Australian National University

PRIVACY
Awareness

ANU University Legal Office and Privacy Officer

November 2019

PRIVACY

The *Privacy Act 1988* (Cth)
regulates the collection, use & disclosure of

personal information

Privacy law reform

- Most personal information handling requirements have not changed for the University
- New unified, national scheme of privacy principles
- New enforcement powers for the Information Commissioner
- New penalties: up to $1.7m per breach

  (more on this later)

Privacy law reform

- Changes to the Privacy Act commenced in March 2014 and February 2018
- 13 Australian Privacy Principles (APPs)
- Combines and replaces separate public and private sector schemes

Privacy law reform

Objects of the reforms are:

- Protection of privacy
- Promotion of transparency
- Balancing individual privacy, and business and government activities
- Providing consistent national regulation for responsible , transparent information handling
- Provide system for complaints
- implement Australia's international obligations

Privacy law reform

APPs structured to reflect the information life cycle:

- collection
- use and disclosure
- quality and security
- access and correction

How does the Act apply to ANU

- ANU is an institution established for a public purpose under a Commonwealth statute

  The Australian National University Act 1991 (Cth)

- ANU is an **APP entity** and an **agency** under the Privacy Act

Personal Information

"information or an opinion about an identified individual or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not."

Personal Information

- Information or opinion
  - Not limited to fact
- Individuals
  - Living natural persons, any age
- Reasonably identifiable
  - Take cautious approach
- True or not true
  - includes inaccurate information

Personal Information

Also includes:

- sensitive information,
- health information,
- credit information,
- Govt identifiers and Tax File Numbers.

Sensitive Information

Information or an opinion about an individual's:

- Racial or ethnic origin,
- Political, religious or philosophical opinion, belief or affiliation
- Trade or professional affiliation, membership or association
- Sexual orientation or preferences
- Criminal record
- Health, genetic or biometric information or template

Health information

Information or an opinion (that is also personal information) about an individual's:

- health or disability
- health services desired or received
- genetic information
- donation of body, organs, parts or substances
- other information associated with provision of health services

How does it apply?

These are deemed to be acts of the University:

- University employees
  - conduct in the course & scope of employment
- Contracted service providers handling personal information of or for the University
  - conduct consistent with the terms of the contract
  - ANU must include a privacy clause in most agreements

APP 1

Open and transparent management of personal information

- APP entities must manage personal information in an open and transparent way, by having:

➢ a clearly expressed and up to date APP privacy policy

➢ Freely available in a range of formats

➢ Inquiry and complaint handling systems

APP 2: Anonymity & pseudonimity

- APP entities must give individuals the option of interacting anonymously or pseudonymously where practicable
- ANU usually requires people to identify themselves in order to meet requests or provide services

➢ Only collect enough information as is necessary

APP 3: Collection of solicited information

When can ANU collect personal (not sensitive) information?

- where it is reasonably necessary for, or directly related to, the University's functions or activities

Where from?

- From the individual concerned
- If collection is required or authorised by or under a law, from third parties

Sensitive information:

- As above but only with the person's consent (unless an exception appplies)

Collection must be lawful and fair – get consent

APP 4: Unsolicited personal information

What is it?

- Personal information that is not requested or actively acquired

What to do with it?

- Destroy or de-identify unless it forms part of a Commonwealth record
  - Most information created or received by ANU forms part of a Cth record
- Otherwise handle in accordance with the APPs

APP 5: Notice of collection

- At the time of collection, must tell the person:
  - What it will be used for
  - Consequences of not collecting it
  - If it will be disclosed, to whom, and why
  - If it will be stored, transferred or disclosed overseas and if possible, where to
  - Name and contact details of ANU
  - Location of privacy policy and that the policy contains complaint information

APP 6: Use and disclosure

If information is held for a particular purpose, it must not be used or disclosed for another purpose unless:

- The person consents to the secondary use or disclosure
- The use or disclosure is required by law
- A **permitted general situation** applies
- Disclosure is to an enforcement body for enforcement purposes

Permitted general situations (s16A)

- The Privacy Act authorises disclosure without consent in certain circumstances
  - To prevent a serious threat to life, safety or public health
  - To investigate unlawful activity or misconduct
  - To law enforcement for location of persons declared missing
  - In relation to legal proceedings or dispute resolution
  - For diplomatic or defence reasons
- This is a decision for the University – contact the Legal Office – do not disclose without advice

APP 8: Cross-border disclosure

- In combination with other provisions of the Privacy Act, APP 8 introduces accountability for the acts of overseas recipients of personal information, unless an exception applies
- Contracts with overseas providers must usually include
  - a clause that applies the University's privacy obligations and standards to the information recipient
  - An indemnity of $1.7m per occurrence for breach of the privacy obligations

APP 10: Quality of personal information

- Reasonable steps must be taken to ensure that information collected, used and disclosed is accurate, up-to-date, relevant and complete
- 'reasonable steps' depends on the circumstances
  - consequences of error to the individual concerned
  - resources available to the entity for quality control
  - reliability of the source
- More care expected to be taken with sensitive information
- Only disclose relevant information

APP 11: Security of personal information

- Must take reasonable steps to protect information it holds from misuse, interference, loss, unauthorised access, modification or disclosure
- Reasonable steps include
  - Secure storage, controlled access, audit capability, staff training
  - Reasonable steps relative to risk of security breach
- More care expected to be taken with sensitive information
- If the information is no longer needed and is not part of a Cth record - de-identify or destroy

APP 12: Access

- Individuals have the right to access their personal information subject to limitations in the Freedom of Information Act or any other law that authorises the University to refuse access
- Access requests should be directed to

  privacy@anu.edu
- The University must
  - respond to access requests within 30 days
  - If possible, provide access in the manner requested
  - Provide reasons for refusal of access

APP 13: Correction

- Personal information may be corrected if:
  - ANU considers the information is inaccurate, out of date, incomplete, irrelevant or misleading
  - The individual requests, and ANU agrees to make, the correction
  - Free of charge
- Notify any recipients of incorrect information if requested by the individual
- If correction is refused and the individual, a statement of requested correction can be attached to the record at the request of the individual
- Notify the individual of appeal rights - policy
- Refer correction requests to privacy@anu.edu.au

APPs 7 and 9

- APP 7: use of personal information for direct marketing
- APP 9: adoption of government-related identifiers
- These do not apply to the University but may apply to contracted service providers
- Think about covering in the contract clause

Guidelines under section 95 of the Privacy Act 1988 (2014)

- The CEO of the NHMRC may, with the approval of the Commissioner, issue guidelines for the protection of privacy by agencies in the conduct of medical research.

- Acts done by agencies in accordance with these guidelines do not breach the Act.

http://www.comlaw.gov.au/Details/F2014L00245

Guidelines under section 95A of the Privacy Act 1988 (2014)

- Section 95A guidelines provide a framework for HRECs to assess proposals to handle health information without the consent of the subject, for the purposes of research, the compilation or analysis of statistics, or health service management.
- They also require that ethics committees weigh the public interest in those activities against the public interest in the protection of privacy.

http://www.oaic.gov.au/privacy/applying-privacy-law/legally-binding-privacy-guidelines-and-rules/guidelines-under-section-95a-of-the-privacy-act-1988-2014

Enforcement and penalties

The Information Commissioner can:

- Conduct performance assessments and own-motion investigations
- Require privacy impact assessments to be conducted
- Seek enforceable undertakings
- Seek civil penalty orders
  - For serious or repeated interferences with privacy
  - Fines of up to $1.7m (entity) or $340,000 (individual)

Update

- Privacy Impact Assessment Guideline
- The Guidelines on Privacy Impact Assessment provide an essential tool to assist projects and services ensure they comply with the Privacy Act 1988 and they assist with the implementation of good privacy practice.

Data breach response plan

- Procedure - Data breach response plan
- implements the mandatory notifiable data breaches scheme that applies under the Privacy Act 1988.

EU General Data Protection Regulations

- applies to two categories of entities: "controllers" and "processors" of "personal data
- GDPR applies to the extent that a controller or processor **falls within the territorial scope of the GDPR**, if it:
  - has an "establishment" in the EU and processes personal data in the context of the activities of the establishment (Article 3(1)); or

  - offers goods or services to individuals in the EU (Article 3(2)(a)); or
  - monitors the behaviour of individuals in the EU (Article 3(2)(b)).
- There are a number of exceptions in certain circumstances
- To seek advice on specific matters contact the Privacy Officer privacy@anu.edu.au

OAIC Privacy materials

- The OAIC website contains lots of helpful privacy resources for agencies
- www.oaic.gov.au

Acknowledgements

This presentation was made with the assistance of resources from the Office of the Australian Information Commissioner under a creative commons licence