SESSION 4: DATA PRIVACY AND GDPR - NAVIGATING THE NEW ERA OF DATA PROTECTION

WIN In-House Counsel Day Brisbane 2018

Wednesday, 28 February 2018
Navigating the key requirements of EU GDPR for Australian Organisations
Agenda - Key Focus Areas

- Overview of Current Landscape
- EU GDPR - Why important for Australian organisations?
- Comparative view with Australian Privacy Act and APPs
  - Territorial Scope
  - Data Breach Notifications
  - Tougher Sanctions & Fines
  - Data Subject Rights
  - International Transfers
- Key Takeaways
EU General Data Protection Regulation (GDPR)

- The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) enacted by European Parliament, the Council of the European Union and the European Commission to strengthen and harmonise data protection for all EU individuals.

- GDPR in force on 25 May 2018

- NO Transition Period

- Organisations caught by GDPR will need to:
  - map current data collection, use and disclosure;
  - carry out a gap analysis of current privacy compliance and maturity against GDPR; and
  - create and implement a remediation plan, prioritizing high risk areas.
5 key reasons why important for Australian organisations

1. Extra-territorial Scope under Article 3(2)
2. Significant fines for breach – akin to anti-trust fines – up to 2 - 4% of global annual turnover of Group
3. Definition of 'undertaking' – implications for even small, non-participating members of a Group organisation
4. Customers may require compliance through contract – knowledge of your obligations will be key!
5. Brand and Reputational Protection – reviews and maintenance required to determine if caught; put appropriate measures in place to protect
### Key definitions within the GDPR

Key definitions relate to personal data, data subject, data controller / processor and the activity of data processing.

<table>
<thead>
<tr>
<th>Term</th>
<th>EU GDPR Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal data</td>
<td>• Any information relating to an identified or identifiable natural person, who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.</td>
</tr>
<tr>
<td>Special categories of personal data</td>
<td>• A subset of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, the processing of genetic or biometric data in order to uniquely identify a person, or data concerning health, sex life or sexual orientation.</td>
</tr>
<tr>
<td>Data Subject (identifiable person)</td>
<td>• One who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.</td>
</tr>
<tr>
<td>Data Controller</td>
<td>• Natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.</td>
</tr>
<tr>
<td>Data Processor</td>
<td>• Natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.</td>
</tr>
<tr>
<td>Data processing</td>
<td>• Any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.</td>
</tr>
</tbody>
</table>
Territorial scope of the GDPR

The GDPR is very broad in terms of territorial scope. Has extra-territorial jurisdiction over non-EU organisations in certain cases.

Takeaway: Even though this is an EU Regulation, it will have an impact on non-EU organisations.
Territorial Scope of the GDPR

GDPR Article 3 – applies to the processing of personal data:

- in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not;

- of data subjects who are in the Union by a controller or processor NOT established in the Union if:
  - the processing relates to the offering goods or services to individuals in the Union (whether paid or not); or
  - monitoring their behaviour as far as their behaviour takes place in the Union (e.g. profiling; use of cookies).
The GDPR introduces new requirements in 5 key areas

- **Lawful Processing: Operational Requirements**
  - Data Protection by design/default (data security)
  - Data Protection Impact Assessments
  - Golden Record: Records of Processing Activities/Data Inventory

- **Personal Data Security and Breaches**
  - Obligation to notify supervisory authorities
  - Obligation to notify data subjects

- **Lawful Processing: Balancing Organisation v Data Subject Rights**
  - Data Protection Principles
  - Legitimate grounds for lawful processing
  - Rights of data subjects
  - Fairness and transparency

- **Transfers of Personal Data**
  - Intra-group transfers
  - Transfers to third parties
  - Transfers in the context of litigation and investigations

- **Governance, Organisation and Policy Framework**
  - Lead Supervisory Authority
  - Data Protection Officer
  - Risk-based approach to compliance
Data Breach Notification - GDPR

- Under Article 33: the **controller** must:
  - without undue delay, and where feasible, **not later than 72 hours after having become aware of it**, [to] notify the ... breach to the supervisory authority" (Article 33(1))
  - when the personal data breach is likely to result in a **high risk to the rights and freedoms of individuals**, notify the affected individuals "without undue delay" (Article 34)

- **Processors** are required to notify the controller "without undue delay" having become aware of the breach (Article 33(2))

- Recent opinion A29 WP – 'deemed awareness' = immediate notification
Data Breach Notification – Some Practical Implications

- Build up data breach infrastructure to enable prompt, compliant notification
- Requires co-ordinated approach - technology, breach response procedures and staff training
- Technology requirements:
  - combination of firewalls, log recording, data loss prevention, malware detection and similar applications
  - Regular privacy impact assessments and upgrades of technology
- Breach response procedures – test regularly!
- Staff training / Consider privilege and confidentiality
- Cyber insurance
- Develop standard notification procedures
- Appoint advisors now!
Tougher Sanctions – Significant Fines

Data controller and / or data processor failing to comply with the GDPR provisions may be exposed to high administrative fines imposed by data protection authorities.

<table>
<thead>
<tr>
<th>Provision of the GDPR Breached</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Up to EUR 20m</strong> or <strong>up to 4% of the total global turnover in the preceding year (whichever is higher)</strong></td>
</tr>
<tr>
<td><strong>Basic principles governing data processing</strong></td>
</tr>
<tr>
<td><strong>Transferring personal data to third countries (e.g. the US)</strong></td>
</tr>
<tr>
<td><strong>Obligations under the national law adopted pursuant to chapter IX of the GDPR</strong></td>
</tr>
<tr>
<td><strong>Non-compliance with the order to restrict or suspend data processing or flow, temporarily or permanently, issued by the supervisory authority, or failure to provide access resulting in breach</strong></td>
</tr>
<tr>
<td><strong>Up to EUR 10m</strong> or <strong>up to 2% of the total global turnover in the preceding year (whichever is higher)</strong></td>
</tr>
<tr>
<td><strong>Certain obligations of the controller and processor referred to in the GDPR</strong></td>
</tr>
<tr>
<td><strong>Certain obligations of the certification body referred to in the GDPR</strong></td>
</tr>
</tbody>
</table>
Tougher Sanctions – Significant Fines

- Key points to note:
  - **Security and data breach notifications failures** - 10 million Euros or 2% of annual worldwide turnover, potentially for **both** the controller and the processor
  - **Fines can be accumulated** i.e. if other areas of non-compliance, possible that higher cap fines of up to 20 million Euros or 4% of annual worldwide turnover also triggered
  - Revenues of an "**undertaking**" rather than the revenues of the relevant controller or processor (Recital 150 GDPR)
  - **Group revenues** – even if some group companies have nothing to do with the processing of data to which a fine related, provided deemed part of the undertaking
Rights of the data subjects

The GDPR has introduced a set of data subjects' rights - which will be also available to an organisation's clients and staff.

<table>
<thead>
<tr>
<th>Rights of Data Subject</th>
<th>Practical implications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right of access to their data</td>
<td>Publicity surrounding GDPR is likely to increase enforcement of these rights.</td>
</tr>
<tr>
<td>Right to rectification of their data</td>
<td>Significant time and effort required to deliver these rights – e.g.</td>
</tr>
<tr>
<td>Right to erasure (&quot;Right to be forgotten&quot;)</td>
<td>- Subject access requests</td>
</tr>
<tr>
<td>Right to restriction of processing</td>
<td>- Right to erasure</td>
</tr>
<tr>
<td>Right to data portability</td>
<td>Could also be used as leverage in litigation. Increased risk of group action.</td>
</tr>
<tr>
<td>Right to receive a copy of the data</td>
<td></td>
</tr>
<tr>
<td>Right to object to automated individual decision making (including profiling)</td>
<td></td>
</tr>
</tbody>
</table>
When processing personal data of customers, clients and staff, organisations must do so in compliance with the basic principles set out in the GDPR.

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
<th>Practical Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fairness</td>
<td>Personal data shall be processed fairly</td>
<td>Clear and honest communication with data subjects</td>
</tr>
<tr>
<td>Lawfulness</td>
<td>Personal data shall be collected and processed only as permitted by applicable law</td>
<td>There must be a demonstrable legal basis for all processing of personal data (consent, necessary for the performance of a contract, legitimate interests). N.B. Some justifications trigger additional rights</td>
</tr>
<tr>
<td>Transparency</td>
<td>Personal data shall be processed in transparent manner in relation to the data subject</td>
<td>Data subjects should be fully informed about all aspects related to the processing of their personal data</td>
</tr>
<tr>
<td>Purpose Limitation</td>
<td>Personal data shall be processed only for the specified, explicit and legitimate purpose for which it was initially collected</td>
<td>Personal data shall not be processed for additional purposes</td>
</tr>
<tr>
<td>Data Minimisation</td>
<td>Amount of data obtained must be adequate, relevant and limited to what is necessary for the purposes for which data was collected</td>
<td>The less data is processed, the safer this is from the perspective of the EU GDPR. Cannot simply gather data that is &quot;nice to have&quot;</td>
</tr>
</tbody>
</table>
Basic principles governing processing personal data of clients and staff

When processing personal data of clients and staff, organisations must do so in compliance with the basic principles set out in the GDPR.

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
<th>Practical Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy</td>
<td>Personal data must be accurate and kept up-to-date</td>
<td>Processes for checking data quality, and updating personal data, will be required. Self-serve HR databases should help deliver this requirement.</td>
</tr>
<tr>
<td>Time Limitation</td>
<td>Data shall not be processed for any longer than is necessary for the purposes for which it was collected</td>
<td>Do not store data when it is no longer necessary</td>
</tr>
<tr>
<td>Integrity</td>
<td>Data must be protected against unauthorised/unlawful/accidental loss, destruction and damage</td>
<td>Put appropriate security measures in place to protect data (see also technical and organisational measures)</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Data must be protected against unauthorised access</td>
<td>Do not disclose data to third parties without a legal basis for doing so</td>
</tr>
<tr>
<td>Accountability</td>
<td>Data controller shall be able to demonstrate compliance with the EU GDPR</td>
<td>Records of processing activities will need to be kept to demonstrate that data is processed in accordance with the GDPR, including a &quot;Golden Record&quot;</td>
</tr>
</tbody>
</table>
International transfers

The GDPR restricts disclosure of personal data outside of the EU. Transfers are permitted to a limited number of countries enjoying the benefit of an adequacy decision, though these countries may be reviewed in light of the higher standards imposed by GDPR.

Countries with Adequacy Decision:
- Andorra
- Argentina
- Canada
- Switzerland
- Faeroe Islands
- Guernsey
- State of Israel
- Isle of Man
- Jersey
- New Zealand
- United States (EU-US Privacy Shield regime only)
- Eastern Republic of Uruguay
Key takeaways

Scope

- GDPR has a wide extra-territorial scope. It is a challenge for organisations globally in many cases.
- The regulated perimeter is wider: e.g. personal data and processing are defined extremely broadly.

Enforcement & Claims

- Principle based law, but prescriptive articles with vague legal standard coupled with anti-trust scale fines.
- GDPR changes the game for data risk. FS, retail and technology sectors will be likely focus for regulators and privacy activists. Certain factors will heighten risk profile further – e.g. expansion into markets with tougher laws.
- Increased media attention in the run up to May 2018, mandatory data breach notification and enhanced rights of individuals also likely to increase enforcement activity.
- Increased risk of private claims flowing from regulatory action.

Key challenges

- **GDPR Readiness**: several big lifts required including data mapping / inventory; supply chain re-papering; customer and HR notice updating; policy updating; training and creating ongoing governance regime.
- **Time limitation**: significant challenge to align current data retention practices with GDPR time limitation.
- **Strategy**: many important strategic decisions required by organisations. For example: strategy for lawful processing; strategy for breach notification; strategy for responding to subject access requests and other rights.
- **Accountability & Governance**: organisations need to build a governance and accountability infrastructure to ensure readiness for and ongoing compliance with GDPR.
Any questions?
Australian Privacy Act – Mandatory Notifiable Data Breach Regime
Agenda

1. Quick overview of the new regime
2. When do you need to notify?
3. What can you be doing now?
4. Data breach scenarios
Flow chart – when do you need to notify?

No mandatory obligation to notify

Has a data breach occurred that involves Personal Information of Australian citizens?

- Yes
  - Do you suspect that a data breach may have occurred that involves Personal Information of Australian citizens?
    - Yes
      - You will need to undertake a “reasonable and expeditious” assessment. Is a breach identified that involves Personal Information of Australian citizens?
        - Yes
          - Is there a risk of “serious harm”?
            - Yes
              - Remedial actions prevent the risk of harm?
                - No
                  - Does an exemption apply?
                    - Yes
                      - Eligible data breach exists. Obligation to notify.
                    - No
                      - No
                        - No
                          - Eligible data breach exists. Obligation to notify.
                - No
                  - Eligible data breach exists. Obligation to notify.
            - No
              - Remedial actions prevent the risk of harm?
                - No
                  - Eligible data breach exists. Obligation to notify.
                - Yes
                  - Eligible data breach exists. Obligation to notify.
        - No
          - Eligible data breach exists. Obligation to notify.
    - No
      - Eligible data breach exists. Obligation to notify.
- No
  - Eligible data breach exists. Obligation to notify.
What can you be doing now?

- Preparation is key – review and test your response plan:
  - Establish an Incident Response Team (IRT)
  - Revise your internal processes and align with the regime
  - Test your response plan. Develop scenarios relevant to your business and circumstances
  - Regularly review Privacy Commissioner guidance
  - Be familiar with the form of online notification preferred by the regulator:
What can you be doing now?

- Impact on third party arrangements
  - Will a third party eligible data breach = your eligible data breach?
  - Have you assessed intragroup contracts and arrangements for compliance?
  - Have existing third party agreements been amended/assessed for compliance?
  - Have you established clear procedures and communicated those?
What can you be doing now?

- Have you updated your template agreements to reflect the new regime?
- Template clauses should ideally address:
  - Timeframe to notify you of an Eligible Data Breach (ASAP but within 2 business days)
  - Obligations to provide information to you about event
  - Your ability to participate in assessment of the event and remediation plans
  - Process for agreeing who will issue and content of the draft notification
  - Obligation to tell you if there is an investigation about an actual/suspected Eligible Data Breach
Data Breach Scenario A

An employee accidentally sends a data file with customer personal information to an outside entity. They realise their mistake and reach out to the external party to discuss the issue.

- What interim steps can the employee or their employer take to protect customer information?
- What factors should be considered when assessing potential harm to customers?
- Is the company required to notify the OAIC and affected individuals?
- How would the external party deleting the files affect this?

Source: Office of Australian Information Commissioner Online Resources
Data Breach Scenario A

- What interim steps can the employee or their employer take to protect customer information?
  - Consider possible steps to mitigate unauthorised use or disclosure, such as asking the entity to delete the files

- What factors should be considered when assessing potential harm to customers?
  - The nature of the information
  - The identity of the external party in receipt of the information
  - The type(s) of harm might result from unauthorised access to this information

- Is the company required to notify the OAIC and affected individuals?
  - Yes if there has been unauthorised access or disclosure or there are reasonable grounds to believe this has occurred, and there is a risk of serious harm as a result

- How would the external party deleting the files affect this?
  - The risk of harm has been mitigated, the company would not have to notify
Data Breach Scenario B

Malicious software installed on a company website is discovered to have accessed customer payment details from the website which is hosted on the company's overseas service provider's server.

- What interim steps can the company take to protect customer information?
- What factors should be considered when assessing potential harm to customers?
- Is the company required to notify the OAIC and affected individuals?
- How would different uses of the compromised customer data affect the outcome?

Source: Office of Australian Information Commissioner Online Resources
Data Breach Scenario B

- **What interim steps can the company take to protect customer information?**
  - Implement its data breach response plan and perform a risk assessment

- **What factors should be considered when assessing potential harm to customers?**
  - Identify the extent of the breach: are all or only some customers affected? It may be that only people who made purchases within a certain time-frame are impacted
  - The nature of the data, payment information, suggests a risk of financial harm

- **Is the company required to notify the OAIC and affected individuals?**
  - Yes, unauthorised access to some customers' data has been established and it is likely that financial harm may arise
  - Mandatory notification requirements still apply as if the Company held the information itself (even though its service provider and the personal information is held overseas)
  - A statement to the OAIC should be prepared and affected individuals notified

- **How would different uses of the data affect the outcome?**
  - If the data was found not to be able to be used by malicious third parties because, for example, it was well encrypted then notification may not be required
Key Contacts

Sinead Lynch
Special Foreign Legal Counsel, Sydney
T +61 2 9286 8296
sinead.lynch@dlapiper.com

Sharyn Law
Senior Associate, Brisbane
T +61 7 3246 4040
sharyn.law@dlapiper.com