The GDPR – EU General Data Protection Regulation

Considerations for the Victorian public sector

The EU General Data Protection Regulation (**GDPR**) is designed to harmonise data privacy laws across the European Union **(EU)** and offer enhanced privacy protections for individuals in the EU. The GDPR came into effect on **25 May 2018**.

Entities that fall within the scope of Article 3 of the GDPR will attract obligations to protect the personal data of individuals in the EU, in accordance with the GDPR.

The extra-territorial reach of the GDPR is arguably the biggest regulatory change for data privacy laws internationally. The extra-territorial scope of the GDPR is designed to make entities accountable for their data processing activities, regardless of their location, when processing the personal data of individuals in the EU.

The purpose of this document is to provide a comparison between the Information Privacy Principles (IPPs) under the *Privacy and Data Protection Act 2014* (PDP Act) and the incoming GDPR.

Extra-territorial scope: Key considerations for Victoria

Victorian Public Sector **(VPS)** organisations may have obligations under the GDPR, to the extent that they:

- offer goods or services to data subjects in the EU (regardless of whether payment is required);[1] or
- monitor the behaviour of data subjects in the EU, in so far as the behaviour takes place within the EU.[2]

Examples of where a VPS organisation may be considered to be monitoring persons in the EU include activities that track online behaviour or profile individuals.

The GDPR may also apply to VPS organisations that have a physical or legal establishment in the EU, regardless of whether the processing takes place in the EU, in accordance with Article 3(1).

VPS organisations already have obligations under the PDP Act to protect personal information they hold. VPS organisations may also have obligations under the GDPR in certain instances, for example, where a Victorian university is offering exchange programs to students in the EU. Any contracted service providers engaged by the VPS may also have obligations under the GDPR.

In general, VPS organisations should consider the geographical reach of their activities and seek independent legal advice regarding their data processing activities, as the extent to which the GDPR may apply to them will depend on the particular circumstances of each organisation.

Key terminology in the GDPR

There are a number of key terms under the GDPR that define the types of entities and activities captured by the new Regulation, as well as the individuals afforded protection under the GDPR.

Data controller: means a natural or 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.

Data processor: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of a data controller.

[1] Article 3(2)(a).
[2] Article 3(2)(b). For example, by tracking individuals on the internet or for predicting the personal preferences, behaviours and attitudes of individuals (Recital 24).

Data subject: means an identified or identifiable natural person.[3]

Data processing: refers to any operation, or set of operations, which are performed on personal data, or sets of personal data, whether or not by automated means.[4]

Key themes in the GDPR

Emphasis on clear, plain language drafting

The GDPR places obligations on data controllers and processors to ensure any information or communications relating to the processing of personal data be easily accessible and drafted in clear, plain language.[5]

Demonstrated compliance

Data controllers are expressly required to demonstrate compliance with the principles relating to the processing of personal data, outlined in Article 5.[6]

Article 24 stipulates that data controllers are to implement appropriate measures in compliance with the GDPR.[7] This includes integrating a 'data protection by design' approach and ensuring that, by default, only personal data which is necessary for a specific purpose is processed.[8] Should a controller wish to appoint a processor, Article 28 requires controllers to only engage processors that guarantee compliance with the GDPR.[9]

Under Article 35, controllers are required to undertake a data protection impact assessment for any processing activities likely to result in high risks to the rights and freedoms of individuals. Controllers are required to seek the advice of their Data Protection Officer (**DPO**), where designated, when carrying out the assessment.

Mandatory appointment of a data protection officer

Article 37 requires that controllers and processors appoint a DPO, where:

- the processing is carried out by a public authority[10]
- an activity may require the monitoring of data subjects on a large scale[11], or
- the core activities of the controller or the processor consist of processing special categories of personal data (sensitive data) on a large scale, under Articles 9 and 10.[12]

Like a Privacy Officer, the DPO is the main point of contact for individuals for privacy enquiries[13] and is responsible for conducting staff privacy awareness training activities. The DPO is to report to the highest level of management within the entity.

Enhanced individual rights

Data subjects are granted enhanced, actionable individual rights under Chapter 3 of the GDPR, including:

- the right to be forgotten
- the right to restrict processing
- the right to data portability
- the right to object to processing in limited circumstances, including where personal data is processed for direct marketing purposes, and
- the right not to be subject to automated decision making and profiling.

[3] Article 4(1). Note that this may include data subjects who are EU residents or citizens, who are, or will be, in the EU. See the European Commission's guidance page, Reform of EU data protection rules for more information.
[4] Includes the collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (see, Article 4(2)).
[5] Recital 39.
[6] Article 5(2).
[7] These measures are subject to review and updating where necessary (see Article 24(1)).
[8] Article 25(2).
[9] In the form of a binding written agreement or other legal act of Union or Member State law which must include conditions as outlined in Article 28(3). Further detail about the contents of such agreements or legal acts is provided under Recital 81.

[10] Except for courts acting in their judicial capacity, Article 37(1)(a).
[11] Article 37(1)(b).
[12] Article 37(1)(c).
[13] As well as the supervisory authority in relevant Member States of the EU. Chapter 6 of the GDPR sets out the procedure for the establishment, role and parliamentary oversight requirements of independent supervisory authorities, in each Member State of the EU.

However, the rights provided for under Articles 12 – 22 may be restricted in limited circumstances under Union or Member State law.[14]

Cross-border transfers of data

Under Article 45, a transfer of personal data to a third country or international organisation can only take place where the Commission[15] has decided that the receiving country or organisation has an adequate level of protection.[16] If the protection level is inadequate upon review,[17] the Commission may repeal the country's status without retroactive effect.[18] Currently, Australia is not considered an 'adequate' jurisdiction for the purposes of Article 45.[19]

In the absence of the Commission granting 'adequacy' status to a country under Article 45, cross-border transfers may take place with public authorities on the basis of a legally binding and enforceable instrument, that provides for appropriate safeguards.[20] Transfers made between organisations within a corporate group are governed by binding corporate rules under Article 47.

Joint responsibility for compliance

Where two or more controllers are acting together (as joint controllers),[21] they must form an 'arrangement' between them to clearly assign compliance responsibilities in a transparent manner.[22] A summary of this arrangement must be made available to the data subject.[23]

Mandatory data breach notification requirements

Under Article 33, data controllers are obligated to report data breaches to the supervisory authority[24] within 72 hours of the breach occurring. Data controllers must also communicate to data subjects personal data breaches that pose a high risk to their rights and freedoms, under Article 34.

Consent

Entities captured by the GDPR are now expressly required to draft terms of use in clear and plain language. Provisions seeking consent must be clearly distinguished from other provisions, under Article 7. This means that entities cannot bundle provisions seeking consent amongst other terms and conditions. For consent to be informed and meaningful it must be specific, freely given, and the data subject's agreement must be clear and unambiguous. Consent should cover all processing activities carried out for the same purpose or purposes.[25]

The controller should be able to demonstrate that the data subject has given informed consent to the processing operation. Where the consent declaration is pre-drafted for the individual, this document should be intelligible and easily accessible with clear, plain language.[26]

---

[14] Article 23.
[15] The European Commission.
[16] Under Article 45(1). Adequate protection takes into account the legislative framework and respect for fundamental rights, effective oversight and safeguarding mechanisms and international commitments that the receiving country is party to (see Article 45(2)).
[17] A mechanism for periodic review may be implemented by the Commission (by way of an implementing act) to take place at least every four years (see Article 45(3)).
[18] Article 45(5).
[19] See the factsheet Adequacy of the protection of personal data in non-EU countries for a list of current adequacy decisions.
[20] Article 46(2)(a), and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available (Article 46(1)). Article 46(2) lists appropriate safeguards that may be implemented to allow for cross-border transfers in compliance with the GDPR.
[21] Where two or more controllers jointly determine the purposes and means of processing, they will be considered joint controllers, Article 26
[22] Article 26(1) and Recital 79.
[23] Article 26(2).
[24] Each Member State of the EU is required to appoint a supervisory authority. A supervisory authority is one or more independent public authorities, responsible for monitoring compliance with the GDPR. More information on supervisory authorities can be found here: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en.
[25] Recital 32. Consent is an active action to enter into an agreement; inactivity (such as pre-ticked boxes) does not constitute consent.
[26] Recital 42.

Case Study: a Victorian university offering goods and services to students in the EU

A Victorian university may demonstrate an intention[27] to offer goods and services to students in the EU, by:

- allowing payment for services in Euros
- targeting EU students via a website drafted in a European language, and
- mentioning students or users in the EU, for example.

If these processing activities do fall within the scope of the GDPR,[28] some steps the Victorian university may take to ensure compliance with the GDPR could include:

- Reviewing any privacy communications, including Privacy Policies and Collection Notices to ensure they are drafted in plain, accessible language.
- Where the processing of personal information will be based on consent, ensuring that all Collection Notices seeking individuals' consent are drafted in a way that allows consent to be freely given (for example, on a positive opt-in basis), specific to an identified purpose, clearly distinct from other matters and in clear, accessible language.
- Ensuring the university has appointed a Privacy Officer, who is responsible for the university's privacy compliance activities. The university shall also appoint a DPO, for the purposes of the GDPR (this may also be the university's Privacy Officer).
- The university needs to ensure that the DPO is supported, well-resourced and independent enough to carry out the tasks of the DPO, including the delivery of advice on, and monitoring of, GDPR compliance. Like a Privacy Officer, the DPO is the main point of contact for individuals for privacy enquiries[29] and responsible for conducting all staff privacy awareness training activities. The DPO shall report to the highest level of management of the university.
- Adopting a Privacy by Design approach to any new program or initiative, through undertaking regular Privacy Impact Assessments, under the guidance of the DPO.
- Ensuring that all procedures in place to allow individuals access and correction of their personal information account for the enhanced rights for individuals under the GDPR, including the right to data portability (to receive a copy of their data in a machine-readable format) and the right to be forgotten (amongst others).
- Implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risk to the personal information.
- Ensuring that any data breach response plans account for the mandatory breach notification requirements under the GDPR.

Please note, these are an example of general steps a VPS organisation may take to ensure compliance, having regard to their existing obligations under the PDP Act. These steps are not a checklist and VPS organisations should carefully assess whether their data processing activities would fall within the scope of the GDPR.

[27] Recital 23 contains more information relevant to ascertaining whether a controller envisages offering services to data subjects in one or more Member States in the EU.
[28] Under Article 3(2).

[29] As well as the supervisory authority in relevant Member States of the EU.

The GDPR and the IPPs under the PDP Act: Comparison table

This table is designed to help VPS organisations understand where the protections under the PDP Act may be equivalent or different to those under the GDPR. Please note that this table does **not** outline all of the requirements under the GDPR.

It is important to note that the privacy protections under the PDP Act are principle-based, allowing a degree of flexibility for VPS organisations to comply with their obligations in a way that suits their needs or resources. In contrast, the GDPR combines a principle-based *and* prescriptive approach to the protections afforded for data subjects, introducing strict, mandatory obligations for data controllers and processors.

VPS organisations should continue to comply with their obligations under the PDP Act and make a judgement as to whether any data processing activities meet certain threshold requirements under the GDPR.

IPPs	Relevant GDPR Provisions	Comparison notes
IPP 1 – Collection **An organisation may only collect personal information if it is necessary to fulfil its functions. It must collect personal information only by a lawful and fair means and provide notice of collection, for both direct and indirect collection activities.**	**Article 5** contains a number of principles for processing personal data under the GDPR, including a requirement that data is collected for a **specified, explicit and legitimate purpose** and **limited to what is necessary** for the identified purpose**.** **Articles 12, 13 and 14** outline the rights of data subjects to be notified where their personal data is collected, directly or indirectly. **Article 21** provides data subjects the right to object to the processing of personal data in limited circumstances, including where personal data is processed for **direct marketing purposes**. Data subjects need to be made aware of these rights **at the time of the first communication with the data subject.**	**IPP 1.1** contains a similar requirement to **Article 5**, providing that organisations must only collect personal information that is necessary for one or more of its functions. The notice requirements under **Articles 12, 13 and 14** are generally more prescriptive than **IPPs 1.3 to 1.5**. In particular, **Article 12** requires that any information notifying data subjects of the collection of their personal data be drafted in a **concise, transparent, intelligible and easily accessible form** (especially if the information is addressed to a child). **Article 12** also provides for the use of visual aids, to assist data subjects understand any information provided in a notice of collection.[30]
IPP 2 – Use and Disclosure **Personal information may only be used and disclosed for the primary purpose for which it was collected, or for a reasonably expected secondary purpose (amongst**	**Article 5** restricts the processing of personal data beyond the specified purpose for collection, however **Article 6** outlines a number of lawful bases for the processing of personal data, including where the data subject has provided informed **consent** or where processing is deemed **necessary for compliance with legal obligations to which the controller is subject.**	The conditions for reliance on consent as a lawful basis for processing are stricter under the GDPR (under **Articles 7 and 8**).[31] **Article 7** requires controllers to demonstrate the data subject's consent to processing and that any requests for consent are **clearly distinguishable from other matters**, using **clear and plain language**. **Article 8** outlines the procedures for gaining

[30] See Recital 58 for more information on the requirements for information addressed to the public or data subjects. Of interest, Recital 58 specifically notes the need for clear communications where the "technological complexity of the practice make it difficult for the data subject to…understand" the purpose of collection.

[31] Additionally, Recital 43 notes that consent should not form the legal basis for processing where there is a clear imbalance between the data subject and controller, for example, where the controller is a public authority.

IPPs	Relevant GDPR Provisions	Comparison notes
other limited circumstances).		consent (in relation to information society services)[32] where the data subject is a child, stipulating that consent may form the lawful basis of processing where the child is **at least 16 years old.** Processing on the basis of consent is only permitted for a child under 16 years upon parental consent. In comparison, the PDP Act does not set clear age brackets for the consent requirements of children, under **s 28**. Instead, the consent of minors is primarily addressed as a matter of policy, supported by relevant case law, in Victoria.[33]
IPP 3 – Data Quality **Organisations must take reasonable steps to ensure that personal information collected, used or disclosed is accurate, complete and up to date.**	**Article 5** stipulates that personal data shall be **accurate** and **kept up to date**, and where personal data is shown to be inaccurate, organisations must take **every reasonable step** to ensure the data is **erased or rectified without delay.** **Article 18** also provides a right to the restriction of processing of personal data, where the data subject has contested the accuracy of the personal data (amongst other grounds).	In addition to data quality requirements at the time information is collected, organisations bound by the IPPs have ongoing obligations to ensure personal information used and disclosed is accurate, complete and up to date, **but no positive obligation to proactively take every reasonable step to erase personal information that may be inaccurate, under IPP 3.** **Article 18** provides a much more prescriptive avenue for redress than **IPP 6**. While organisations are required to take reasonable steps to correct personal information about an individual upon their request under IPP 6, Article 18 provides that following action to contest the accuracy of the personal data, processing may only occur upon gaining the data subject's consent (amongst other limited circumstances) and that the data subject will be informed by the controller before processing resumes.
IPP 4 – Data Security **Organisations must take reasonable steps to protect personal information it holds from misuse, loss, unauthorised access, modification or disclosure. An organisation must take reasonable steps to destroy or permanently de-identify personal information when it is no longer needed.**	**Article 5** stipulates that personal data shall be processed **in a manner that ensures appropriate security, protection against unauthorised or unlawful processing, accidental loss, destruction or damage, using inappropriate technical or organisational measures.** **Article 32** requires data controllers and processors **to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk** (to the personal data). **Articles 33 and 34** introduce mandatory data breach notification	Obligations for organisations to ensure data security under the IPP 4 are articulated in terms of "reasonable steps." It is the position of the Office of the Victorian Information Commissioner that compliance with the **Victorian Protective Data Security Framework** amounts to reasonable steps for the purposes of IPP 4.1. While OVIC encourages VPS organisations to report any serious data breaches, the PDP Act does not impose mandatory data breach notification requirements. VPS organisations should consider their data breach notification requirements under any enabling legislation, contractual agreements and the Commonwealth Notifiable Data Breaches (**NDB**)

[32] 'Information society service' is defined under Article 4(25) to mean "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services" (pursuant to point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council).

[33] The test for determining the competence of a minor to consent comes from the English case of *Gillick v West Norfolk AHA* [1986] AC 112. Please refer to page 17 of the *Guidelines to the Information Privacy Principles*, available on OVIC's website, for more information on the consent of minors.

IPPs	Relevant GDPR Provisions	Comparison notes
	requirements, within 72 hours to the relevant supervisory authority. Where the data breach is likely to result in a **high risk to the rights and freedoms of natural persons**, controllers must notify the data subject of the personal data breach without undue delay. The GDPR also provides for the **pseudonymisation** of personal data, as a method to reduce the risks to the data subjects and help controllers and processors to meet their data-protection obligations.[34]	scheme, in relation to Tax File Number information.[35] In relation to the de-identification of personal information, IPP 4.2 places obligations on VPS organisations to take reasonable steps to destroy or permanently de-identify personal information when it is no longer needed. The notion of permanence in relation to de-identified information has raised some issues in practice, considering the ongoing risk of the re-identification of personal information.[36] The GDPR provides for the 'pseudonymisation' of personal data, which refers to the processing of personal data in a way that **can no longer be attributed to a specific data subject without the use of additional information.**[37] To address the risk of re-identification, **Recital 26** notes that any personal data that has undergone pseudonymisation, **which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable person.**
IPP 5 – Openness **Organisations must have clearly expressed policies on the way they manage personal information and make that these policies generally available.**	**Article 5** stipulates that personal data must be processed **lawfully, fairly and in a transparent manner**.[38] **Article 13** provides that a data subject has the right to be made aware of the existence of automated decision-making processes[39] and provided **meaningful information about the logic involved as well as the envisaged consequences** for such processing for the data subject. **Article 30** also requires controllers and processors to keep a record of any processing activities and make this record available to the supervisory authority (independent public authority responsible for monitoring compliance with the GDPR) upon request.	**IPP 5** requires organisations to be transparent about their information handling practices, usually through a current and publicly available Privacy Policy. It is best practice for VPS organisations to draft any Privacy Policies in clear and accessible language, which is consistent with the GDPR requirements. **IPP 5** does not place strict algorithmic-transparency obligations on VPS organisations the way that **Article 13** does for data controllers.
IPP 6 – Access and Correction	**Article 15** provides for a right of access for the data subject, including the right to access their personal data and	The rights of access under **Article 15** are much broader than the rights provided for under **IPP 6**. IPP 6 provides individuals with the right to

[34] Recital 28.
[35] See OVIC's resource on the obligations for the VPS under the NDB scheme, available on OVIC's website. The Office of the Australian Commissioner has published a number of resources available to agencies or organisations captured by the NDB scheme, available here: https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme.
[36] See OVIC's report on de-identification, available on OVIC's website.
[37] Article 4(5) provides that any additional information needs to be kept separately and be subject to technical and organisational measures to ensure that the data no longer relates to an identified or identifiable natural person.
[38] Recital 39 further explains the principle of transparency, requiring that any information and communication relating to the processing of personal data be easily accessible and easy to understand and drafted in clear and plain language.
[39] As referred to in Article 22, which provides data subjects with the right not to be subject to a decision based solely on automated processing, except in certain situations.

IPPs	Relevant GDPR Provisions	Comparison notes
Organisations must provide individuals with a right of access to their personal information, as well as a right to make corrections, if required. An organisation may only refuse a request for access or correction in limited circumstances.	**confirmation that personal data concerning the data subject is being processed**. Article 15 also provides the right for a data subject to access information about the processing of their personal data, including the purpose for processing, how long the data will be stored and, where personal data is transferred to a third country or international organisation, the safeguards in place for the transfer under **Article 46.** **Article 16** provides data subjects with the right to rectification of any **inaccurate personal data**, as well as the **completion** of any incomplete personal data. **Article 17** provides for the right to erasure, or the **right to be forgotten**, which places an obligation on controllers to erase the personal data of a data subject in certain circumstances, including where the personal data is no longer necessary for the specified purpose of collection, or where the data subject withdraws consent for the processing. **Article 19** places obligations on controllers to communicate **any rectification, erasure or restriction of processing** carried out where a data subject has exercised their **right to rectification, right to be forgotten or right to restriction of processing**) to each recipient of the personal data,[40] and inform the data subject who those recipients are upon request. **Article 20** also provides data subjects a **right to data portability**, that is, a right to receive their personal data in a **structured, commonly used and machine-readable format**. The data subject has the right to have their personal data transmitted to another controller.	access their personal information, however, this right does not extend to information surrounding the handling of their personal information specifically, like in the case of **Article 15**.[41] Notification obligations for controllers under **Article 19,** to alert recipients of any rectification, erasure or restriction of processing, are not expressly contemplated under IPP 6. The scope of the right to be forgotten under **Article 17** is greater than the express scope of the equivalent requirements under **IPP 4.2,** to take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose. **Article 17(2)** provides that, where the controller has made the personal data public and the data subject has exercised their right to be forgotten, **the controller shall take reasonable steps (taking into account the available technology and cost of implementation) to inform controllers processing the personal data that the data subject has requested erasure.**
IPP 7 – Unique Identifiers **The use of unique identifiers (usually a number) is only allowed where an**	'Identification number' forms part of the definition of **personal data** under **Article 4.** **Article 87** provides that EU Member States are free to determine the conditions for the processing of	Unique identifiers are defined under the PDP Act to expressly exclude **an identifier that consists only of the individual's name**, whereas the definition of personal data under Article 4 of the GDPR encompasses **identifiers such as a name, an identification number, location data,**

[40] Unless it is impossible or involves disproportionate effort, under Article 19.
[41] This information may be provided to individuals at the time of collection, via a collection notice under IPP 1.3.

IPPs	Relevant GDPR Provisions	Comparison notes
organisation can demonstrate that the assignment is necessary to carry out its functions efficiently by organisations.	national identification numbers or any other identifier of general application, subject to the appropriate safeguards for the rights and freedoms of data subjects under the GDPR.	**an online identifier** etc.
IPP 8 – Anonymity **Where lawful and practicable, individuals must have the option of transacting with an organisation anonymously.**	**Recital 26** defines anonymous information as **information which does not relate to an identified or identifiable natural person, or personal data rendered anonymous in such a manner that the data subject is no longer identifiable**. Recital 26 also notes that the data protection principles under the GDPR are not intended to apply to anonymous information.	Where an individual's identity is not **reasonably ascertainable** from the information held by a VPS organisation, the information will not be considered personal information for the purposes of the PDP Act. Where individuals are able to transact with VPS organisations anonymously, in accordance with **IPP 8**, the organisation may not attract obligations to protect the information under the PDP Act.
IPP 9 – Transborder Data Flows **Personal information can travel outside of Victoria only in certain limited circumstances, outlined under IPP 9.**	**Chapter 5** contains a number of protections for international transfers of personal data. **Article 45** provides for international transfers of personal data based on an **adequacy decision**, where the Commission has decided that the recipient (including a third country or international organisation) offers an adequate level of protection. In the absence of an adequacy decision, international transfers of personal data can be made (in accordance with **Article 46**) where there are appropriate safeguards in place, such as a **legally binding agreement between public authorities and bodies**, **binding corporate rules** (**Article 47**) or **standard data protection clauses adopted by the Commission** (amongst others).[42] **Article 49** provides that derogations from **Articles 45 and 46** may be made in very specific circumstances, such as where the data subject has **explicitly consented to the proposed transfer**.	Under **IPP 9**, VPS organisations can only transfer data outside of Victoria in a number of limited circumstances, including where the organisation **reasonably believes** that the recipient is subject to a law, binding scheme or contract which is **substantially similar to the IPPs**, or where the individual has **consented to the transfer.** The GDPR offers more prescriptive protections for international data transfers, stipulating that controllers and processors may only transfer personal data to a third country or international organisation in limited circumstances, outlined in **Articles 45, 46 and 47** (and Article 49, where applicable).
IPP 10 – Sensitive Information **Special restrictions are placed on organisations collecting sensitive information, as**	**Article 9** prohibits the processing of "special categories of personal data" (sensitive data) including racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. Further, the processing of genetic data, biometric	Both the GDPR and **IPP 10** recognise that higher protections need to be afforded for defined types of sensitive information, and provide that sensitive information must not be handled (or processed, under the GDPR), unless an individual has provided explicit consent (or some other limited circumstance applies).[44]

[42] Article 50 provides for the international cooperation for the protection of personal data, requiring that the Commission and supervisory authorities shall take steps to develop cooperation mechanisms to facilitate effective enforcement of relevant legislation, provide mutual assistance in the enforcement of legislation, including through notification, complaint referral and investigate assistance (amongst other measures) and engage relevant stakeholders to further international cooperation in the enforcement of legislation.

IPPs	Relevant GDPR Provisions	Comparison notes
defined in Schedule 1 of the PDP Act.	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 is prohibited (except in certain, limited circumstances, outlined in Article 9(2)). **Article 10** applies to the processing of personal data relating to criminal convictions and offences based on Article 6(1).[43]	The definition of sensitive information under the PDP Act includes an individual's criminal record, whereas personal data relating to criminal convictions and offences are defined separately from sensitive data, under **Article 10**. The PDP Act also does not apply to health information (whereas Article 9 applies to **data concerning health**).

[43] Article 10 provides that the processing of personal data relating to criminal convictions and offences shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.
[44] See, Article 9(2) and IPP 10.1 and 10.2.

Useful resources

- The Office of the Australian Information Commissioner (**OAIC**) has produced a resource for Australian businesses explaining their obligations under the GDPR. The OAIC also has information available for Australian government agencies, considering whether the GDPR may apply to some of their activities.
- The Information and Privacy Commission in NSW has produced a factsheet, NSW public sector agencies and the GDPR.
- The EU GDPR Portal contains helpful summaries of the Articles of the GDPR and a FAQs series.
- The UK's Information Commissioner's Office has published a Guide to the General Data Protection Regulation.

Further Information

Contact Us

t: 1300 00 6842
e: enquiries@ovic.vic.gov.au
w: ovic.vic.gov.au

Disclaimer

The information in this document is general in nature and does not constitute legal advice.