested?

3. Monitor
   - Do we have a role that can fulfil the responsibilities of a Data Protection Officer?
   - Have we assessed the risk exposure of the EU GDPR to our organisations?
   - How will we ensure all new business processes undergo a risk analysis and/or PIA?

4. Respond
   - Do we have a process for managing and specifically logging data breaches?
   - Is there a process for responding to any global regulatory changes?
   - Can we provide access to the information an individual requests?
"The internet knows no border—a problem in one country can have a knock-on effect in the rest of Europe…"

European Commission’s Digital Chief, Andrus Ansip
Our team have assisted clients in a range of industries – including the public sector – to embed privacy into business and technology transformation projects, including initial current state assessments through to setting up, managing and delivering privacy transformation and technology programs.

Within Australia, Deloitte has individuals that are privacy and information security subject matter experts and can bring relevant and pragmatic industry expertise.
Appendix A – Privacy thought leadership

Through surveys and interviews with organisations and consumers across Australia, the Deloitte Australian Privacy Index is created each year. The Index ranks industry privacy performance, delivers key trends and offers insights into data breach costs, good practices of privacy-effective organisations and what builds trust with individuals in terms of management of their personal information.

Insights

Deloitte Australian Privacy Index 2017
Trust starts from within

In a data driven economy, organisations need to build trust with their employees as ultimately, employees are the guardians of an organisation’s data.

To offer clarity and insights over common issues, Deloitte released a white paper (‘The not-so new Privacy Principles’) through its Forensic Foresight series of publications. The paper covers the key problems organisations face when considering the Australian Privacy Principles and the impacts upon their operations, including re-identification of desensitised data, cloud and cross-border disclosures.

Organisations are engaging third parties to deliver non-core business services increasing their privacy and data protection risk exposure. How can you involve your third parties to be a part of your first line of defence?

Contacts

Sydney
Tommy Viljoen
Partner
Cyber Risk Services
+61 2 9322 7713
tfviljoen@deloitte.com.au

Sydney
Marta Ganko
National Privacy and Data Protection Lead
Cyber Risk Services
+61 2 9322 3143
mganko@deloitte.com.au

Sydney
David Owen
Partner
Cyber Risk Services
+61 2 9322 7000
dowen@deloitte.com.au

Sydney
Sid Maharaj
Partner
Risk Advisory
+61 2 6263 7160
sidmaharaj@deloitte.com

Melbourne
Greg Janky
Partner
Cyber Risk Services
+61 3 9671 7758
gjanky@deloitte.com.au

Melbourne
Puneet Kukreja
Partner
Cyber Risk Services
+61 3 9671 8328
pkukreja@deloitte.com.au

Brisbane
Craig Mitchell
Partner
Risk Advisory
+61 7 3308 7400
cmitchell@deloitte.com.au

Adelaide
David Hobbis
Partner
Risk Advisory
+61 8 8407 7283
dhobbis@deloitte.com.au