aiia
australian information
industry association

Welcome

Oury Clark

GORDIAN

Agenda

aiia
australian information
industry association

- GDPR is in force now and applies to Australian businesses
- What does GDPR require?
- How does an Australian business comply?
- Action Plan

Oury Clark

GORDIAN

aiia
australian information
industry association

Section 1: GDPR is here

Oury Clark

GORDIAN

Privacy in the digital age

aiia
australian information industry association

"Historically, privacy was almost implicit, because it was hard to find and gather information. But in the digital world, whether it's digital cameras or satellites or just what you click on, we need to have more explicit rules – not just for government but for private companies."

– Bill Gates

Oury Clark

GORDIAN

What is the GDPR?

- The Global Data Protection Regulation (GDPR) approved by the Parliament of the European Union on 14 April 2016 comes into force on 25 May 2018
- Imposes restrictions on the transfer and processing of personal data both within and outside of the EU
- Harmonises Privacy Law across the EU
- Directly applicable
- Protects the fundamental human right of privacy

How does it affect Australian businesses?

aiia
australian information industry association

- Australian businesses are **subject to** GDPR if they:
  - have a presence in the EU; **or**
  - "offer" products or services to EU residents; **or**
  - monitor the behavior of EU residents (e.g. analytics on your website)
- Australian business may also be **required to comply** with GDPR by their customers

Oury Clark

GORDIAN

How does it affect Australian businesses?

aiia
australian information industry association

- Broader, business-wide transformational impact
- Affects the entire supply chain
- Not just - "update my privacy policy"
- Typical compliance project for a small-medium IT business in non-complex environment takes 3-6 months and costs $100 - 200,000
  - costs of creating a GDPR compliant product/service are in addition

Oury Clark

GORDIAN

The intent of GDPR

aiia
australian information industry association

- Extra territorial impact of GDPR is no accident
- Entirely focused on rights of individual
- Trying to generate a broader cultural change
- GDPR acknowledges that there is a potential negative impact on trade
- Transfers of personal data outside the EU are severely restricted
- Many grey areas

Oury Clark

GORDIAN

Data Protection Principles

aiia
australian information industry association

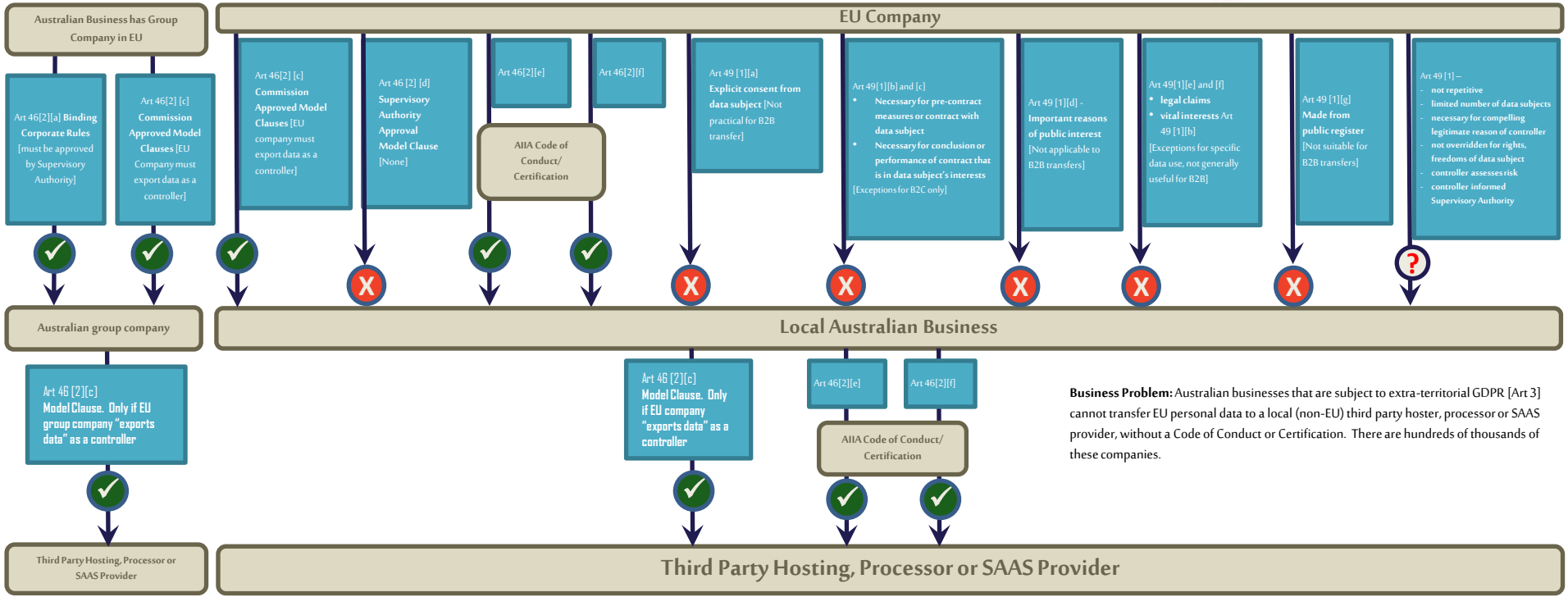
- Lawfulness, fairness and transparency
- Purpose limitations
- Data minimisation
- Accuracy
- Storage limitations
- Integrity and confidentiality
- Underpinned by principle of accountability/demonstrability

Oury Clark

GORDIAN

Transfers of Personal Data from EU Companies to Australian Business

aiia
australian information industry association



Business Problem: Australian businesses that are subject to extra-territorial GDPR [Art 3] cannot transfer EU personal data to a local (non-EU) third party hoster, processor or SAAS provider, without a Code of Conduct or Certification. There are hundreds of thousands of these companies.

Oury Clark

GORDIAN

Likelihood and cost of data breaches

- 1 in 4 chance of a data breach globally
- Average cost of data breach is $3.62m, involves 24,000 records, and costs $141 per record lost

  (source: Ponemon Institute study 2017)

- At least 40% of data subjects will exercise their rights
  - Mainly rights of access and to be forgotten Regulators, individuals and competitors can complain
- 8% of data subjects who exercise their rights will do so just to get revenge

(source: Veritas survey 2017)

Consequences of non-compliance

aiia
australian information industry association

- Need not have a data breach to be in breach of GDPR
- Sanctions:
  - Fines: 4% of global turnover or €20m
  - Stop processing order (Supervisory Authority)
- Collapse of value e.g., Facebook
- Collapse of entire business e.g., Cambridge Analytics

Oury Clark

GORDIAN

Consequences of non-compliance

- Consumers will avoid companies who they don't trust to protect their privacy (OAIC Survey 2017)
  - Biggest risk: online services
  - 58% consumers decided not to deal with business (this percentage is increasing y-on-y)
  - 93% are concerned with overseas transfers
  - Nearly 90% view use for another purpose as being "mis-use"

GDPR Day 1

aiia
australian information industry association

- NOYB makes complaints in 4 countries
  - Facebook ($8.1 BN), Google, Whatsapp, Instagram
  - "lack of real consent"
- Max Schrems privacy activist
  - behind the case that ended the US Safe Habor program
- US news publishers prevent access from EU
  - LA Times
  - Chicago Times
- Yeelight stops smart appliances working

Oury Clark

GORDIAN

Competitive advantage

aiia
australian information industry association

- GDPR compliance can be a differentiator
- Opportunity to create new products and services

Oury Clark

GORDIAN

aiia
australian information
industry association

Section 2: What's in GDPR?

Oury Clark

GORDIAN

Lawful basis of processing

aiia
australian information industry association

- Six lawful purposes:
  1. Consent
  2. Legitimate purpose - needs balancing act
  3. Contract (for the benefit of the data subject)
  4. Legal obligation (not a contract)
  5. Vital interests
  6. Public task

Oury Clark

GORDIAN

Lawful basis of processing

Consent

- freely given, specific, informed, unambiguous, time-bound
- not part of T&Cs, no bundling, no default, not tied to 'no service'
- consent for processing special category data must be "explicit"

Lawful basis of processing

- No data must be processed unless it is "necessary"
  - if there is another reasonable way to process without personal data you MUST do it
  - processing for marketing purposes may be "necessary"

- Anonymisation of data/data aggregation
  - especially were data is not in current use

- No automatic profiling where decisions are made affecting data subject automatically.
  - must disclose rules
  - rules must not be bias

Key Rights under GDPR

aiia
australian information industry association

- New rights:
  - rights to object to certain types of processing
  - right to data portability
  - right to be forgotten/erasure

- Existing rights:
  - right to be informed
  - right of access
  - right of rectification

Oury Clark

GORDIAN

GDPR vs Privacy Act

aiia australian information industry association

Supplied by OAIC	EU GDPR	AUSTRALIAN PRIVACY ACT
Who does this apply to?	Data processing activities of businesses, regardless of size, that are data processors or controllers	Most Australian Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses.
What does it apply to?	Personal data – any information relating to an identified or identifiable natural person: Art 4(1)	Personal information (PI) – information or an opinion about an identified individual, or an individual who is reasonably identifiable: s 6(1)
Jurisdictional link	Applies to data processors or controllers: •with an establishment in the EU, or •outside the EU, that offer goods or services to individuals in the EU or monitor the behaviour of individuals in the EU: Art 3	Applies to businesses: •incorporated in Australia, or •that 'carry on a business' in Australia and collect PI from Australia or hold PI in Australia: s 5B
Accountability and governance	Controllers generally must: •implement appropriate technical and organisational measures to demonstrate GDPR compliance and build in privacy by default and design: Arts 5, 24, 25 •undertake compulsory data protection impact assessments: Art 35 •appoint data protection officers: Art 37	APP entities must take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs and to enable complaints: APP 1.2 Businesses are expected to appoint key roles and responsibilities for privacy management and to conduct privacy impact assessments for many new and updated projects
Consent	Consent must be: •freely given, specific and informed, and •an unambiguous indication of the data subject's wishes which, by a statement or by a clear affirmative action, signifies agreement to processing: Art 4(11)	Key elements: •the individual is adequately informed before giving consent, and has the capacity to understand and communicate consent •the consent is given voluntarily •the consent is current and specific: OAIC's APP GLs
Data Breach notifications	Mandatory DBNs by controllers and processors (exceptions apply): Arts 33-34	From 22 February 2018, mandatory reporting for breaches likely to result in real risk of serious harm
Individual rights	Individual rights include: •right to erasure: Art 17 •right to data portability: Art 20 •right to object: Art 21	No equivalents to these rights. However, business must take reasonable steps to destroy or de-identify PI that is no longer needed for a permitted purpose: APP 11.2. Where access is given to an individual's PI, it must generally be given in the manner requested: APP 12.5
Overseas transfers	Personal data may be transferred outside the EU in limited circumstances including: •to countries that provide an 'adequate' level of data protection •where 'standard data protection clauses' or 'binding corporate rules' apply •approved codes of conduct or certification in place: Chp V	Before disclosing PI overseas, a business must take reasonable steps to ensure that the recipient does not breach the APPs in relation to the information: APP 8 (exceptions apply). The entity is accountable for a breach of the APPs by the overseas recipient in relation to the information: s 16C (exceptions apply)
Sanctions	Administrative fines of up to €20 million or 4% of annual worldwide turnover (whichever is higher): Art 83	Powers to work with entities to facilitate compliance and best practice, and investigative and enforcement powers: Parts IV and V

Oury Clark

GORDIAN

GDPR vs Privacy Act – key points

aiia
australian information industry association

- Explicit detail as to transparency and accountability
- No exceptions for SMEs
- Existing consents may not be valid if not in the GDPR-compliant format
- New rights for data subjects: objection, portability and right to be forgotten
- Notifications to third parties when receive their data from other sources
- Much tighter restrictions on overseas transfers
- Breach timeframes and procedures
- Penalties and remedies

Oury Clark

GORDIAN

aiia
australian information
industry association

Section 3:
Practical application of GDPR

Oury Clark

GORDIAN

Documentation

- Businesses need to document all decisions regarding privacy, including reasons for decisions:
  - Appointing a EU DPO and/or Representative
  - Policies: privacy, security, data retention, collection notices
  - Data Protection Impact Assessment Statements
  - Breach notification process
  - Mandatory Contracts: employees, customers, suppliers, inter-company

Documentation

Decisions should evidence and document balancing rights and freedoms with technical and organisational measures and costs

GDPR – data breach notifications

aiia
australian information industry association

Steps:

- Assess the risk to individuals' rights and freedoms
- Notify:
  - Supervisory Authority within 72 hours (prescribed information)
  - Data subject (high risk only)
  - Other organisations/regulators (if required)
- Document your decision making
- Failure to notify - fine of up to €10m or 2% of global turnover

Oury Clark

GORDIAN

Data breach notification – GDPR comparison with Privacy Act

- Definition of personal data is different
- Does the law apply to me?
  - No SME exclusion under GDPR
- What is a data breach
  - Unauthorised access, disclosure or loss where access or disclosure is likely
- Test for informing individual is different:
  - GDPR – "High risk to the rights and freedoms of individuals"
  - Privacy Act – only notify "eligible data breaches", being "serious harm" (undefined) and "unable to prevent risk of serious harm with remedial action"
- Need to contract through supply chain to ensure prompt notification

Data breach notification – GDPR comparison with Privacy Act

- Notifying Regulator is different
  - GDPR – relevant Supervising Authority (via Representative or DPO)
    - data breaches that are "likely to result in a risk to individual's rights and freedoms"
  - Privacy Act - Office of Australian Information Commissioner
    - "eligible data breaches" only
- Content of notification is different
- Timeframe for notification is different
  - GDPR - 72 hours (not business hours) to notify Supervisory Authority, and individuals without "undue delay". A data processor must inform the data controller "without undue delay".
  - Privacy Act - OAIC - "as soon as practicable", and individual, at least within 30 days.

The European experience to date

- Cost of compliance – nobody budgeted for this
- Renegotiation of contracts is a major hurdle
- General feel amongst business community that baby has been chucked out with the bathwater – 'I am not Facebook'
- Looking for the a silver bullet, but GDPR is a bigger compliance/governance project

The European experience to date

aiia
australian information industry association

- Impact of Brexit?
- Disillusionment with inbox spamming and low uptake of re-consent (possibly as low as 4%)
- Change has largely been driven by demands further up the supply chain

Oury Clark

GORDIAN

The European experience to date

- HR aspect has been an unwanted distraction
- Volume of misinformation and scaremongering
- Changing tone of the regulator – ICO wants to work with business

aiia
australian information
industry association

Section 4: Action Plan

Oury Clark

GORDIAN

Action plan – immediate actions

- **Learn** – understand the Privacy Laws that apply to you; educate executive management and obtain support
- **Budget** – obtain budget for a compliance program
- **Appoint** – a Representative and a DPO (if required); establish a person responsible for privacy within your organisation
- **Collection** – minimize the data you collect and update your collection notices to ensure you are collecting data lawfully
- **Update** - privacy policy, data retention policy, security policy and customer contracts
- **Insurance** - check insurance policies

Action plan – next 12 months

aiia
australian information industry association

- Full data audit
- Start conducting Data Protection Impact Assessments of high risk business activities
- Appoint a DPO if necessary
- Educate all senior management and line managers
- Contract review/renegotiation (all organisations in your supply chain)
- Amend employee agreements and HR policies

Oury Clark

GORDIAN

Action plan – next 12 months

- Internal Governance, e.g.:
  - Internal Privacy Notices
  - Organisational Privacy Standard
  - Data Breach and Security Incident Management Policy
  - Corporate Risk register
  - Data Inventory
  - Subject Access Request Response Policy and Register
  - Data Retention Policy
  - Backup Restoration Policy
  - Internal audit procedure

Action plan – next 12 months

- Technological security measures:
  - pseudonymisation and encryption of personal data and devices
  - maintaining suitable firewalls
  - installing suitable antivirus / malware protection with regularised patched updates;
  - segment networks to reduce single points of failure
  - avoidance of email for sensitive personal data transfers
  - engage of a managed security service provider for testing / detection / response
  - endpoint detection and response technologies
  - regular testing and evaluation of technical and organisational
  - adherence/accreditation to codes of conduct or certifications (ISO 27001, SOC 2)

Action plan – next 12 months

aiia
australian information industry association

- If you have a software product then update it to enable you to easily comply with data subjects' rights:
  - Deletion of data
  - Correction (via self-service)
  - Withdrawal of consent
  - Portability
  - Complaints
- Anonymise data wherever possible

Oury Clark

GORDIAN

Action plan – next 12 months

- Auditable documentation trail
  - Needs to be available to the Supervisory Authority
- Test, review, monitor, improve
- Privacy by Design and Default is the new culture

We can help!

aiia
australian information industry association

- You will need support from different professionals
- Assist you to develop and implement your GDPR strategy
- Work with you to minimise business risks
- Advise on complex areas to find commercial solutions

Oury Clark

GORDIAN

Thank you

Mike Pym
CEO, Gordian Lawyers
Ph: 02 8075 3805

Suite 3, Level 23, MLC Centre
19-29 Martin Place
Sydney NSW 2000 Australia

gordianlawyers.com

Ben Robson
Partner, Oury Clark Solicitors
Ph: +44 (0) 20 7067 4300

10 John Street
London WC1N 2EB
United Kingdom

ouryclark.com