THE UNIVERSITY of ADELAIDE

Legal Compliance Education and Awareness

CRICOS PROVIDER 00123M

Privacy Act 1988

(Commonwealth)

Background

- The *Privacy Act 1988* (Cth) applies to some private sector organisations and Commonwealth government agencies
- State government agencies and universities would be governed by State Privacy laws, however there is currently no South Australian law on Privacy
- Even though there is currently no Privacy law that applies directly to the University, the University has – through its Privacy Policy - elected to adopt the Australian Privacy Principles under the *Privacy Act 1988* (Cth)
- The University is also contractually bound to abide by the Australian Privacy Principles under funding agreements from Commonwealth agencies

What does the Privacy Act do?

- Regulates the way organisations and agencies handle **personal information** of individuals
  - Stricter obligations on **sensitive information**
- Grants individuals rights to
  - Know why their **personal information** is being collected
  - How their **personal information** will be used
  - Who their **personal information** will be disclosed to
  - Ask for access to, or correction of, their **personal information** held by an entity

What does the Privacy Act do? (cont.)

- Regulates credit providers' use of credit-related personal information
- Regulates the collection, use and disclosure of tax file numbers
- Grants powers to the Office of the Australian Information Commissioner to investigate complaints and make orders
- Does not regulate the way individuals handle other individuals' personal information
- Does not apply to personal information of deceased persons

THE UNIVERSITY of ADELAIDE

What is Personal Information?

- **Personal information** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:
  - Whether the information or opinion is true or not; and
  - Whether the information or opinion is recorded in a material form or not
- Examples: name; contact details; date of birth; passport number; emergency contact details; academic record; photographs

THE UNIVERSITY of ADELAIDE

What is Sensitive Information?

Sensitive information means:

- Information or an opinion about an individual's
  - Racial or ethnic origin
  - Political opinions
  - Membership of a political association
  - Religious beliefs or affiliations
  - Philosophical beliefs
  - Membership of a professional or trade association
  - Membership of a trade union
  - Sexual orientation or practices
  - Criminal record

  that is also **personal information**

- health information about an individual
- genetic information about an individual
- biometric information
- biometric templates

Whose personal information does the University collect and deal with?

Most obviously students and staff, but also:

- Titleholders
- Alumni
- Prospective students
- Research participants
- Participants in University outreach activities
- Members of the public who attend University events
- Library patrons
- Other users of University facilities

THE UNIVERSITY of ADELAIDE

How does the Act apply to the University?

- The University adopts the requirements of the Commonwealth Privacy Act, specifically the Australian Privacy Principles (APPs), under its Privacy Policy
- 13 APPs came into force in 2014 and are 'best practice' privacy standards in Australia (replaced previous National Privacy Principles)
- The University has contracts with Government organisations that require compliance with the APPs
-
- The *Higher Education Support Act 2003* (Cth) imposes privacy obligations on the University regarding to student personal information that are consistent with the APPs

The APPs and University's Public Policy

The following slides provide a summary of the APPs and how they are reflected in the University's Privacy Policy.

Guidance to staff on practical application and procedures is provided in the Privacy Management Plan. Staff – particularly those who deal with personal information - should familiarise themselves with both the Privacy Policy and the Privacy Management Plan.

APP 1: Open and transparent management of personal information

- Entities must have a clearly expressed and up-to-date privacy policy
- Entities must implement practices that will ensure compliance with the APPs

❖ Adopted in University Privacy Policy principles 1 & 2

APP 2: Anonymity and pseudonymity

- Entities must give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

❖ Adopted in University Privacy Policy principle 1(g)

The APPs and University's Public Policy (cont.)

APP 3: Collection of solicited personal information

- Outlines when an entity can collect personal information that is solicited
- Applies higher standards to the collection of **sensitive information**

❖ Adopted in University Privacy Policy principle 1(a), (b) & (c)

APP 4: Dealing with unsolicited personal information

- Limits entities' ability to retain unsolicited personal information (e.g. information received in error or not requested by the entity)

❖ Adopted in University Privacy Policy principle 1(f)

The APPs and University's Public Policy (cont.)

APP 5: Notification of the collection of personal information

- When collecting personal information, entities must notify the individual of certain details about that collection

❖ Adopted in University Privacy Policy principle 1(e)

APP 6: Use or disclosure of personal information

- Entities must only use or disclose personal information for the purposes made known to the individual, or a directly related purpose.
- Some exemptions apply (e.g. disclosure required by law)

❖ Adopted in University Privacy Policy principle 2(a),(b),(c) & (d)

The APPs and University's Public Policy (cont.)

APP 7: Direct marketing

- Entities may only use or disclose personal information for direct marketing purposes if certain conditions are met
- Direct marketing = issuing marketing or promotional materials to the individual by hardcopy or electronic means

❖ Adopted in University Privacy Policy principle 2(g)

APP 8: Cross-border disclosure of personal information

- Outlines the steps an entity must take to protect personal information before it is disclosed overseas

❖ Adopted in University Privacy Policy principle 2(e) & (f)

The APPs and University's Public Policy (cont.)

APP 9: Adoption, use or disclosure of government related identifiers

- Entities may not adopt a government related identifier (e.g. Tax File Number, passport number) of an individual as its own identifier

- Not specifically adopted in University Privacy Policy, however university practice of assigning own ID numbers to staff and students ensures compliance

APP 10: Quality of personal information

- Entities must take reasonable steps to ensure the personal information they collect and use is accurate, up to date and complete

- Adopted in University Privacy Policy principle 3

- The University provides various online self-serve portals that enable staff, students and alumni to update their own personal information

The APPs and University's Public Policy (cont.)

APP 11: Security of personal information

- Entities must take reasonable steps to protect personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure
- If no longer required, entities must take steps to destroy or de-identify the personal information

❖ Adopted in University Privacy Policy principle 3

APP 12: Access to personal information

- Entities must, upon request, provide an individual with access to his/her own personal information held by the entity

❖ Adopted in University Privacy Policy principle 4

APP 13: Correction of personal information

- Entities must make corrections to personal information if requested by the individual or if the entity discovers any errors.

❖ Adopted in University Privacy Policy principle 4(d),(e) & (f)

THE UNIVERSITY of ADELAIDE

Loss or unauthorised disclosure of personal information

- This may occur in a variety of ways, whether inadvertent, deliberate or malicious, e.g.
  - mistakenly emailing a list of student bank details to someone else instead of Student Finance
  - loss or theft of laptops or removable storage devices containing personal information collected form research studies
  - University databases being hacked

THE UNIVERSITY of ADELAIDE

Loss or unauthorised disclosure of personal information (cont.)

- Data breaches have potential to result in harm to the individuals affected and expose the University to legal, financial or reputational risk
- If you become aware of a data breach, immediately notify your area manager
- Your area manager must:
  - take immediate action to contain the data breach
  - Notify the Manager, Compliance in Legal & Risk branch
- If there is a real risk of serious harm to the affected individuals, notification must be provided to the individuals to enable them to take steps to minimise adverse impact

Top 10 tips for privacy compliance

1. Only collect personal information to the extent necessary for the University's functions or activities

    - Will de-identified data be sufficient?
    - Are there categories of information you don't need?
    - Don't collect information 'just in case' it might come in useful

2. When collecting personal information, provide a Privacy Statement (refer Privacy Management Plan section 2.2) to the individual

3. Be extra careful when collecting **sensitive information**

Top 10 tips for privacy compliance (cont.)

4. Only use or disclose personal information for the purposes it was collected unless you are confident that an exemption applies

   - e.g. if a Government organisation requests it pursuant to a law that authorises them to obtain information
   - e.g. police requests it under a warrant

5. Do not use personal information to issue direct marketing materials unless the individual has consented or would reasonably expect it

   e.g. if someone registers to attend an event, do not then send them marketing materials unless they have asked to be added to your mailing list

6. Consult with Legal & Risk branch before disclosing personal information to parties located overseas – some due diligence and a written contract will be necessary

Top 10 tips for privacy compliance (cont.)

7. Store personal information securely. Don't share it with others who aren't authorised, and don't access any personal information that you aren't authorised to

8. If you no longer require the personal information, consider disposal in accordance with University recordkeeping requirements (see Records & Archives Management Handbook)

   - do not retain personal information longer than you need to

9. Notify the Manager, Compliance in Legal & Risk Branch of any privacy complaints

10. Immediately notify your area manager if you become aware of any data breaches involving personal information (loss or unauthorised disclosure)

THE UNIVERSITY of ADELAIDE

What can happen if we don't comply?

Individual consequences

Even though the *Privacy Act* does not impose any personal liability, a breach of University's Privacy Policy may have the following consequences:

- constitute misconduct and may result in disciplinary action taken by the University
- unauthorised disclosure of student personal information may constitute a breach of *Higher Education Support Act* → criminal penalties (up to 2 years jail)

THE UNIVERSITY of ADELAIDE

What can happen if we don't comply? (cont.)

University consequences

Even though the Office of the Australian Information Commissioner does not have jurisdiction to investigate the University for privacy breaches, the following consequences are possible:

- Non-compliance with Privacy Act may constitute a breach of some Government contracts → loss of funding
- Negative publicity
  - Damage to University reputation
  - Attraction & retention of staff & students is compromised
- Aggrieved persons may sue on other legal grounds (e.g. breach of contract, negligence)

Additional Resources

- Ben McKay, Legal Counsel
  - 8313 0065
- Richard Duddy, Legal Counsel
  - 8313 0085
- University of Adelaide Privacy Policy and Privacy Management Plan
- Privacy Act 1988 (Cth) and Australian Privacy Principles
- Office of the Australian Information Commissioner
  - APP Guidelines
- University of Adelaide Records & Archives Management Handbook

THE UNIVERSITY of ADELAIDE

Disclaimer

The content of this material is intended only to provide a summary and general overview of the Privacy Act as it applies to the University of Adelaide.

It is not intended to be comprehensive nor does it constitute legal advice.

You are advised to refer to the University's Privacy Management Plan for further guidance.

Please contact Legal & Risk branch if you are unsure of your compliance obligations under this Act