**Assignment Q1**

**Summary:**

Both GDPR and Australian Privacy Act are two significant privacy regulations.

GDPR aims to strengthen data protection and privacy rights for individuals, encourage transparency and accountability from organizations, and foster a culture of responsible data handling.

The Australian Privacy Act aims to protect the privacy of individuals and promote responsible handling of personal information by organizations. It provides individuals with rights and avenues for redress, establishes obligations for organizations, and sets standards for the handling of personal information.

Although GDPR and Australian Privacy Act have different implement ways that in different areas, but all of them aim to maintain and protect the right of individual privacy.

**Overview of GDPR and Australian Privacy Act**

The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros[[1]](#footnote-27800).

The General Data Protection Regulation applies to Personal data, sensitive personal data, controllers and processors.

There are 7 key principles of GDPR[[2]](#footnote-28272):

* Lawfulness, fairness and transparency
  + Lawfulness means that controllers and processors cannot do anything with the personal data which is unlawful in a more general sense
  + Fairness means that processing must be done in ways that people would reasonably expect and not in ways that have unjustified adverse effects on them
  + Transparent processing means being clear, open and honest with data subjects from the start about by whom and how data are handled
* Purpose limitation
  + The purposes for the processing must be specified to ensure that the reasons for processing are clear and open, and in line with the reasonable expectations of the individuals concerned
* Data minimization
  + Organizations should not collect more personal information than they need from their users.
* Accuracy
  + Data must be ‘accurate’, ‘kept up to date’ and ‘erased or rectified’ when inaccurate
* Storage limitation
  + Personal data must be kept in a form that makes it possible to identify data subjects for no longer than is necessary for the purposes of the processing.
* Integrity and confidentiality
  + Personal data must be protected against unauthorized or unlawful processing as well as accidental loss, destruction or damage.
* Accountability
  + Documenting how personal data is handled and the steps taken to ensure only people who need to access some information are granted access.

There are also 8 individual rights in GDPR:

* The right to be informed
* The right of access
* The right to rectification
* The right to erasure
* The right to restrict processing
* The right to data portability
* The right to object
* The rights around automated decision making and profiling

Australian Privacy Act (The Privacy Act 1988) was introduced to promote and protect the privacy of individuals and to regulate how Australian Government agencies and organizations with an annual turnover of more than $3 million, and some other organizations, handle personal information[[3]](#footnote-5452).

There are 13 Australian Privacy principles[[4]](#footnote-28185):

* Open and transparent management of personal information
  + Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.
* Anonymity and pseudonymity
  + Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.
* Collection of solicited personal information
  + Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of ‘sensitive’ information.
* Dealing with unsolicited personal information
  + Outlines how APP entities must deal with unsolicited personal information.
* Notification of the collection of personal information
  + Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.
* Use or disclosure of personal information
  + Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.
* Direct marketing
  + An organization may only use or disclose personal information for direct marketing purposes if certain conditions are met.
* Cross-border disclosure of personal information
  + Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.
* Adoption, use or disclosure of government related identifiers
  + Outlines the limited circumstances when an organization may adopt a government related identifier of an individual as its own identifier or use or disclose a government related identifier of an individual.
* Quality of personal information
  + An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.
* Security of personal information
  + An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorized access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.
* Access to personal information
  + Outlines an APP entity’s obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.
* Correction of personal information
  + Outlines an APP entity’s obligations in relation to correcting the personal information it holds about individuals.

**Comparison between GDPR and Australian Privacy Act**

Both laws place a general obligation to keep data secure. For the most part, however, they stop short of mandating methods by which to do this.

***Similarities***

1. Fairness and Lawfulness: Lawfulness means that controllers and processors cannot do anything with personal data which is unlawful in a more general sense.
   1. Both GDPR and Australian Privacy Act demand the organization should use legal ways to collect and process individual data.
2. Protected target: To alter how businesses and other organizations can handle information of those that interact with them.
   1. Both GDPR and Australian Privacy Act aim to protect individual’s privacy right.
3. Security: Personal data must be protected against unauthorized or unlawful processing as well as accidental loss, destruction or damage.
   1. Both GDPR and Australian Privacy Act use appropriate ways to protect personal data, keep away from unauthorized access and data breach.
4. Transport overseas: ensure personal data has been protected when transport overseas.
   1. Both supply the protection and regulation regarding transport individual data overseas.
5. Report and supervision: there should be some institutions to supervise the organizations and handle the report of data breaches.
   1. Both established supervision institutions to manage and handle individual reports and breach behaviors.

***Differences***

1. Scope: the scope of two regulations may be various in some fields.
   1. The GDPR is executed in Europe, but The Australian Privacy Act is valid in Australia. Different areas have various laws of privacy.
   2. GDPR aims to process individual personal data in EU, Australia Privacy Act applies to the government institutions and firms.
2. Privacy principles: Obviously they comply with totally different principles.
   1. GDPR uses 7 European Privacy Principles, Australia Privacy Act complies 13 Australian Privacy Principles.
3. Fines: If there are data breaches or privacy security issues, the regulations conduct fines to the organizations which break the principles.
   1. GDPR gives more Fines to whom breach the regulations than Australia Privacy Act.
4. Individual rights: Individual should have the vary rights to determine, access and disclose to their personal data.
   1. GDPR supplies more individual rights like the right of access and the right of erasure than Australia Privacy Act.
5. Notification: If there are data breaches, the organizations should have responsibility to notify the relevant institutions and individuals.
   1. GDPR demands when there is a data breach, the organization should report to the privacy supervisor institution and notify it to individual in 72 hours (about 3 days).
   2. Australian Privacy Act demand when there is a data breach that causes critical impact, the organization should report to individual and security office.

**Your thoughts on the difference between GDPR and Australian Privacy Act**

Different areas or countries have different cultures and principles about privacy. It is not appropriate to apply certain regulations to the whole world. GDPR is the newest regulation of privacy recently. So, it has much improvement and more scope than Australian Privacy Act. I think GDPR is better than Australian Privacy Act in some fields. For example, GDPR has a wider scope than Australian Privacy Act. It means GDPR can cover more fields and protect almost all individual privacy. Nowadays, people use the internet every day. Privacy breaches are the most significant issue of internet privacy. GDPR conducts more penalties to those who breach the regulations. That is a good way to resolve the privacy breaches issue. No matter which regulation has been implemented now, all of them aim to protect individual privacy. Although Australian Privacy Act was published in 1988, it is still improving and become more and more completed.

**References**

1. <https://gdpr.eu/what-is-gdpr/>
2. <https://moodle.uowplatform.edu.au/pluginfile.php/4094293/mod_resource/content/2/WG%20CSIT970%20W9%20AUT2023.pdf>
3. <https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act#:~:text=The%20Privacy%20Act%201988%20was,other%20organisations%2C%20handle%20personal%20information>.
4. <https://moodle.uowplatform.edu.au/pluginfile.php/4094293/mod_resource/content/2/WG%20CSIT970%20W9%20AUT2023.pdf>

1. [↑](#footnote-ref-27800)
2. [↑](#footnote-ref-28272)
3. [↑](#footnote-ref-5452)
4. [↑](#footnote-ref-28185)