Comparing privacy laws:
GDPR v. Australian Privacy Act

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE
CLYDE&CO

About the authors

OneTrust DataGuidance™ provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk, and achieve global compliance.

OneTrust DataGuidance™ Regulatory Research includes focused guidance around core topics (i.e. GDPR, data transfers, breach notification, among others), Cross-Border Charts which allow you to compare regulations across multiple jurisdictions at a glance, a daily customised news service, and expert analysis.

These tools, along with our in-house analyst service to help with your specific research questions, provide a cost-effective and efficient solution to design and support your privacy programme.

Clyde & Co is a global law firm providing a complete service to clients in its core sectors of insurance, transport, energy, infrastructure and trade & commodities in a range of areas, in particular, cyber, risk under the Risk, Resillience and Response practice group, and privacy. With over 2,500 legal professionals operating from over 50 offices and associated offices across six continents, Clyde & Co offers a comprehensive range of legal services and advice to businesses operating at the heart of global trade and commerce.

Contributors

OneTrust DataGuidance™
Angela Potter, Holly Highams, Tooba Kazmi, Angus Young, Kotryna Kerpauskaite, Theo Stylianou, Victoria Ashcroft, Alexis Kateifides

Clyde & Co
Alec Christie, James Wong

Image production credits:

Cover/p.5/p.51: cnythzl / Signature collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com
Scale key p6-49: enisaksoy / Signature collection / istockphoto.com
Icon p.33-40: AlexeyBlogoodf / Essentials collection / istockphoto.com
Icon p.47-51: cnythzl / Signature collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com

Table of contents

Introduction

On 25 May 2018, the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') came into effect. The Privacy Act 1988 (Cth) ('the Privacy Act') is Australia's consolidated data protection law (although 'privacy' not 'data protection' is not terminology used in Australia) which aims to promote the protection of individuals' privacy. Given the Australian practice of using the Australian Privacy Principle ('APP') Guidelines issued by the Office of the Australian Information Commissioner ('OAIC') to interpret and apply the Privacy Act, comparable to the Recitals of the GDPR, the guide also refers to relevant APP Guidelines provisions.

In particular, both laws are comprehensive in nature regarding material and territorial scope. For example, the Privacy Act refers to personal information which, in practice, is a similar concept to personal data under the GDPR, and both define special categories of data, as well as include specific requirements for the processing of such data. Furthermore, the GDPR outlines similar requirements to the Privacy Act in relation to its extraterritorial scope, and both texts include comparable provisions in relation to the right to access and the right to be informed.

Nevertheless, there are some key differences between the GDPR and the Privacy Act. In particular, the Privacy Act does not distinguish between data controllers and data processors. In addition, the GDPR contains provisions outlining the legal basis of processing, whereas the Privacy Act provides that personal information may only be collected by fair and lawful means, and for purposes relating to the entity's functions and activities. Moreover, the Privacy Act does not explicitly provide individuals with some of the key data subject rights provided by the GDPR, including the right to erasure, the right to object, and the right to data portability.

Further differences can be found in relation to the obligations of controllers and processors. For instance, the GDPR requires that data controllers and data processors maintain a record of their processing activities, conduct a data protection impact assessment ('DPIA'), and appoint a data protection officer ('DPO') in certain circumstances, whereas the Privacy Act does not contain similar provisions. In addition, whilst both the GDPR and the Privacy Act provide for monetary and administrative penalties, the stated amounts of the fines under each differ significantly, although in practice the civil penalties under the Privacy Act may be applied such that in large scale serious interferences with privacy, the amount of the fines under each may be similar. Also, there is no direct cause of action for individuals to seek compensation under the Privacy Act; individuals must first submit a complaint to the OAIC.

At the time of writing the Privacy Act is the subject of a review being conducted by the Australian Government's Attorney-General's Department. This review could lead to significant reform of the Privacy Act, including broader general application, altered exemptions and/or new rights for individuals in line with GDPR requirements.

This guide is aimed at highlighting the similarities and differences between these two key pieces of legislation in order to assist organisations in complying with both.

Structure and overview of the Guide

This Guide provides a comparison of the two pieces of legislation on the following key provisions:

1. Scope
2. Key definitions
3. Legal basis
4. Controller and processor obligations
5. Individuals' rights
6. Enforcement

Each topic includes relevant articles and sections from the two laws, a summary of the comparison, and a detailed analysis of the similarities and differences between the GDPR and the Privacy Act, with reference to the APP Guidelines.

Key for giving the consistency rate

Consistent: The GDPR and the Privacy Act bear a high degree of similarity in the rationale, core, scope, and the application of the provision considered.

Fairly consistent: The GDPR and the Privacy Act bear a high degree of similarity in the rationale, core, and the scope of the provision considered; however, the details governing its application differ.

Fairly inconsistent: The GDPR and the Privacy Act bear several differences with regard to scope and application of the provision considered, however its rationale and core presents some similarities.

Inconsistent: The GDPR and the Privacy Act bear a high degree of difference with regard to the rationale, core, scope and application of the provision considered.

Usage of the Guide

This Guide is general and educational in nature and is not intended to provide, and should not be relied on, as a source of legal advice. The information and materials provided in the Guide may not be applicable in all (or any) situations and should not be acted upon without specific legal advice based on particular circumstances.

1. Scope

Fairly inconsistent

1.1. Personal scope

The GDPR applies to data controllers and data processors, which may be businesses, institutions, public bodies, as well as not-for-profit organisations. The Privacy Act on the other hand does not distinguish between data controllers and data processors and applies to all 'APP entities' (that may be public authorities or private organisations, including not-for-profit organisations).

Both pieces of legislation protect living individuals in relation to their personal data. However, the Privacy Act does not provide a definition of 'data subject' but does provide a definition of 'individual' which is the subject of the protections under the Privacy Act.

GDPR Articles 3, 4(1) Recitals 2, 14, 22-25	The Privacy Act Sections 6, 80G(2)

Similarities

The GDPR **only** protects **living individuals**. The GDPR **does not** protect the personal data of deceased individuals, this being left to Member States to regulate.

The Privacy Act protects the personal information of '**individuals**,' defined as 'natural persons.' While not specifically noted, as an 'individual' implies a living person, the Privacy Act does not (except as specifically noted) apply to the information of or about deceased persons.

The APP Guidelines clarify that the definition of 'personal information' refers to an opinion about 'a natural person.' The ordinary meaning of a 'natural person' does not include deceased persons. However, information about a deceased person may include information about a living individual and be 'personal information' for the purposes of the Privacy Act.

The GDPR **applies** to data controllers and data processors that may be **public bodies**.

The Privacy Act **applies** to all APP entities (that may be **public authorities** or private organisations, including not-for-profit organisations).

Differences

The GDPR defines a **data controller** as a 'natural and legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.'

The Privacy Act **does not** distinguish between data controllers and data processors under the Privacy Act. All APP entities are subject to the same obligations under the Privacy Act (i.e. whether a data controller or a dataprocessor). The

GDPR	The Privacy Act
Differences (cont'd)	
	Privacy Act defines '**APP entity**' as an agency or organisation. 'Agency' is further defined to mean Federal public authorities outlined under Section 6 of the Privacy Act (e.g. Australian Government departments). 'Organisation' is defined to include an individual, a body corporate, a partnership, any unincorporated associated or a trust (that is not a small business operator, unless 'trading' in personal information or a health service, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory).
The GDPR defines a **data processor** as a 'natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.'	The Privacy Act **does not** distinguish between data controllers and data processors.
The GDPR provides that it 'should apply to natural persons, **whatever their nationality or place of residence**, in relation to the processing of their personal data.'	The Privacy Act **does not** explicitly refer to nationality or place of residence. However, personal information processed by an APP entity will be subject to the Privacy Act.
Article 4(1) of the GDPR clarifies that a **data subject** is 'an identified or identifiable natural person.'	The Privacy Act **does not** provide the definition of data subject but provides a definition of 'individual' which means a natural person.

1.2. Territorial scope

With regard to extraterritorial scope, the GDPR applies to data controllers and data processors that do not have a presence in the EU where processing activities take place in the EU. Similarly, the Privacy Act applies to acts or practices engaged in by organisations outside of Australia that have an Australian link.

GDPR	The Privacy Act
Articles 3, 4, 11 Recitals 2, 14, 22-25	Sections 4, 5A, 5B, 6

Similarities

The GDPR applies to organisations that have a presence in the EU, notably entities that have an '**establishment**' in the EU. Therefore, the GDPR applies to the processing of personal data by organisations **established** in the EU, regardless of **whether the processing takes place in the EU or not**.

In relation to **extraterritorial scope**, the GDPR applies to the processing activities of data controllers and data processors that **do not have any presence in the EU**, where processing activities are related to the **offering of goods, or services to individuals in the EU, or to the monitoring of the behaviour of individuals in the EU**.

The Privacy Act applies to **APP entities** and extends to all of Australia's **external Territories**. An APP entity means an agency or organisation.

The Privacy Act also applies to an act done, or practice engaged in, or **outside Australia (and Australia's external Territories**) by an organisation, or small business operator (in certain circumstances), that has an **Australian link**.

An organisation or small business operator may have an **Australian link** if the organisation or small business operator is:

- an **Australian citizen**;
- a person whose **continued presence in Australia** is not subject to a limitation as to time imposed by law;
- a **partnership formed in Australia** or an Australian external Territory;
- a **trust created in Australia** or an Australian external Territory;
- a **body corporate incorporated in Australia** or an Australian external Territory; or
- an unincorporated association that has its **central management and control in Australia** or an Australian external Territory.

An organisation or small business operator may also have an **Australian link** if the following apply:

- the organisation or operator **carries on business in Australia or an Australian external Territory**; and

GDPR	The Privacy Act

Similarities (cont'd)

	• the **personal information was collected or held** by the organisation or operator in Australia or an Australian external Territory, **either before or at the time** of the act or practice. The APP Guidelines state that the phrase 'carries on business in Australia' focuses on whether the activity is undertaken in Australia as part of the entity's business. Factors that may be considered in assessing if an entity carries on business in Australia include whether: • the entity has a place of business in Australia; • individuals who undertake business acts for the entity are located in Australia; • the entity had a website that offers goods or services to countries including Australia; • Australia is one of the countries on the drop-down menu appearing on the entity's website; • web content that forms part of the business, was uploaded by or on behalf of the entity, in Australia; • business or purchase orders are acted upon in Australia; or • the entity is the registered proprietor of trademarks in Australia. However, the APP Guidelines note that the presence or absence of one of the above factors may not be determinative in assessing whether an entity carries on business in Australia. For example, where an entity does not have a place of business in Australia, this does not necessarily mean that it does not carry on business in Australia. The APP Guidelines clarify that personal information collected 'in Australia' means information collected from an individual who is physically present in Australia or an Australian external Territory, regardless of where the collecting entity is located or incorporated. For example, the collection of personal information from an individual who is physically located via a website that is hosted outside Australia and owned by a company located outside of, or that is not incorporated in, Australia, is collection in Australia.

Differences

Not applicable.	Not applicable.

1.3. Material scope

The GDPR defines 'personal data,' while the Privacy Act defines 'personal information,' which in practice is considered to be a similar concept as both relate to information regarding an identified or identifiable individual. In addition, both pieces of legislation provide a list of information that is regarded as 'sensitive' and provide specific requirements for the processing of sensitive data. Furthermore, both laws exempt personal data processing for personal, household or journalistic purposes.

While the GDPR explicitly excludes anonymised data from its application, the Privacy Act does not. However, anonymised data does not fall within the definition of 'personal information,' and therefore is not subject to the obligations of the Privacy Act.

GDPR	The Privacy Act
Articles 2-4, 9, 26 Recitals 15-21, 26	Sections 6, 6C, 16, 7B

Similarities

The GDPR applies to the '**processing**' of personal data. The definition of 'processing' covers 'any operation' performed on personal data 'such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.'

The Privacy Act applies to '**the collection, holding, use or disclosure of personal information**' **by an APP entity**. However, the Privacy Act does not use the term or provide a definition of 'processing.'

The GDPR defines '**personal data**' as 'any information' that directly or indirectly relates to an identified or identifiable individual. The GDPR does not apply to the personal data of deceased persons.

The Privacy Act defines '**personal information**' as information or an opinion about an identified individual, or an individual who is reasonably identifiable, irrespective of whether the information or opinion is true or not, and regardless of whether it is recorded in a material form or not. While not specifically noted, as an 'individual' implies a living person, the Privacy Act does not (except as specifically noted) apply to the information of or about deceased persons.

The APP Guidelines clarify that the definition of 'personal information' refers to an opinion about 'a natural person.' The ordinary meaning of a 'natural person' does not include deceased persons. However, information about a deceased person may include information about a living individual and therefore be 'personal information' for the purposes of the Privacy Act.

GDPR	The Privacy Act
Similarities (cont'd)	
The GDPR defines '**special categories of personal data**' as personal data revealing **racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation**. The GDPR also provides specific requirements for its processing.	The Privacy Act defines '**sensitive information**' as 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, genetic information that is not otherwise health information about an individual, biometric information that is to be used for the purpose of automated biometric verification or biometric identification and biometric templates**. The Privacy Act provides for additional requirements (on top of those for other personal information) for the collection, use and disclosure of sensitive information.
The GDPR **excludes** from its application the processing of personal data by individuals for **purely personal or household purposes**. This is data processing that has 'no connection to a professional or commercial activity.'	The Privacy Act **excludes** from its application the collection, holding, use or disclosure of personal information by an individual, or personal information held by an individual, only for the purposes of, or in connection with, his/her **personal, family or household affairs**. Likewise, an act done, or practice engaged in, by an individual is exempt from the application of the Privacy Act if the act is done, or the practice is engaged in, **other than in the course of a business carried on by the individual**.
The GDPR provides requirements for specific processing situations including processing for **journalistic purposes and academic, artistic or literary expression**.	The Privacy Act provides an exemption for acts done and practices engaged in by organisations **in the course of journalism**.
The GDPR excludes **anonymous data** from its application, which is defined as information that does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.	While the Privacy Act does not explicitly exclude anonymous information from its application, **the definition of 'personal information' does not include anonymous information** so it is not subject to or covered by the Privacy Act.
The GDPR **excludes** from its application data processing in the context of **law enforcement or national security**.	The Privacy Act **does not** contain a direct equivalent to this exclusion, but there are some exclusions from certain obligations for these in certain circumstances.

GDPR	The Privacy Act
Differences	
The GDPR applies to the processing of personal data **by automated means or non-automated means if the data is part of a filing system**.	The Privacy Act **does not** differentiate between the collection, holding, use or disclosure of personal information by automated and non-automated means.
The GDPR **does not** include a general exemption where personal data is an employee record.	Under the Privacy Act, acts done or practices engaged in by an organisation directly relating to a current or former employment relationship between the organisation and an individual and/or an **employee record** held by the organisation relating to the employee is generally **exempt from the requirements of the Privacy Act** (once the relevant information has been collected). Employee records are defined to include personal information about the engagement, training, disciplining, resignation, termination, conditions of employment, performance/conduct, salary/wages, leave, taxation and/or banking/superannuation affairs of an employee when processed by the employer.
The GDPR **does not** make an exemption available to small businesses.	Under the Privacy Act an individual, body corporate, partnership, other incorporated entity or trust that is a '**small business operator**' is not an 'organisation' and thus not an 'APP entity' subject to most requirements of the Privacy Act. A 'small business operator' is an individual, body corporate, partnership, unincorporated association or trust that carries on 'small businesses' only. A 'small business' is a business whose annual turnover for the previous financial year did not exceed AUS 3 million (approx. €1.9 million) (or none of its group/related companies' turnover). However, all processing of tax file numbers is covered by the Privacy Act (including processing completed by small businesses). In addition, otherwise exempt small businesses will be subject to the Privacy Act where they collect, use, or disclose health information as part of a health service, or 'deal in' personal information.

2. Key definitions

2.1. Personal data

The GDPR provides a definition of 'personal data' while the Privacy Act defines 'personal information' which, in practice, is a similar concept. In addition, both the laws define special categories of data/information and only apply to data that is used to identify the data subject or individual.

GDPR Articles 4(1), 9 Recitals 26-30	The Privacy Act Sections 6, 6FA, 6N, 7B

Similarities

The GDPR defines '**personal data**' as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person as one that can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'

The Privacy Act defines '**personal information**' as information or an opinion about an identified individual, or an individual who is reasonably identifiable, irrespective of whether the information or opinion is true or not, and regardless of whether it is recorded in a material form or not. While not specifically noted, as an 'individual' implies a living person, the Privacy Act does not (except as specifically noted) apply to the information of or about deceased persons.

The APP Guidelines clarify that the definition of 'personal information' refers to an opinion about 'a natural person.' The ordinary meaning of a 'natural person' does not include deceased persons. However, information about a deceased person may include information about a living individual and be 'personal information' for the purposes of the Privacy Act.

The concept of 'personal information' is broad and whether certain information is personal information or not will often depend on the specific circumstances.

The GDPR does not apply to **anonymised data**, where the data can no longer be used to identify the data subject.

While the Privacy Act does not explicitly exclude anonymous information from its application, the definition of '**personal information**' **does not include anonymous information** so is not subject to the Privacy Act.

GDPR	The Privacy Act

Similarities (cont'd)

The GDPR defines **special categories of personal data** as data revealing a data subject's 'racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.'

The Privacy Act defines **special categories of personal information** which includes 'sensitive information, health information, and genetic information.' The Privacy Act defines 'sensitive information' as information or an opinion about an individual's: racial or ethnic origin; political opinions; religious beliefs; philosophical beliefs; membership of a professional or trade association or trade union; sexual preferences; and criminal record. 'Sensitive information' also includes health information and certain genetic information.

Differences

The GDPR **does not** include credit information, tax file number information, and employee records within the definition of special categories of personal information.

The Privacy Act defines **special categories of personal information** which includes credit information, tax file number information, and employee records.

The GDPR specifies that **online identifiers** such as **IP addresses, cookie identifiers and radio frequency identification tags**.

The Privacy Act **does not** specifically address IP addresses, cookie identifiers and radio frequency identification tags. However, there is case law that explores the question of whether an IP address is considered personal information and, depending on the circumstances, these categories of data can be (and in practice often are) personal information. That is, where such identifies or can reasonably identify a natural person.

The Australian Government's Attorney-General's Department is currently conducting a review of the Privacy Act which may widen the definition of 'personal information' to definitively include IP addresses, device identifiers, location data and other online identifiers regulated (e.g. as personal information).

2.2. Pseudonymisation

Fairly inconsistent

The GDPR defines pseudonymised data, whereas the Privacy Act refers to the term in relation to the identity of individuals when dealing with an APP entity. The Privacy Act defines the term de-identified information as information which is no longer about a natural person.

GDPR	The Privacy Act
Articles 4(5), 11 Recitals 26, 28	Section 6 APP 2

Similarities

GDPR	The Privacy Act
Not applicable.	Not applicable.

Differences

GDPR	The Privacy Act
The GDPR defines **pseudonymised data** as 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.'	The Privacy Act **does not** define pseudonymisation. However, the Privacy Act defines 'de-identified' information as information which is no longer about an identifiable individual (i.e. natural person) or an individual who is reasonably identifiable. The APP Guidelines clarify that de-identification may not altogether remove the risk that an individual can be re-identified. There may, for example, be a possibility that another dataset or other information could be matched with the de-identified information.

2.3. Controllers and processors

Fairly inconsistent

Unlike the GDPR, the Privacy Act does not distinguish between 'data controllers' and 'data processors.' Instead, the Privacy Act provides the definition of an 'APP entity.' An 'APP entity' includes most private organisations, such as an individuals, body corporates, partnerships, unincorporated associations, trusts, and Commonwealth Government agencies.

Similarly, both the GDPR and the Privacy Act provide that data controllers and APP entities must ensure that personal information is accurate, up-to-date and complete.

GDPR	The Privacy Act
Articles 4, 5, 6, 24, 28, 30, 32, 45 Recitals 64, 90, 93	APPs 6, 8, 10, 11, 12

Similarities

The GDPR requires that personal data be '**accurate and, where necessary, kept up to date**' and that 'every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.'

The Privacy Act provides that an APP entity must take reasonable steps to ensure that personal information it collects is **accurate, up-to-date and complete**. An APP entity must also take reasonable steps to ensure that personal information it uses or discloses is accurate, up-to-date, complete and relevant, having regard to the purpose use or disclosure.

A data controller must collect personal data only for **specified, explicit and legitimate purposes** and not further process such in a manner that is incompatible with those purposes.

An APP entity may only use or disclose personal information for a notified **purpose for which it was collected** (known as the 'primary purpose') or for a secondary purpose if an exception applies.

Differences

A **data controller** is defined as a natural or legal person, public authority agency or other body that determines the **purposes** and **means** of the processing of personal data, alone or jointly with others.

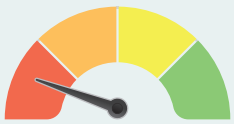
The Privacy Act **does not** provide a definition for data controller, nor does it distinguish between data controllers and data processors. Instead, the Privacy Act provides the concept of '**APP entities**,' which includes private organisations, such as an individual, body corporate, partnership, unincorporated association, trusts, and Commonwealth Government agencies, whether they are acting as a data controller or data processor.

A **data processor** is defined as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

The Privacy Act **does not** provide a definition for data processors. Instead, the concept of '**APP entities**' is provided, which encompasses both data controllers and data processors.

GDPR	The Privacy Act
Differences (cont'd)	
The GDPR provides that a data controller or data processor conduct **DPIAs** in certain circumstances.	The Privacy Act **does not** explicitly require that APP entities conduct PIAs in order to comply with the APPs. However, the APP Guidelines encourage them and note that it is good practice is to commit to conducting a PIA for new projects in which personal information will be handled, or when a change is proposed to information handling practices as a good way to ensure compliance.
The GDPR stipulates that data controllers and data processors keep **records of processing activities** and provides an exception from this obligation for small organisations. It also provides for the designation of a **DPO** by data controllers or data processors.	The Privacy Act **does not** explicitly provide that APP entities keep records of processing activities, nor does it provide the definition for DPO or the need to appoint one.
The GDPR requires processing by a processor to be governed by a **contract or another legal act**, 'that is binding on the processor with regard to the controller and that sets out the subject matter and the duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects and the obligations and rights of the controller.'	The Privacy Act **does not** explicitly provide that processing is bound by a contract or another legal act. Although, in practice, a binding contract is used as between an APP entity and an overseas recipient in a non-equivalent country to meet the requirements of APP 8. However, while such a contract is recommended, in practice, it is often not implemented as between two APP entities.
The GDPR states that the controller and processor shall **take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them** except on instructions from the controller, unless they are required to do so by EU or Member State law.	The Privacy Act **does not** contain an express requirement to take steps to ensure that an individual acting under the authority of the entity does not handle personal information, except on the instructions of the entity. However, in practice, all APP entities processing personal information are bound to comply with the APPs, in particular, APPs 1 and 11. APP 1 requires the entity to 'take such steps as are reasonable in the circumstances to implement practices, procedures and systems that ensure compliance with the APPs. APP 11 requires, among other things, that the entity take reasonable steps in the circumstances to protect personal information from misuse, unauthorised access and unauthorised disclosure. These requirements have the effect of subjecting the entity to a requirement to ensure that individuals acting under their authority (e.g. employees, contractors and the like) comply with the APPs and the APP entity's privacy policy.

2.4. Children



Inconsistent

The GDPR provides special provisions for protecting children's data, particularly with regard to obtaining consent. Whilst the GDPR provides protections in relation to the provision of information services, the Privacy Act seems to be wider in scope. According to the APP Guidelines, an individual under the age of 18 has capacity to consent, for privacy law purposes, when they have sufficient understanding and maturity to understand what is being proposed. In practice, the age of consent for children under the Privacy Act is similar to the age prescribed under the GDPR.

In addition, the GDPR provides detailed requirements when providing information addressed specifically to a child, whereas the Privacy Act does not.

GDPR Articles 6, 8, 12, 40, 57 Recitals 38, 58, 75	The Privacy Act Section 6AA(11), 12B(2) APP 1
Similarities	
Not applicable.	Not applicable.
Differences	
The GDPR **does not** define 'child' nor 'children.'	The Privacy Act **refers to the definition** of 'child' in the Family Law Act 1975 ('the Family Law Act'). According to the Family Law Act a 'child' is defined as a person who is under 18.
Where the processing is based on consent, the consent of a parent or guardian is required for providing information society services to a child below the **age of 16**. EU Member States can **lower this age limit to 13**.	The Privacy Act **does not** specify an age of consent. However, the APP Guidelines suggest that an APP entity must determine on a case-by-case basis whether a child has the capacity to consent. Where case-by-case assessment is not practicable, an individual aged under the age of 15 may be presumed not to have capacity to consent and n individual aged 15 and over may be presumed to have the capacity to consent (in the absence of anything that indicates otherwise). In some circumstances, 'it may be appropriate for a parent or guardian to consent on behalf of a young person, for example, if the child is young or lacks the maturity or understanding to do so themselves.
The GPDR provides that data controllers are required to make reasonable efforts to **verify** that **consent** is given or authorised by a parent or guardian of a child.	The Privacy Act **does not** expressly provide that an APP entity must verify that consent is given or authorised by a parent or guardian.

GDPR	The Privacy Act
Differences (cont'd)	
	In practice, however, where there is a failure to take reasonable steps to verify this the consequence is that the law may deem the 'consent' given or 'choice' made to provide their personal information by a child to be ineffectual and the APP entity will not be able to rely on that consent/choice.
When any information is addressed specifically to a child, controllers must take **appropriate measures** to provide **information** relating to processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language, that the child can easily understand.	The Privacy Act **does not** modify the general requirements for situations where information is addressed to children.
The GDPR applies to **information services**.	The Privacy Act appears to be **wider** in its scope.

2.5. Research

Fairly consistent

Under the GDPR, the processing of sensitive data is not prohibited when necessary for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes. The Privacy Act, similarly, makes exceptions for the collection, use and disclosure of health information where such is necessary for research and public health or safety purposes, where the use of de-identified information is not possible, subject to approved guidelines when research involves health information.

GDPR	The Privacy Act
Articles 5(1)(b), 9(2)(j), 14(5), 17(3), 21(6), 89 Recitals 33, 159-161	Sections 6, 16B, 95, 95A APP 3, 6

Similarities

Under the GDPR, the processing of personal data for **research purposes** is subject to **specific rules** (e.g. with regard to the purpose limitation principle, right to erasure, data minimisation and anonymisation etc.).

Under the Privacy Act, where **health information is processed for research** and related purposes and the 'permitted health situation' exception to consent is relied on, **specific rules** apply (e.g. the purpose for collection cannot be served by the collection of de-identified information, it is impracticable to obtain individuals' consent to the collection, use or disclosure).

Under the GDPR, where personal data is processed for research purposes, it is possible for Member States to **derogate from some data subjects' rights**, including the right to access, the right to rectification, the right to object and the right to restrict processing, insofar as such rights are likely to **render impossible or seriously impair the achievement of the specific purposes**, and such derogations are necessary for the fulfilment of those purposes.

The Privacy Act provides that the rights of an individual to access and correct personal information in APPs 12 and 13 are not specifically modified where such information is processed for research purposes. However, in practice, where personal information is being held for research purposes, it may be unreasonable to give the data subject the rights of access and correction. APP 12 provides that an APP **entity is not required to give the individual access** to their personal information 'to the extent that the entity reasonably believes that **giving access would pose a serious threat to the life, health or safety or any individual, or to public health or public safety**' and this will cover some research scenarios. Similarly, APP 13 only requires an APP entity to take 'reasonable' steps to correct personal information, having regard to the purpose for holding the information.

According to the GDPR, the processing of **sensitive data is not prohibited when 'necessary for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes**, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.'

The Privacy Act makes **special provisions for the collection, use and/or disclosure of health information or genetic information**, which are both a type of sensitive information, including where the collection of such is necessary for the **analysis of statistics relevant to public health or public safety**. However, this is only possible where the project has been approved by an ethics committee and the purpose cannot be served by the use of de-

GDPR	The Privacy Act

Similarities (cont'd)

	identified information and, in such a case, it is impracticable to obtain individuals' consent to the collection, use or disclosure.

Differences

The data subject has the **right to object** to the processing of personal data for research purposes unless such research purposes are for reasons of public interest.	The Privacy Act **does not** provide individuals with the right to object.

3. Legal basis

Unlike the GDPR, the Privacy Act does not provide a detailed list of legal bases for the processing of personal data. Instead, the Privacy Act provides that personal information may only be collected by fair and lawful means for purposes relating to the APP entity's 'functions and activities.'

Similarly to the GDPR, the Privacy Act provides a general prohibition on the collection, use or disclosure of sensitive personal information unless the individual has consented to such or an applicable exemption applies.

GDPR	The Privacy Act
Articles 5-10 Recitals 39-48	Sections 16A-16B, 80P APP 3

Similarities

Under the GDPR, data controllers can only process personal data when there is a legal ground for it. The legal bases include processing for the **legitimate interest** of the data controller when this does not override the fundamental rights of the data subject.

Under the GDPR, the **legal bases that a data controller must rely on to process** special categories of personal data are listed under **Article 9(2)** and include:

- when the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes;
- processing is necessary for the **establishment, exercise or defence of legal claims** or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of public interest in the area of **public health** or substantial **public interest**; or
- processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**.

The GDPR **recognises consent** as a legal basis to process personal information. However, consent under the GDPR cannot be implied.

Under the Privacy Act APP entities must not collect personal data unless the data is **reasonably necessary** for, or directly related to, one or more of the **entity's functions or activities**.

Under the Privacy Act, an APP entity **must not collect, use or disclose sensitive nformation without consent unless**:

- the individual **consents** and the information is **reasonably necessary** for one or more of the APP entity's functions or activities;
- a **permitted health situation exists**; or
- the collection of the information is required or authorised by or under an **Australian law or a court/tribunal order**.

Permitted health situations include:

- research relevant to **public health** or **public safety**; or
- the **compilation or analysis of statistics** relevant to public health or public safety.

The Privacy Act **recognises express and implied consent**.

GDPR	The Privacy Act

Differences

Under the GDPR, the **legal bases** that a data controller must rely on to process **personal data** are **listed under Article 6(1)** and include:

- processing that is **necessary for the performance of a contract** to which the data subject is a party;
- processing is **necessary for compliance with a legal obligation** to which the controller is subject;
- processing is necessary in order to protect the **vital interests** of the data subject or another natural person; or
- processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller.

The Privacy Act **does not** provide a list of legal bases that personal data can be processed under; rather it states that personal information may only be collected by fair and lawful means and must be reasonably necessary for the APP entity's 'functions and activities.'

Under the GDPR, the **legal bases that a data controller must rely on to process special categories of personal data** are listed under **Article 9(2)** and include:

- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of **employment and social security** and social protection law;
- processing is necessary to protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- processing is carried out in the course of its **legitimate activities with appropriate safeguards** by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim;
- processing relates to personal data which are manifestly **made public by the data subject**; or
- processing is necessary for the purposes of **preventive or occupational medicine**.

Under the Privacy Act, an APP entity **must not collect, use or disclose sensitive information without consent unless a permitted general situation exists** in relation to the collection of the information by the APP entity.

Permitted general situations include:

- when it is **unreasonable or impracticable to obtain the individual's consent** to the collection, use or disclosure;
- the entity has reason to suspect that **unlawful activity, or misconduct** of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;
- the entity reasonably believes that the collection, use or disclosure is reasonably necessary to assist any APP entity, body or person **to locate a person who has been reported as missing**; or
- the collection, use or disclosure is reasonably necessary for the purposes of a confidential alternative **dispute resolution process**.

4. Controller and processor obligations

4.1. Data transfers

Fairly inconsistent

Both the GDPR and Privacy Act regulate the international transfer of personal data to/access by overseas recipients. However, whereas the GDPR has a mechanism for recognising jurisdictions that are 'adequate,' the Privacy Act places the onus on the APP entity to come to a view as to whether the overseas recipient's jurisdiction has adequate protections.

GDPR	The Privacy Act
Articles 44-50 Recitals 101, 112	Section 16A APP 8

Similarities

The GDPR **permits the international transfer of personal data** to a third country, a territory or one or more specified sectors within that third country, or an international organisation which ensures an **adequate level of protection**, as assessed by the European Commission.

The Privacy Act **permits international transfers of personal information** without further requirements where the country of the recipient has a law or binding rules that has the effect of protecting the personal information in a way that, overall, **is at least substantially similar to the way in which the APPs protect the information**; and there are mechanisms under which the data subject can take action to enforce the protection of the law or binding rules.

Other legal grounds on the basis of which data transfers are allowed are:

- **judicial cooperation** by means of international agreements;
- when the data subject has **explicitly consented**;
- when the transfer is necessary for the **performance or conclusion of a contract**;
- when the transfer is necessary for important reasons of **public interest**;
- when the transfer is necessary for the **establishment, exercise or defence of legal claims**; and
- when the transfer is necessary in order to protect the **vital interests** of the data subject or of other persons.

Other legal grounds on the basis of which data transfers are allowed are:

- the transfer is **required or authorised by or under an Australian law** or a court/tribunal order;
- the data subject **consents** to the transfer after being **expressly informed** by the entity that the entity does not take steps to ensure that the overseas recipient does not breach the APPs;
- when the transfer is necessary to lessen or prevent a serious threat **public health or safety** as provided under 16A of the Privacy Act;
- the **entity is a Commonwealth Government agency** and the **transfer is required or authorised under an international agreement** on information sharing to which Australia is a signatory;
- the entity is a Commonwealth Government agency, the transfer is reasonably necessary for **enforcement related activities** and the overseas recipient performs similar functions to the entity; and
- the entity reasonably believes that the collection, use or disclosure is **necessary to lessen or prevent a serious threat**

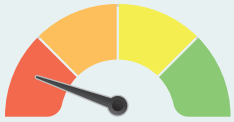
Similarities (cont'd)

	to the life health or safety of any individual, as provided under a '**permitted general situation**' defined in section 16A of the Privacy Act.
The GDPR permits the international transfer of personal data to a third country, a territory or one or more specified sectors within that third country, or an international organisation which ensures an **adequate level of protection**, as assessed by the European Commission.	The Privacy Act permits international transfers of personal information without further requirements where the country of the recipient has a law or binding rules that has the effect of protecting the personal information in a way that, overall, is at least substantially similar to the way in which the APPs protect the information; and there are mechanisms under which the data subject can take action to enforce the protection of the law or binding rules.

Differences

The GDPR also provides that data transfers can occur where: • the **transfer is made from a register** which according to the Union or Member States law is intended to provide information to the public and which is open to consultation; and • is based on the **legitimate interest of the controller if the transfer is not repetitive**, concerns only a limited number of data subjects and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.	The Privacy Act **does not** specifically provide for the international transfer of data on the basis of a register which is intended to provide information to the public, nor based on the legitimate interest of the controller. However, where consent is not provided and the transfer is not to an 'adequate' country, the Privacy Act requires similar safeguards for the transfer of personal information, which include taking such steps that are reasonable to ensure the overseas recipient does not breach the APPs (other than APP 1) and the disclosing APP entity remains liable for any such breaches as if they had occurred in Australia and were breaches of that APP entity.
In the absence of a decision on adequate level of protection, a transfer is permitted when **the data controller or data processor provides appropriate safeguards** with effective legal remedies that ensure the data subjects' rights as prescribed under the GDPR. Appropriate safeguards include: • binding corporate rules with specific requirements (e.g. a legal basis for processing, a retention period, complaint procedures, etc.); • standard data protection clauses adopted by the EU Commission or by a supervisory authority; • an approved code of conduct; or • an approved certification mechanism.	The Privacy Act **does not** provide similar appropriate safeguards to the transfer of personal data. However, the Privacy Act permits the international transfer of personal information to an overseas recipient outside Australia where: in the reasonable opinion of the entity, the overseas recipient is subject to a law or binding rules that has the effect of protecting the personal information in a way that, overall, is at least substantially similar to the way in which the APPs protect the information; and there are mechanisms under which the data subject can take action to enforce the protection of the law or binding rules.
The GDPR **does not** contain a similar provision.	Under the Privacy Act, an organisation may adopt, use or disclose a **government-related identifier** (e.g. Medicare numbers, Centrelink Reference numbers, driver licence numbers or passport numbers) except in a few specified circumstances.

4.2. Data processing records



Inconsistent

The GDPR requires controllers and processors to maintain a record of their processing activities. However, the Privacy Act does not contain a specific record-keeping requirement with respect to processing activities.

GDPR Articles 30 Recital 82	The Privacy Act APP 1
Similarities	
Not applicable.	Not applicable.
Differences	
Under the GDPR, controllers and processors must **maintain a record** of their processing activities.	The Privacy Act **does not** provide a specific requirement for entities to maintain a record of their processing activities. However, APP 1 requires that APP entities 'manage personal information in an open and transparent way' and 'take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities' that will ensure compliance with the APPs. In practice, in certain circumstances this may mean keeping records about collection, use and disclosure of personal information by the APP entity.
The GDPR **prescribes a list of information** that data processors must record.	The Privacy Act **does not** provide a list of information that should be recorded.

4.3. Data protection impact assessment

Under the GDPR a DPIA must be conducted in specified circumstances. Whilst the Privacy Act does not explicitly require APP entities to conduct a privacy impact assessment ('PIA'), the APP Guidelines state that APP entities should consider conducting a PIA to assist them with compliance.

GDPR Articles 35-36 Recitals 75, 84, 89-93	The Privacy Act APP 1

Similarities

Not applicable.	Not applicable.

Differences

Under the GDPR a **DPIA must be conducted** under specific circumstances.	The Privacy Act **does not** contain a specific requirement to conduct a PIA. However, there is a general requirement to take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs and enable them to deal with enquiries or complaints about privacy compliance. PIAs help an entity comply with this APP 1 requirement. The APP Guidelines provide that APP entities should implement a variety of practices, procedures and systems to ensure compliance, including considering conducting a PIA for new projects in which personal information will be handled, or when a change is proposed to information handling practices.

4.4. Data protection officer appointment

The GDPR requires the appointment of a data protection officer ('DPO') in specified cases, while the Privacy Act does not.

GDPR Articles 13-14, 37-39 Recital 97	The Privacy Act APP 1

Similarities

Not applicable.	Not applicable.

Differences

The GDPR requires data controllers and processors to **appoint a DPO** in specified circumstances.	The Privacy Act **does not** include a requirement to appoint a DPO. The APP Guidelines recommend appointing a privacy officer who can take on the role of implementing and reporting on practices, procedures and systems to ensure compliance with the APPs.

4.5. Data security and data breaches

Fairly consistent

Both the GDPR and the Privacy Act include data breach notification provisions. However, the GDPR is more prescriptive overall. Both laws, in relevant circumstances, require notification to the supervisory authority and affected individuals, and in practice are considered similar.

GDPR	The Privacy Act
Articles 5, 24, 32-34 Recitals 74-77, 83-88	Part IIIC APPs 1, 11

Similarities

The GDPR recognises **integrity and confidentiality as fundamental principles** of data protection by stating that personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Privacy Act recognises **security of personal information as a fundamental principle** of data protection by requiring that APP entities 'take such steps as are reasonable in the circumstances to protect the [personal] information' from: misuse, interference and loss; and unauthorised access, modification or disclosure. The more personal information an APP entity has and/or the more sensitive it is, the greater this security obligation is.

The GDPR states that data controllers and data processors must adopt **technical and organisational security measures** that ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

The Privacy Act states that entities must 'take such steps as are reasonable in the circumstances **to implement practices, procedures and systems relating to the entity's functions or activities'** to ensure compliance with the APPs including with respect to the security of personal information. The more personal information an APP entity has and/or the more sensitive it is, the greater this security obligation is.

Under the GDPR, in case of a data breach, the data controller must **notify the competent supervisory authority** unless the personal data breach is unlikely to result in a risk for the data subject. The data controller **must also notify the data subjects** involved, without undue delay, when the personal data breach is likely to result in a high risk.

An APP entity is required to notify **the OAIC and all affected individuals to whom the information relates** where: (i) the APP entity holds personal information; and (ii) there is unauthorised access, disclosure of loss of that information; and (iii) such is likely to result in 'serious harm' to an individual.

The GDPR provides a **list of information** that must be, at minimum, **included in the notification of a personal data breach**. For example, notification must include, among other things:

- **description of the nature of the breach**;
- where possible, the **categories** and the approximate number of the data subject concerned, and the categories and approximate number of personal data records concerned; and
- **contact details of the DPO** or other contact point.

The Privacy Act provides that **notification must include**, among other things:

- a description of the eligible data breach that the entity has reasonable grounds to believe has happened;
- the **kinds of information** concerned; and
- the **identity and contact details** of the entity.

GDPR	The Privacy Act
Similarities (cont'd)	
The GDPR provides an exception to data breach notification to the data subject when the data controller has **taken measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise**.	The Privacy Act provides an exception to mandatory breach notification to the individual when the **risk of any serious harm can be mitigated before any serious harm is suffered** by the individuals to whom the information relates.
The GDPR includes **specific provisions** with regard to the notification of a personal data breach to data subjects.	The Privacy Act includes **specific provisions** relating to the notification of an 'eligible data breach' to individuals. These relate to the way the notification is made. The required content of the notification is the same as that for the notification to the OAIC.
The GDPR sets a time frame to **notify the competent national authority** as 'without undue delay and, where feasible, not later than **72 hours** after having become aware of it.'	The Privacy Act requires that the entity **notify the data breach to the OAIC and all affected individuals as soon as practicable** after the entity becomes aware or reasonably believes that there may have been an eligible data breach.
The GDPR provides a **list of information** that must be, at minimum, **included in the notification of a personal data breach**. For example, notification must include: • the likely **consequences** of the breach; • **measures taken** or proposed to be taken to **mitigate** the possible adverse effects; and • the **reason of the delay**.	The Privacy Act provides the inclusion of **similar information in the notification**.
Differences	
The GDPR provides a **list of security measures** that the **controller and processor may implement**, which include: • the **pseudonymisation and encryption** of personal data; • measures that ensure the ongoing **confidentiality, integrity and availability** and resilience of processing systems and services; and • measures that **restore the availability and access to personal data** in a timely manner in the event of a physical or technical incident.	The Privacy Act **does not** detail specific security measures that must be in place and leaves this to the discretion to the entity insofar as the entity takes steps that are reasonable in the circumstances to protect the information. That is, the obligation changes depending on the circumstances. As the circumstances change (e.g. the entity holds more personal information or, even more so, more sensitive information), the steps considered reasonable will be more onerous. It is an expectation of the OAIC that organisations have a data breach response plan to meet their obligations to notify all 'eligible data breaches.'
The GDPR provides exceptions to data breach notification to the data subject when the data controller has **implemented appropriate technical and organisational** protection measures and where it would involve **disproportionate effort**.	The Privacy Act **does not** contain similar provisions. However, in the event of a security incident as long as reasonable security steps have been taken an entity will not be in breach of the Privacy Act.

4.6. Accountability

While the GDPR explicitly refers to the concept of accountability, the concept of accountability is built into the Privacy Act's legal framework through its general obligations. In addition, the APP Guidelines outline that accountability is an objective of APP 1.

GDPR	The Privacy Act
Articles 5, 24-25, 35, 37 Recital 39	Section 16C APP1

Similarities

The GDPR recognises **accountability** as a fundamental principle of data protection. Article 5 states that 'the controller shall be responsible and able to demonstrate compliance with data protection laws.' In addition, the principles can be taken to apply to several other principles as mentioned in other sections of this report, including the appointment of a DPO, and DPIAs.

The Privacy Act does not explicitly refer to accountability. However, APP 1 states that APP entities 'manage personal information in an **open** and **transparent** way,' and further, the APP Guidelines reinforce that accountability is an objective of APP 1. In addition, **the requirements of the Privacy Act reflect accountability**, such as Privacy by Default and Privacy by Design principles, as well as the requirement that APP entities should be accountable for the conduct of overseas recipients to which the Australian entity discloses personal information, making the Australian entity accountable for breaches of the APPs committed by the overseas recipient.

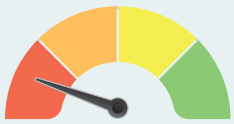
Differences

Not applicable.

Not applicable.

5. Individuals' Rights

5.1. Right to erasure



Inconsistent

The GDPR provides data subjects with the right to erasure and stipulates requirements relating to grounds for exercising the right, when fees are applicable and the information that must be provided to data subjects regarding the right, among other things. The Privacy Act does not contain an equivalent express right. However, APP 11.2 outlines obligations for deleting or de-identifying personal data irrespective of any request from an individual.

GDPR	The Privacy Act
Articles 12, 17 Recitals 59, 65-66	APP 11.2

Similarities

Not applicable.	Not applicable.

Differences

The GDPR provides data subjects with a right to erasure without undue delay where specific grounds apply, such as where **consent of the data subject is withdrawn** and there is with **no other legal ground** for processing, or the personal data **is no longer necessary** for the purpose of which it was collected. There are a number of exceptions to this right including compliance with a legal obligation and reasons of public interest.

The Privacy Act does not provide individuals with the right to erasure. However, APP 11.2, which addresses security of personal information, provides that **personal information must be destroyed or de-identified when:**

- **it is no longer needed** for the notified purposes for collection; and
- no other Australian law or court/tribunal requires the personal information to be retained.

The current review of the Privacy Act being conducted by the Australian Government's Attorney-General's Department may see a right to erasure introduced to the Privacy Act in some form.

5.2. Right to be informed

Both the GDPR and the Privacy Act recognise the right to be informed and impose an obligation to inform individuals of specific information relating to the 'processing' of personal data/information.

Unlike the GDPR, the Privacy Act does not address the right of data subjects to be informed regarding the existence of automated decision-making and profiling.

GDPR Articles 5-14, 47 Recitals 58-63	The Privacy Act APPs 1, 3, 5, 6, 11

Similarities

Data subjects must be provided with information relating to the processing of personal data, including:

- **purposes** of processing, including the legal basis for processing;
- **data subjects' rights** (e.g. the right to erasure, right to object, right of withdrawal, right to lodge a complaint to a relevant authority, etc.);
- **recipients or their categories** of personal data;
- any intention to **transfer** personal data to **third countries**;
- **contact details** of the data controller or its representative and the DPO;
- whether the provision of personal data is a **statutory** or contractual requirement; and
- the right to **lodge a complaint** with the authorities.

Individuals must be provided with information relating to the following at or prior to, or if not reasonably practicable, as soon as practicable after, collection:

- **purposes** for which the APP entity collects the personal information;
- **individual rights** (i.e. right to access and correction);
- **recipients or the categories of recipients** to which the APP entity usually discloses personal information;
- if the APP entity is **likely to disclose** the personal information to **overseas recipients**, and if so, the **countries** in which such recipients are likely to be located;
- **identity and contact details** of the APP entity;
- if the collection of the personal information is **required or authorised under an Australian law** or a court/tribunal order; and
- how the individual may **complain** about a breach of the APPs or a registered APP code, and how the entity will deal with such a complaint.

In addition, data subjects must be informed of the possible **consequences** of a failure to provide personal data whether in complying with statutory or contractual requirements, or a requirement necessary to enter into a contract.

In addition, individuals must be informed of the main **consequences** for them if their personal information is not provided to the APP entity.

Information can be provided to data subjects in an easily accessible form with clear and plain language, which can be in **writing and other means such as electronic format**.

Information must be provided to individuals in a clearly expressed and up-to-date policy or statement about the management of their personal information by the APP entity. An

GDPR	The Privacy Act
Similarities (cont'd)	
	APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available at or prior to collection or, if not reasonably practicable, as soon as practicable after, collection free of charge and **in such form as is appropriate**. If a person requests a **copy** of the privacy policy in a particular form, the entity must take such steps as are reasonable in the circumstances to give the person a copy in that form.
The GDPR provides that the **source** from which the personal data originated should be provided to data subjects when their personal data has been collected from a **third party**, which includes the sources from which the data was collected.	The Privacy Act also provides that, if the APP entity collects the personal information **indirectly** or the individual may not be aware of the collection of his/her data, the individual **must be notified** of the fact that the APP entity collects (or has collected) their information via a third party and the **circumstances** of that collection.
In the case of **indirect collection**, a data controller must provide information relating to such collection to data subjects within a reasonable period after obtaining the data, but at the latest within one month, or **at the time of the first communication with the data subject, or when personal data is first disclosed to the recipient**.	In the case **indirect collection** or where the individual may not be aware of the collection of his/her personal information, an APP entity must notify the individual of the collection of personal information via a third party, or otherwise ensure that the individual is aware of such information, **at or before the time or**, if that is not practicable, **as soon as practicable after, an APP entity collects the personal information** about an individual.
Information relating to personal data processing (e.g. the purpose of the processing, the rights of data subjects, etc.) must be provided to data subjects by the data controller **at the time when personal data is obtained**.	Notification of the collection of personal information, or otherwise ensuring that the individual is aware of such collection (e.g. notifying the purpose of the processing, the rights of data subjects, etc.) must take place **at or before the time or**, if that is not practicable, **as soon as practicable after, an APP entity collects the personal information** about an individual.
A data controller cannot collect and process personal data for purposes other than the ones about which the data subjects were informed, **unless the data controller provides them with further information**.	An APP entity cannot collect, use or disclose personal information other than for the notified purposes for collection. If an APP entity holds personal information about an individual that was collected for a particular notified purpose (i.e. the primary purpose), the entity generally must not use or disclose the information for another purpose (i.e. the secondary purpose) **unless the individual has consented to that use or the disclosure of the information**.

GDPR	The Privacy Act
Similarities (cont'd)	
Information can be provided to data subjects in **writing form, through electronic means, or orally**.	The Privacy Act requires a privacy policy or statement containing the mandatory information but is **does not prescribe the form of such (although in practice it is usually in writing)**.
Differences	
A data controller must inform data subjects of the existence or absence of an **adequacy decision**, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference the **appropriate or suitable safeguards** and the means by which to obtain a copy of them or where they have been made available.	The Privacy Act **does not** contain a direct equivalent to this requirement but, to avoid liability for disclosure of personal information outside of Australia, an APP entity has to obtain the informed consent of the individual to send their personal information to a recipient in a 'non-adequate' country.
Data subjects must be informed of the existence of **automated decision-making, including profiling**, at the time when personal data is obtained.	The Privacy Act **does not** address the right of data subjects to be informed regarding the existence of automated decision-making and profiling.
Data subjects must be provided with information relating to **data retention periods**.	The Privacy Act **does not** explicitly require APP entities to provide information relating to data retention periods to individuals but does require that personal information is deleted or de-identified when: • it has been used for the notified purposes for which it was collected; and • the legal retention period has expired.

5.3. Right to object

The GDPR provides data subjects with the right to object to the processing of personal data, as well as the right to withdraw consent to the processing of personal data. The Privacy Act does not explicitly provide individuals with the right to object to the processing of personal data/information or the right to withdraw consent.

Similarly to the GDPR, the Privacy Act provides that an individual may request not to receive direct marketing communications from organisations or not to have their information disclosed to third parties for such purposes.

GDPR Articles 7, 12, 18, 21	The Privacy Act Section 6

Similarities

Data subjects have the right to withdraw consent to the processing of their personal data where the purpose of such processing is for **direct marketing purposes**.

Under the Privacy Act APP 7.6, an individual may request not to receive **direct marketing communications** from an organisation and for that organisation not to disclose their personal information to others for direct marketing purposes.

Differences

Data subjects shall have the right to **withdraw** their consent to the processing of their personal data **at any time**.

The Privacy Act **does not** explicitly provide individuals with a right to withdraw their consent to the processing of their personal information at any time. However, in practice, if consent to processing is required (e.g. for sensitive information) it can be withdrawn for any future collection, use, or disclosure of sensitive information.

Under the GDPR, data subjects are provided with the **right to object** to the processing of their personal data in specific circumstances including where:

- the processing of personal data is due to **tasks carried out in the public interest** or **based on a legitimate interest pursued by the data controller** or **third party**; or
- the processing of personal data is for **scientific, historical research or statistical purposes**.

The Privacy Act **does not** provide the right to object to the processing of personal information for circumstances similar to those in the GDPR.

The GDPR provides data subjects with a right to the **restriction of processing** of personal data which must be responded to without undue delay and in any event within **one month** from the receipt of request. The deadline can be extended by **two additional months** taking into account the complexity and number of requests.

The Privacy Act **does not** provide the individual with a right to restrict the processing of personal information.

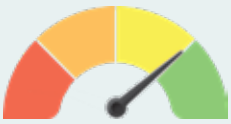
GDPR	The Privacy Act

Differences ('cont'd)

The GDPR provides data subjects with the **right not to be subject to decisions based solely on automated processing**, including profiling.

The Privacy Act **does not** contain a similar provision. Where the individual has provided their personal information for notified purposes they do not have a right to object. However, where sensitive information is involved (or otherwise personal information is collected with 'consent') an individual could withdraw their consent to the processing of such information or opt to limit their consent to non-automated decision making.

5.4. Right to access



Fairly consistent

Both the GDPR and the Privacy Act provide individuals with the right to access their personal data when it is held or processed by a data controller or APP entity. However, the laws have several differences with regard to the timeline for responses, the ability to charge a fee, the identification of individuals and exceptions.

GDPR Article 15 Recitals 59-64	The Privacy Act APP 12

Similarities

The GDPR recognises that data subjects have the **right to access** their personal data that is processed by a data controller.

The Privacy Act recognises individuals have the **right to access** personal information held about them by an APP entity.

The GDPR provides that the right of access **must not adversely affect the rights or freedoms of others**. Restrictions to the right of access, may be also imposed by **EU or Member State law**. In particular, these may be provided in relation to personal data processed for scientific or historical research purposes or statistical purposes, or for archiving purposes in the public interest.

The Privacy Act provides that an APP entity is not required to provide an individual with access to personal information if the access would **pose a serious threat to the life, health or safety of any individual** or have **an unreasonable impact on the privacy of other individuals**. Relevant scenarios include where:

- the information relates to existing or anticipated **legal proceedings** between the entity and the individual, and would not be accessible by the process of discovery in those proceedings;
- giving access would reveal the intentions of the entity in relation to **negotiations** with the individual in such a way as to prejudice those negotiations;
- giving access would be **unlawful**;
- denying access is required or authorised by or under an **Australian law or a court/tribunal order**;
- both of the following apply:
  - the entity has reason to suspect that **unlawful activity**, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;
  - giving access would be likely to **prejudice the taking of appropriate action** in relation to the matter;
- giving access would be likely to prejudice one or more **enforcement related activities** conducted by, or on behalf of, an enforcement body; or
- giving access would **reveal evaluative information** generated within the entity in connection with a commercially sensitive decision-making process.

GDPR	The Privacy Act
Similarities (cont'd)	
Data subjects must have a variety of means through which they can make their request, including orally and through electronic means. In addition, when a request is made through electronic means, a **data controller should submit a response through the same means**.	APP entities must give access to the information in the **manner requested by the individual** if it is reasonably practicable to do so.
A data controller can refuse to act on a request when it is **manifestly unfounded, excessive, or has a repetitive character**.	An APP entity may refuse an access request if the request is **frivolous or vexatious**.
Data subjects' requests under this right must be replied to **without 'undue delay and in any event within one month from the receipt of a request.'** The deadline can be extended by **two additional months** taking into account the complexity and number of requests. In any case, the data subject must be informed of such an extension within one month from the receipt of a request.	The Privacy Act provides that if the APP entity is an organisation it must respond to a subject access request **within a reasonable period** of time after the request is made. The APP Guidelines suggest that, as a general guide, a reasonable period **should not exceed 30 calendar days**.
The GDPR specifies that a data controller **must have in place mechanisms** to identify that a request is made by a data subject whose personal data is to be deleted.	The Privacy Act does not explicitly address mechanisms to identify that a request is made by the individual to whom the personal information relates. **Failure to have such mechanisms would breach APP 1** and wrongful disclosure (i.e. to the wrong person) could be a notifiable data breach. Thus, in practice, reasonable steps to verify identity are required.

GDPR	The Privacy Act
Differences	
The GDPR specifies that, **when responding to an access request**, the data controller must indicate the following information: • the **purposes** of the processing; • the **categories** of personal data concerned; • the recipients or categories of recipients to whom the personal data has been or will be **disclosed**, in particular recipients in third countries or international organisations; • where possible, the envisaged **period** for which the personal data will be **stored**, or, if not possible, the criteria used to determine that period; • the existence of the right to request from the controller **rectification or erasure** of personal data or restriction of processing of personal data concerning the • data subject or to object to such processing; • the right to lodge a **complaint** with a supervisory authority; • where the personal data are not collected from the data subject, any available information as to their **source**; and • the existence of **automated decision-making**, including profiling.	The Privacy Act **does not** prescribe what needs to be included in responding to an access request.
The right to access can be exercised **free of charge**. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive, or have a repetitive character.	If the APP entity is an organisation it **may decide to charge** the individual for access to the personal information, the charge must not be excessive and must not apply to the making of the request.
The GDPR provides that the right of access must not adversely affect the rights or freedoms of others, **including those related to trade secrets**.	The Privacy Act **does not** explicitly address trade secrets in relation to the right of access.
The GDPR provides that a data controller can **refuse** to act on an access request where: • it is able to demonstrate that it is not in a position to **identify the data subject**; and • the request is **manifestly unfounded or excessive**, in particular because of its repetitive character.	The Privacy Act **does not** contain similar exceptions. However, in practice the list of exemptions to providing access deliver a similar result.

5.5. Right not to be subject to discrimination in the exercise of rights

Consistent

The right not to be subject to discrimination in exercising rights is not explicitly mentioned in the GDPR or the Privacy Act. However, under the GDPR and the Privacy Act the right not to be subject to discrimination can be implied from the fundamental rights of the data subject and, in Australia, under anti-discrimination legislation.

GDPR	The Privacy Act
Similarities	
The GDPR **does not** explicitly address the right not to be subject to discrimination; therefore, no scope of implementation is defined.	The Privacy Act **does not** explicitly address the right not to be subject to discrimination; therefore, no scope of implementation is defined. However, other Australian laws (e.g. Commonwealth, State and Territory equal opportunity and anti-discrimination legislation) do address and prohibit discrimination.
Differences	
Not applicable.	Not applicable.

5.6. Right to data portability

The GDPR provides data subjects with the right to data portability, whereas the Privacy Act does not contain an equivalent right. However, in certain sectors in Australia the consumer data right ('CDR') has been introduced (starting with the banking, then it will move to the retail electricity and telecommunications sectors) and this does provide, for those sectors, data access/portability under a parallel regime to the Privacy Act.

GDPR Articles 12, 20, 28 Recitals 68, 73	The Privacy Act
Similarities	
Not applicable.	Not applicable.
Differences	
The GDPR **provides** individuals with the right to data portability. The GDPR defines the right to data portability as the r**ight to receive data processed on the basis of contract or consent and processed by automated means, in a 'structured, commonly used, and machine-readable format'** and to transmit that data to another controller without hindrance.	The Privacy Act **does not** include a direct equivalent to the right to data portability.

6. Enforcement

6.1. Monetary penalties

Fairly consistent

Both the GDPR and the Privacy Act provide for monetary penalties to be issued for non-compliance, however the amounts differ significantly.

GDPR Articles 83, 84 Recitals 148-152	The Privacy Act Section 13G

Similarities

The GDPR provides for **monetary penalties** in the case of non-compliance.

The Privacy Act provides for **monetary penalties** in the case of non-compliance.

Differences

Depending on the violation the penalty may be up to either: **2% of global annual turnover or €10 million**, whichever is higher; or **4% of global annual turnover or €20 million**, whichever is higher. The amount of the penalty may also vary depending on 'the nature, gravity and duration of the infringement,' the nature of the processing, the number of data subjects affected and the damages suffered, the negligent or intentional character of the infringement, etc. A complete list can be found in Article 83(2) of the GDPR.

Under the Privacy Act, the maximum penalty for non-compliance is currently a fine of **AUD 2.22 million** (approx. €1.4 million). At the time of publication, this is being revised upward in the near future to be the greater of AUD 10 million (approx. €6.4 million) and 4% of annual domestic revenue.

6.2. Supervisory Authority

Fairly consistent

Both the GDPR and the Privacy Act provide supervisory authorities with investigatory and corrective powers including the power to obtain information, access premises and order individuals to take steps towards compliance, and in practice are considered to be similar. In addition, both laws require supervisory authorities to promote awareness of data protection.

The Australian competition regulator (i.e. the Australian Competition and Consumer Commission) is becoming increasingly involved in the regulation of consumer personal information and has powers similar to those of a supervisory authority.

GDPR Articles 51-59	The Privacy Act Part V, VII

Similarities

Under the GDPR, supervisory authorities have **investigatory powers** which include:

- ordering a controller and processor to **provide information** or access to all personal data and information necessary for the performance of tasks;
- **notifying** the controller or the processor of an alleged infringement; and
- obtaining access to all personal data and to any **premises**.

The OAIC's **investigatory powers** include:

- the power to **obtain information and documents** which are relevant to the investigation;
- **informing** the respondent that the matter is to be investigated; and
- the power to authorise a person to enter the **premises** occupied by an agency or organisation to inspect any documentation kept at the premises.

Under the GDPR, supervisory authorities have **corrective powers** which include:

- issuing **warnings** and **reprimands**; and
- to order the controller or the processor to **comply** with the data subject's requests.

The OAIC's **corrective powers** include:

- making a **determination** stating that the act is an interference with privacy and the person or entity must not repeat or continue the act and seek **injunctions**; and
- making a declaration within the determination ordering the **respondent to take specified steps** within a specified period to ensure that such conduct is not repeated or continued.

Under the GDPR, supervisory authorities can **cooperate** with data protection authorities from other countries.

Under the Privacy Act, the OAIC may also seek to **work in partnership** with privacy regulators in foreign jurisdictions.

Under the GDPR, supervisory authorities are tasked with **promoting public awareness** and understanding of the risks, rules, safeguards and rights in relation to processing as well as promoting the awareness of controllers and processors of their obligations, amongst other tasks.

Under the Privacy Act, the Privacy Commissioner (and therefore the OAIC) is tasked with **promoting an understanding** and acceptance of the APPs and undertaking educational programs for the purposes of promoting the protection of individual privacy.

GDPR	The Privacy Act

Differences

Under the GDPR, supervisory authorities have **investigatory powers** which include:

- conducting data protection **audits**; and
- carrying out a review of **certifications** issued.

The Privacy Commissioner's **investigatory powers** include:

- attempting to **conciliate** a complaint;
- conducting **preliminary inquiries** to determine whether or not to open an investigation;
- deciding whether or not to **hold a hearing**;
- administering an **oath or affirmation**;
- directing a complainant, respondent or other relevant person to **attend a conference** related to a complaint; and
- **referring a complaint** to an alternative complaint body.

Under the GDPR, supervisory authorities have **corrective powers** which include:

- to order the controller to **communicate a personal data breach** to the data subject;
- **withdraw a certification**;
- to order the **suspension of data flows** to a recipient in a third country or to an international organisation; and
- imposing **administrative fines**.

The Privacy Commissioner's **corrective powers** include:

- accepting an '**enforceable undertaking**' made by an entity;
- **bringing proceedings** to enforce an enforceable undertaking or determination; and
- **applying to the court for a civil penalty** order for a breach of a civil penalty provision.

6.3. Civil remedies for individuals

Fairly inconsistent

Both the GDPR and the Privacy Act include the right to lodge a complaint with the supervisory authority. However, the GDPR provides a direct cause of action for a breach of privacy, whereas under the Privacy Act an individual lodges a complaint, which is subject to the review and assessment of the OAIC/the Privacy Commissioner.

GDPR	The Privacy Act
Articles 79, 80, 82 Recitals 131, 146, 147, 149	Sections 25, 52

Similarities

The GDPR provides data subjects with the **right to lodge a complaint** with a supervisory authority.

Under the Privacy Act **individuals may submit a complaint** about a breach of privacy to the Privacy Commissioner via the OAIC.

Differences

The GDPR provides data subjects who have suffered material or non-material damages as a result of an infringement shall have the right to receive **compensation** from the controller or processor **before the competent court**.

The Privacy Act **does not** provide individuals with a direct cause of action to seek redress for a violation of privacy laws before the courts. However, the Privacy Commissioner investigates complaints which could lead to a determination by the Privacy Commissioner that the APP entity pay damages to the individual concerned.

The GDPR allows Member States to provide for the possibility for data subjects to give a mandate for **representation** to a **not-for-profit** association, **association or organisation** that has as its statutory objective the protection of data subject rights.

The Privacy Act **does not** expressly provide for representation by a not-for-profit association in relation to privacy complaints. However, a class complaint to the Privacy Commissioner may be led by a representative body.