Office of the Victorian Information Commissioner

Key Concepts

Freedom of Information | Privacy | Data Protection

Key Concepts

On this page

Document version: Key Concepts 2019.B, 14 November 2019.

K.1 The PDP Act and the IPPs use some key words and phrases. This chapter of the IPP Guidelines explains some of these key concepts. In particular, this chapter discusses:

- Personal information
- Sensitive and delicate personal information
- De-identified information
- Consent
- Purpose
- Necessary
- Reasonable, reasonableness
- Practicable

K.2 The starting point for interpreting words and phrases in the PDP Act is s 3 of the Act, which defines terms used in the Act. If a word or phrase is not defined in the PDP Act, the next checkpoint is the dictionary to find the word's ordinary meaning. In some cases, the meaning of key terms has been considered by tribunals and courts, so case law should be consulted as appropriate.

K.3 In working out the meaning of any provision of the PDP Act or IPPs, the interpretation that promotes the purpose or objects of the Act is preferred. Certain materials beyond the Act may also be relevant, such as the Explanatory Memorandum of the PDP Act or its predecessor, the *Information Privacy Act 2000*. Section 35 of the *Interpretation of Legislation Act 1984* (Vic) addresses the principles for interpreting statutes and includes a list of sources which can aid statutory interpretation.

K.4 The PDP Act, like other privacy and anti-discrimination laws, is regarded as 'beneficial legislation' that should be interpreted in a way that is beneficial to those who it is designed to help.[1] This means the PDP Act should be interpreted in a manner favourable to the people whose privacy it protects. The interpretation and application of Victorian statutes also needs to accord with the Victorian *Charter of Human Rights and Responsibilities Act 2006* (**the Charter**). The Charter requires all statutory provisions be interpreted in a way that is compatible with human rights, so far as it is possible to do so consistently with the statute's purpose,[2] and that Victorian public authorities must act in a way that is compatible with human rights, and give proper consideration to relevant human rights when making a decision.[3] The primary international law prohibition on interferences with privacy and attacks on reputation is Article 17 of the International Covenant on Civil and Political Rights (**ICCPR**) which provides that:

1. No one shall be subjected to arbitrary or unlawful interferences with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interferences or attacks.

Personal information

K.5 The PDP Act regulates the handling of 'personal information'. Personal information is, in summary,

[1] *Jurecek v Director, Transport Safety Victoria* [2016] VSC 285 [24]; *Harrison v Victorian Building Authority* (Human Rights) [2015] VCAT 1791 [16].

[2] *Charter of Human Rights and Responsibilities Act 2006* (Vic) (**Charter**), s 32.

[3] Charter, s 38.

information about an individual who is identified or whose identity is reasonably ascertainable.

K.6 It is usually straightforward to decide whether a piece of information is personal information. In cases of uncertainty, organisations should treat information as personal information and handle it accordingly.

K.7 The purpose of this section is to help organisations identify personal information. It explains the definition of personal information in the PDP Act and provides a checklist to consider when making this assessment.

Checklist for assessing whether information is personal information and whether Part 3 of the PDP Act applies.

If the answer is 'yes' to the next three questions, the information is personal information:

Is the information 'recorded'?

1. only information that is recorded in physical or electronic form can be personal information.

2. if information is transmitted in a non-recorded form (for example, a conversation), any subsequent record of that information may be personal information.

Is the information 'about' an individual?

1. an individual must be a subject matter of the information.

2. information can have multiple subjects. Information primarily about one individual can also be about other people and contain their personal information.

Is the individual's identity apparent or reasonably ascertainable?

1. an individual's identity will be apparent if it is clear from the information itself. For example, if their name and other identifying information is directly connected to the information.

2. an individual's identity is reasonably ascertainable if it can be determined by taking reasonable steps. For example, could other information be combined with the information in question that would lead to the individual's identity becoming apparent?

Note: if the personal information is also 'sensitive information' under the PDP Act, there are additional requirements about how it is handled (IPP 10 (Sensitive Information)).

However, if the answer is 'yes' to any of the below questions, Part 3 of the PDP Act will not apply, even if the information is personal information.

Does an exemption apply?

1. For example, is the personal information contained in a 'generally available publication'?

Is all of the information in question health information?

1. Personal information becomes health information when it is information collected for a

health service.

2. Health information is not only held by health service providers.

3. Health information is defined in Schedule 1 of the *Health Records Act 2001* (Vic). It includes, among other things, information or an opinion about:

* the health (physical, mental or psychological) of an individual;
* an individual's disability; or,
* an individual's expressed wishes about future provision of health services to him or her.[4]

K.8 'Personal information' is defined in s 3 of the PDP Act as 'information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained from the information or opinion but does not include information of a kind to which the *Health Records Act 2001* (Vic) applies.'

Living natural persons

K.9 Personal information must be 'about an individual'. Section 38 of the *Interpretation of Legislation Act 1984* (Vic) defines an 'individual' to mean a natural person. This means deceased people, as well as corporations and other types of 'legal persons' do not have privacy rights under the PDP Act.

K.10 Although personal information does not include information about deceased persons, information about a deceased person may include information about a person who is living. Coronial records, for example, may include information about the deceased person's family, friends, employer and colleagues and relevant medical and police officers involved in the coronial inquiry. The privacy of living relatives and other individuals is protected by the PDP Act.

Recorded

K.11 Under the PDP Act, personal information must be 'recorded'. Personal information communicated in a transitory manner and not in any physical medium is therefore not personal information. Conversations which are not diarised or otherwise recorded fall outside the definition. On the other hand, the Act will apply to conversations which are recorded, for example, if notes are taken of the call.

K.12 The PDP Act will not apply where the information only exists in someone's mind. This point was illustrated under similar legislation in New South Wales where information conveyed to an organisation verbally and held only in the mind could not be caught by the privacy legislation 'provided it was never reduced to a written record'.[5] The NSW Court suggested that to find otherwise would make a nonsense out of having to comply with the other principles in the Act, such as the obligations to ensure information is accurate and up to date and to dispose of information securely.

In any form

K.13 Personal information can come in many forms. This includes handwritten notes, emails, SMS

[4] *Health Records Act 2001* (Vic) s 3.

[5] *Vice Chancellor, Macquarie University v FM* [2005] NSWCA 192.

messages, images, sounds (voice recordings) and information in databases. It can include information concealed in a material item, from which an individual's identity is reasonably ascertainable (for example, DNA in human tissue held in a forensics lab for analysis).

'About' an individual

K.14 The individual must be a subject of the information for the information to be considered 'personal information'. While information can have multiple subjects, if the individual is one of those subjects, that information can be considered 'personal'.[6]

K.15 The degree of connection between the information and the individual can vary. This is a question of fact and involves a case-by-case consideration of the relevant context and circumstances. The Federal Court of Australia is of the opinion that there can be 'different degrees of connection between information and an individual. At some point, the connection will be so tenuous that the information will not be "about" the individual.'[7] While the link will be closer in some circumstances, and more distant in others, at some point it will be too remote to be personal information.

Whether identity is apparent or can be reasonably ascertained

K.16 Whether an individual's identity is apparent or can be reasonably ascertained will depend on both the information and the circumstances.

K.17 An individual's identity is '**apparent**' when someone could look at the information and see plainly it is about that individual. For example, an individual's identity would be apparent if the information mentioned the person's name or was a photograph of the person or where the information was of a 'singular nature'.[8] 'Singular nature' means the information could only relate to one person.

K.18 An individual's identity can be '**reasonably ascertained**' if the relevant information can be linked with other information or if reasonable steps can be taken to make the individual's identity apparent. 'Reasonably ascertainable' varies case-by-case depending on how feasible it would be to identify the individual from the information.

K.19 VCAT has indicated extraneous material can be referred to when determining if an individual's identity is 'reasonably ascertainable'. This is necessary to give the phrase meaning beyond what is captured by 'apparent':

> *[T]here will be cases where there is a string of information which must inevitably lead to the identity of a particular person, depending on the context, without the information revealing a person's name or photograph.*
>
> *If such information can all be put together from what is actually contained in the information and from no other source and identifies the person, it would seem that the identity of the person would be "apparent" from the document. The use of the word "ascertained" must allow for some resort to extraneous material unless it is to be regarded as mere surplusage …*
>
> *It may well be that "reasonably ascertained" from the information recognises the use of some extraneous material or information. Support for this view can be found in a decision*

[6] *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 [63]-[64].

[7] *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 [43].

[8] *WL v La Trobe University* [2005] VCAT 2592 [18].

of the Supreme Court of Victoria in Bailey v Hinch [1989] V.R. 78. A similar, but not identical, provision was considered…".[9]

Case Study KC-A: Identity not 'reasonably ascertainable'[10]

A university (in collaboration with other research institutions) conducted a pilot of a longitudinal study on health and relationships. The pilot was carried out by a contractor (a research foundation) and interviews were conducted by telephone. As part of the pilot, the applicant's partner was interviewed and some very personal questions were asked involving information about the applicant and her partner.

The applicant was concerned that, although she did not participate in the survey, she was very much a part of the information elicited and her publicly listed telephone number was used by the researcher to interview the applicant's partner. It was argued that the applicant's identity could be reasonably ascertained by the researcher from the questions and answers provided by her partner, in conjunction with cross-matching her telephone number with electronic white pages to ascertain her name and address.

The university argued the applicant's identity was not reasonably ascertainable because (i) it could not be assumed that the applicant's contact phone number was the same as that of her partner who had been interviewed (i.e., that he lived there permanently); (ii) there was nothing in the partner's answers to home ownership that could link him to the address associated with the applicant's telephone number; (iii) the contractor kept names and telephone numbers on a separate database from the interview answers and questions; (iv) the contractor does not provide contact details to the university, but only provides the interview answers in de-identified form; and (v) as the applicant complained to the university soon after the interview, the contractor was able to strip her contact details form the database (although it would have been more difficult to do so later).

VCAT accepted the identity of the applicant could not be reasonably ascertained:

Even allowing for the use of external information, the legislation requires an element of reasonableness about whether a person's identity can be ascertained from the information and this will depend upon all the circumstances in each particular case. Here, the alleged process of ascertainment would require inquiries from different databases, cross-matching and then cross-matching with an external database and even then, the making of any possible connections would not identify with certainty. Even on the most favourable view to the applicant, this is beyond what is reasonable.

VCAT found this process of cross-matching research databases with external databases would 'involve taking more than moderate steps.' Accordingly, VCAT was not satisfied the complaint was about 'personal information' within the meaning of the *Information Privacy Act 2000* (Vic), the equivalent legislation to the PDP Act at the time.

[9] *WL v La Trobe University* [2005] VCAT 2592 [44]-[45], [47].

[10] *WL v La Trobe University* [2005] VCAT 2592.

K.20 When examining whether identity is apparent or may reasonably be ascertained, organisations should consider how information from other sources may be used in conjunction with the recorded information or opinion to ascertain identity. For example, in *Complainant AH v Department* [2007] VPrivCmr 3, the Privacy Commissioner decided, although the complainant's name was not specifically mentioned, the Department had disclosed personal information about the complainant as the information could be reasonably ascertained within the small rural community. Organisations should consider whether identity can reasonably be ascertained, not whether anyone (the organisation holding it[11] or a third party[12]) intends to try.

K.21 Interpreting 'reasonably be ascertained' should consider techniques such as email, unique machine addresses for computers connected to the internet (for example, IP addresses), 'cookies' and other monitoring software, increasingly powerful online search engines, social media, biometrics, smart cards, reverse phone directories, video surveillance in public and workplaces, electronic databases of some public register data and other information services. Like the other uses of a reasonableness test in the IPPs, 'reasonably' will qualify the operation of 'ascertained' in practice.

K.22 Biometrics (such as physical[13] or behavioural biometrics[14]) and tissue samples (such as hair, blood and bodily samples) may, in some circumstances, enable a person's identity to be reasonably ascertained.[15] If the information is collected by an entity with the means, or that can reasonably obtain the means, to analyse and identify an individual, these sources of data may be regarded as 'personal information'. A sample of hair may be reasonably identifiable in the hands of a police organisation but would not normally be identifiable in the hands of a member of the public. Where the biometric is used to uniquely identify an individual, IPP 7 (Unique Identifiers) will be relevant. See OVIC's short guide to Biometrics and privacy for more information.

Examples of personal information

K.23 Almost any recorded information about an identifiable living natural person can be personal information. It can include correspondence, audio recordings, images, alpha-numerical identifiers and combinations of these.

K.24 Information found to be 'personal information' include:

Address or contact information

[11] Section 4 of the PDP Act states an organisation 'holds' personal information if the information is contained in a document that is in the possession or under the control of the organisation, whether alone or jointly with other parties, regardless of whether the document is situated in or outside of Victoria.

[12] Third party' is defined in s 3 of the PDP Act as meaning any person or body other than the organisation holding the information and the individual to whom the information relates.

[13] Physical biometrics can include fingerprints and iris scans.

[14] Behavioural biometrics include keystroke dynamics, gait analysis and voice ID.

[15] The GDPR specifically recognises biometric data as a subset of sensitive personal data classed as a 'sensitive category of personal data.' The GDPR definition of biometric data is 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that person, such as facial images or dactyloscopic (fingerprint) data'. See, GDPR at Article 4(13), 9.

1. **an individual's name and residential suburb**: *Roberts v Anglicare Victoria (Human Rights)* [2014] VCAT 1515;
2. **an individual's name and address:** *Duggan v Moira Shire Council*, Unreported, VCAT Reference No. G394/2004 (Senior Member Preuss, 9 February 2005); *Complainant P v Local Council* [2005] VPrivCmr 2; *Complainant D v Minister* [2003] VPriv Cmr 4; *Complainant H v Local Council* [2004] VPrivCmr 2;
3. **an individual's name and unlisted telephone number**: *Whitfield v Greater Bendigo City Council* [2005] VCAT 1756;
4. **an individual's change-of-name and new address details**: *Complainant B v Statutory Entity* [2003] VPrivCmr 2;
5. **an individual's mobile telephone number**: *Complainant K v Local Council* [2004] VPrivCmr 5;
6. **a publication referring to a land dispute between the local council and an individual**: *Complainant Z v Local Council* [2006] VPrivCmr 1;

Digital information

1. **an individual's 'chats' and 'posts' made via their personal Facebook account**: *Jurecek v Director, Transport Safety Victoria* [2016] VSC 285;
2. **an email containing allegations of plagiarism about an individual**: *Kudleck v Victoria University (Human Rights)* [2013] VCAT 1791;
3. **publication of an individual's name on an online register as the holder of a sensitive trade activity**: *Complainant E v Statutory Entity* [2003] VPrivCmr 5;
4. **digital recording of a telephone call in which the individual took part and was named**: *Complainant AP v Organisation B* [2010] VPrivCmr 1;

Employment or academic information

1. **where an individual works**: *Seven Network (Operations) Ltd v Media Entertainment & Arts Alliance* (2004) 148 FCR 145;
2. **an individual's work telephone number**: *Complainant M v Tertiary Institution* [2004] VPrivCmr 7;
3. **electronic copies of an individual's correspondence and academic papers**: *Complainant W v Public Library* [2005] VPrivCmr 5;
4. **records created as a result of workplace monitoring of an individual's emails**: *Complainant L v Tertiary Institution* [2004] VPrivCmr 6; *Complainant AR v the Department* [2010] VPrivCmr 3;
5. **a student's candidature for a PhD**: *Complainant F v Tertiary Institution* [2003] VPrivCmr 6;
6. **non-work related material** transferred by an employer to a corporate computer: *Complainant AO v Organisation* [2009] VPrivCmr 4.

Images and footage

1. **a photograph of an individual at a public protest (without a name or any other identifying information being collected):** *Caripis v Victoria Police (Health and Privacy)* [2012] VCAT 1472;
2. **a photograph of an individual**: *Smith v Victoria Police* [2005] VCAT 654;
3. **a digital (CCTV) recording of events in a classroom involving a teacher and students**: *Ng v Department of Education* [2005] VCAT 1054;
4. **surveillance footage of an individual and the surveillance report of that footage:** *Complainant X v Contracted Service Provider to a Department* [2005] VPrivCmr 6; *Complainant AE v Contracted Service Provider to a Statutory Authority* [2005] VPrivCmr 6.

Police-related information

1. **an individual's prior dealings with police**: *Complainant C v Department* [2003] VPrivCmr 3;
2. **disclosures made to a child protection officer about the custody and welfare of an individual's grandson**: *Creely v Department of Human Services* [2004] VCAT 1746;
3. **the results of an individual's criminal record check**: *Complainant Q v Contracted Service Provider to a Department* [2005] VPrivCmr 3.

Other

1. **an individual's fingerprints**: *Complainant AB v Victoria Police* [2006] VPrivCmr 3;
2. **an individual's bank account and leave details**: *Complainant I v Department* [2004] VPrivCmr 3;
3. **correspondence containing information about an individual's concerns about an entity and information about the individual's character**: *Complainant J v Statutory Entity* [2004] VPrivCmr 4;
4. **letters to and from a named individual**: *Dodd v Department of Education and Training* [2005] VCAT 2207; *Complainant AT v Local Council* [2011] VPrivCmr 2; *Complainant AQ v Contracted Service Department to the Department* [2010] VPrivCmr 2;
5. **the identity of an individual's child involved in an incident being investigated by a department**: *Complainant AA v The Department* [2006] VPrivCmr 2;
6. **individuals' membership of an association and their attendance at meetings**: *Complainants R, S, T, U and V v Local Council* [2005] VPrivCmr 3.

Sensitive and delicate information

K.25 Under the PDP Act, certain types of personal information are subject to higher standards of protection. This is called 'sensitive information' and is defined in Schedule 1 of the PDP Act.

K.26 Some information that does not meet the definition of sensitive information may nonetheless need additional protection due to its private or personal nature. This is referred to as 'delicate information'. Although the term is not defined in the PDP Act, it is a useful concept which highlights how some information warrants more careful handling.

K.27 'Sensitive information' is defined in Schedule 1 of the PDP Act as,

> *Information or an opinion about an individual's—*
>
> *a) racial or ethnic origin; or*
> *b) political opinions; or*
> *c) membership of a political association; or*
> *d) religious beliefs or affiliations; or*
> *e) philosophical beliefs; or*
> *f) membership of a professional or trade association; or*
> *g) membership of a trade union; or*
> *h) sexual preferences or practices; or*
> *i) criminal record—*
>
> *that is also **personal information**.*

K.28 Sensitive information is a subset of personal information and is subject to higher protections under the IPPs. For example:

- IPP 10 places restrictions on the collection of sensitive information by Victorian public sector organisations;
- IPP 2.1(a)(i) provides protections for the use and disclosure of sensitive information.

K.29 'Delicate information' refers to personal information that is of a private or personal nature, or information that the individual it is about would likely regards as requiring a higher degree of protection. While the term 'delicate information' is not used in the IPPs, it may be useful to consider whether information is 'delicate' when applying the IPPs because this encourages organisations to apply information privacy and security standards based on how the information might affect the individual.

What is the difference between sensitive and delicate information?

K.30 'Sensitive information' is any personal information that falls within one of the nine categories listed in Schedule 1 of the PDP Act. While 'sensitive information' has a defined meaning in privacy law, in common usage it can mean different things. What individuals may think of as information that is sensitive to them, for example, information they regard as embarrassing or secret, may not fall within one of the nine categories. The term 'delicate information' is used to refer to such information. For example, an individual may choose to disclose their personal information to another, noting it is a secret. While the secretive information may not be considered sensitive information for the purposes of the PDP Act, the individual will likely expect their information will be kept a secret. In this case, the secretive information should be considered delicate information.

K.31 'Delicate information' does not have a fixed definition. It refers to information of a private or personal nature or information that the individual it is about would likely regard as requiring a higher degree of protection.

K.32 'Sensitive information', as defined under the PDP Act, may not always be delicate information. For example, an individual who is a member of a professional or trade association may not necessarily consider that fact to be delicate. However, information of this type falls within the definition of sensitive information under the PDP Act.

K.33 Conversely, personal information, such as an individual's financial records, would generally not be sensitive information. Nonetheless, an individual may consider their financial records to be delicate and expect them to be kept confidential. Similarly, information about an individual's home address would not usually be sensitive. However, if the individual has chosen to suppress their address due to concerns about stalking, they would likely regard their address as requiring additional protection and the information could be described as delicate.

How will an organisation know when they are dealing with delicate information?

K.34 Whether information will be considered delicate is context specific. For example, an individual's name means one thing in the White Pages, another thing on the Australia Day Honours List and quite another thing again on a register of sex offenders. The same piece of information can be interpreted to mean different things, on a spectrum ranging from neutral or non-identifying, personal, delicate and sensitive information.

K.35 Gleeson CJ in *ABC v Lenah Game Meats Pty Ltd* discussed the related question of what information

can be regarded as 'private':[16]

> *There is no bright line which can be drawn between what is private and what is not…(c)ertain kinds of information about a person, such as information relating to health, personal relationships or finances, may be easy to identify as private; as may certain kinds of activity, which a reasonable person, applying contemporary standards of morals and behaviour, would understand to be meant to be unobserved. The requirement that disclosure or observation of information or conduct would be highly offensive to a reasonable person of ordinary sensibilities is in many circumstances a useful practical test of what is private.*

K.36 When deciding whether information is delicate, organisations should consider what the views of the individual the information is about would most likely be. If it appears the person would consider a higher standard of protection should be applied to the information, it should be treated as delicate information.

K.37 Organisations should consider the wider circumstances surrounding the collection, use and disclosure of information considered delicate. For example, if an individual has provided personal information to an organisation when making a complaint and indicated they are afraid of other parties implicated in the complaint finding out, an organisation may treat this information as delicate. This also highlights that information which is part of a wider class of information regularly handled by an organisation, such as personal information from routine enquiries received by the organisation, may be considered more delicate than other types of information of the same class, depending on the surrounding circumstances.

How should organisations protect delicate information?

K.38 While the term 'delicate information' is not used in the IPPs and there are no specific obligations that attach to it, it may be useful to consider whether information is 'delicate' when applying the IPPs. For example:

- When considering what 'reasonable steps' are needed to protect the information under IPP 4, delicate information may need greater protections than innocuous information.
- When deciding whether a secondary use or disclosure of the information would be within the 'reasonable expectations' of the person it is about, for the purpose of IPP 2. Members of the community will often expect delicate information be used or disclosed more sparingly.

Are biometrics sensitive or delicate information?

K.39 Privacy laws around Australia define personal information and sensitive information differently. Under the federal *Privacy Act 1988*, for example, biometric information (including biometric templates) is considered to be sensitive information, for which higher protections relating to collection and use apply when compared to personal information.

K.40 In Victoria, however, the definition of sensitive information under the PDP Act does not explicitly include biometric information. Nonetheless, some biometric characteristics (for example, facial biometrics) may reveal sensitive information as defined under the PDP Act, such as information about a person's racial or ethnic origin. Further, the higher protections afforded to biometric data in other jurisdictions may impact community expectations about how that data should be treated in

[16] *ABC v Lenah Game Meats Pty Ltd* [2001] HCA 63 [42].

Victoria.

K.41 OVIC suggests organisations regard biometric information as delicate information and handle it accordingly.

De-identified information

K.42 De-identification is often regarded as a way to protect the privacy of personal information when sharing or releasing data.

De-identification in the IPPs

K.43 Section 3 of the PDP Act defines 'de-identified' as 'personal information that no longer relates to an identifiable individual or an individual who can be reasonably identified'.

K.44 'De-identified' also appears under IPP 4.2. Organisations are required to 'take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose'. IPP 4.2 implies it is possible for de-identification to be permanent, however, recent events have demonstrated that while de-identification is important for privacy protection, 'de-identified' is not a permanent state and does not necessarily prevent re-identification.[17]

De-identification in practice

K.45 De-identification involves removing direct identifiers and removing or altering other identifying information such as indirect or quasi-identifiers. Direct identifiers could be a name or address. Examples of indirect or quasi-identifiers are date of birth, gender and profession. In practice, de-identification generally occurs in two contexts: where a duplicate dataset is de-identified for a particular use or disclosure, or where organisations de-identify information they no longer need under IPP 4.2. Where organisations de-identify information they no longer need and de-identification occurs on the original record, records may be destroyed or irrecoverably altered. Organisations need to ensure de-identification occurs consistently with record-keeping obligations under the *Public Records Act 1973* (Vic).[18] IPP 4.2 also provides information about obligations under both acts, see Relevance of the Public Records Act.

K.46 To ensure de-identification has been successful, it is also necessary to consider whether the information might be re-identified, for example, by linking it with other datasets. For more information on de-identification techniques and de-identification in practice, see OVIC's guidance on De-identification and privacy. Whether de-identification is successful depends on the context in which the information will be used or disclosed. Personal information that is de-identified in one context (for example, where the data is used in a controlled environment for a clearly defined purpose) may be re-identifiable in another (for example, in an open data context where auxiliary or additional identifying information can be used to identify them). For example, the risk of re-identification may be especially high where datasets contain information of persons from a small community as a particular combination of information in the datasets may make a person's identity

[17] See, for example, '*Australian Information Commissioner and Privacy Commissioner's investigation into published MBS/PBS dataset*', March 2018, available at www.oaic.gov.au.

[18] This means destruction must be 'authorised'. The Public Records Office Victoria (**PROV**) Disposal Standard explains destruction can be authorised through Normal Administrative Practice, Retention & Disposal Authorities or Single Instance Disposal Authorities. For more information regarding destruction of information, see PROV's Disposal Standard <https://prov.vic.gov.au/recordkeeping-government/document-library/pros-1013-disposal>.

reasonably ascertainable.

K.47 Advancements in technology have increased the types of data and the rate at which it is generated. It is easier to find and link disparate datasets which means the risk of re-identification is higher than ever before. Organisations should assume data can be re-identified. OVIC recommends de-identified data be used in a controlled environment, for example, a data analytics lab.[19]

Related concepts: Pseudonymisation and anonymised data

K.48 The Victorian Centre for Data Insights (**VCDI**) has described pseudonymisation as 'a kind of masking where personal information is replaced with a pseudonym…which does not itself contain personal information'.[20] Just because personal information has been pseudonymised, does not mean it is de-identified.

K.49 'Aggregation' is sometimes used interchangeably with 'de-identification'.[21] 'De-identification' is the term used by OVIC for this concept, as it is used in the PDP Act. As there are many different terms to describe processes similar to de-identification, it is important for organisations to check there is a mutual understanding of the terminology being used between all parties.

Consent

K.50 Assessing whether the necessary consent has been given will depend on the circumstances of each case. The five elements of consent are the individual has the *capacity* to consent and that the consent is *voluntary*, *informed*, *specific* and *current*. Under s 3 of the PDP Act, consent means 'express or implied consent'.

K.51 Consent can be valuable for agencies to satisfy both their own information needs and their obligations under the PDP Act. Consent allows individuals to control how their personal information is collected and used. Organisations which seek to gain consent where possible will have a clear basis for carrying out information handling and are more likely to find community acceptance of their practices.

K.52 Consent is not the only basis by which information can be collected or used. The IPPs allow the collection, use and disclosure of personal information in circumstances where consent has not, or cannot, be obtained. Examples include:

- when an organisation collects information necessary for its functions (see IPP 1);
- when information is used for the primary purpose it was collected (see IPP 2.1);
- when information is disclosed for one of the reasons outlined under IPP 2.1(a), (c)-(h); and
- when information is publicly available.

K.53 The Australian Law Reform Commission (**ALRC**) noted that specific requirements for consent are often highly dependent on the context in which personal information is collected, used or disclosed, including how consent is sought, and the characteristics of the person from whom consent is sought.' Consent may be given on behalf of an individual where the individual lacks capacity to consent in

[19] For more information on de-identification in a controlled environment, see the De-identification Guideline published by the Victorian Centre for Data Insights (**VCDI**) on the VDCI website and OVIC's report Protecting unit-record level personal information.

[20] VCDI, De-identification Guideline, p 10. See the VCDI website.

[21] See, for example, OAIC and Data 61 'The De-Identification Decision-Making Framework,' p 5.

accordance with s 28 of the PDP Act. This is discussed further under 'Capacity'.

Elements of consent

K.54 The elements of consent are:

- Capacity (consider mature minors);
- Voluntary (consider opt in or opt out models);
- Informed;
- Current; and
- Specific (consider bundled consents, express or implied consent).

Capacity

K.55 Capacity to consent arises throughout the PDP Act and is one of the main factors to consider when deciding whether an individual can make a privacy complaint.[22]

K.56 An individual may not be capable of giving consent. Factors which may prevent the individual from understanding the circumstances of consent or communicating their response include:

- physical or intellectual disabilities;
- age; and
- cultural or linguistic differences.

K.57 The individual may not understand the general nature and effect of giving or withholding consent. If an organisation is uncertain that a person has capacity to consent, it should not rely on any purported consent.[23]

K.58 Section 28 of the PDP Act addresses situations where, despite the provision of reasonable assistance by another individual –

- a person is incapable of understanding the general nature and effect of giving consent, making the request or exercising the right of access; or
- communicating the consent or refusal of consent, making the request, or personally exercising the right of access.[24]

K.59 This incapacity may be due to age, injury, disease, senility, illness, disability, physical impairment or mental disorder. Where a person is incapable of consenting or making a request for access or correction of information, an authorised representative may do so on their behalf.[25]

Capacity, consent and mature minors

K.60 Assessing whether a minor has the competence to consent can be difficult. The question of whether

---

[22] Section 59(1) of the PDP Act states a complaint may be made (a) by a child; or (b) on behalf of a child by (i) a parent of a child; or (ii) any other individual chosen by the child or by a parent of the child; or (iii) any other individual who, in the opinion of the Information Commissioner, has a sufficient interest in the subject matter of the complaint. Sub-section (2) states that 'A child who is capable of understanding the general nature and effect of choosing an individual to make a complaint on the child's behalf may do so even if the child is otherwise incapable of exercising powers'.

[23] Further information on assessing the capacity of a person to provide consent, please refer to the *Law Institute of Victoria's LIV Capacity Guidelines and Toolkit*.

[24] PDP Act, s 28(3).

[25] 'Authorised representative' is defined in s 28(6) of the PDP Act and includes a guardian, parent and an individual endowed with an enduring power of attorney.

a mature minor can lawfully provide consent is a complex area and continues to be examined by the courts.[26]

K.61 Advising age ranges in which a minor is considered capable of providing consent may be too prescriptive, as determinations of a child's capacity to provide consent are subjective and depend on the individual minor.[27]

K.62 While s 3 of the PDP Act defines a child as being a person under the age of 18 years, it does not specify an age after which individuals can make their own privacy decisions.

K.63 For consent to be valid, an individual must have capacity to consent. Where consent is needed for an organisation to handle the personal information of an individual under the age of 18, the organisation will need to determine whether that individual has the capacity to consent.

K.64 Where the personal information concerns a child or young person, he or she may be able to exercise their rights under the PDP Act independently of a parent or guardian if he or she has sufficient understanding and intelligence to give valid consent (the 'Gillick competence'). The principle of 'Gillick competence' was stated in the English House of Lords in *Gillick v West Norfolk AHA*(1986) AC 112: 'A minor is, according to this principle, capable of giving informed consent when he or she "achieves a sufficient understanding or intelligence to enable him or her to understand fully what is proposed".'

Voluntary

K.65 An individual must be free to exercise genuine control and choice to provide or withhold consent. Consent must be given without coercion or threat and with sufficient time to understand the request and, if appropriate, get advice.[28]

K.66 Where an individual has no meaningful choice as to whether they provide their personal information, the individual has not provided consent. Similarly, where an individual is expressly required to provide their personal information, organisations should not frame the exchange of information as being based on consent. This may occur where an organisation has the legal authority to collect their personal information for a distinct, lawful purpose. Rather than relying on the consent of the individual, organisations should outline the legal authority to collect the information in a collection notice.

K.67 In many circumstances, an individual does not have a real or effective choice regarding consent. Employees asked to undergo a criminal record check, medical examination, drug test or psychological assessment may not often give voluntary consent.[29] If it is not possible to obtain voluntary consent,

---

[26] See for example, *X v The Sydney Children's Hospitals Network* [2013] NSWCA 320; *Re Jamie* [2013] FamCACF 110; and *Central Queensland Hospital and Health Service v Q* [2016] QSC 89.

[27] The European Union's General Data Protection Regulation (**GDPR**) provides an example of how other jurisdictions approach mature minor consent. Article 8 sets out the conditions applicable to a child's consent to the processing of their personal data in relation to information society services offered directly to a child. The default age at which a person is no longer considered a child is 16, however it allows that limit to be adjusted by member states anywhere between 13 and 16. Any collection of data from children under the age of 13 is prohibited. Implementation of the GDPR will be helpful to inform a view on the lawful consent of minors. It is likely some trends will emerge in this area prompted by the GDPR.

[28] NSW IPC, 'Guidance: Consent'.

[29] For further information on obtaining meaningful consent in the workplace, please see Fairwork Australia's information on workplace privacy.

organisations will need to find some other basis for collecting the information. If the test or check does not involve collection of sensitive or health information, the check or test can be conducted if it is necessary for the organisation's functions and activities, and is not carried out in an unreasonably intrusive way.[30] If the collection involves sensitive information, one of the exceptions in IPP 10 must apply – for example, the check or test must be required by law.[31] If health information is involved, the organisation will need to consider the exceptions in Health Privacy Principle 1.1.[32]

Case Study KC-B: Purported consent not voluntary[33]

The complainant was an employee of the respondent organisation and made a bullying claim against co-workers. The complaint documents consisted of a letter outlining the outcomes the employee sought and a chronological list of all the bullying incidents alleged to have occurred. The complainant met with a staff member of the organisation who explained the complaints process and advised that a full copy of the complaint documents would be provided to each of the alleged bullies. The complainant agreed believing there was no other choice, but later attempted to withdraw her consent as she was anxious about the information contained in the complaint documents. The organisation advised the documents had already been forwarded to the alleged bullies.

The Privacy Commissioner decided the complainant's consent could not be relied on as under IPP 2.1(b) individuals must be provided with a real choice about what will happen with their personal information. The complainant was merely told the disclosure of her complaint documents to the alleged bullies was part of the complaint investigation procedure and that there was, in effect, no other option. Because the complainant was not given a real choice, the purported consent could not be relied on.

Opt In versus Opt Out

K.68 An opt-in consent model means personal information cannot be used or disclosed for purposes (such as marketing) unless the person has given their prior consent to the particular use or disclosure.

K.69 An opt-out model is where individuals are told their personal information will be used or disclosed in a particular way unless they take some action (for example, ticking a box) to say they do not consent.

K.70 The opt-in model is preferable as it requires the individual to actively provide consent. This minimises possible doubt as to whether consent has been voluntarily provided. The opt-in model also assists in ensuring the person has read the purpose of the consent they are providing and therefore have made an informed decision.

K.71 Opt-out models create uncertainty as to whether consent is validly given. Simple failure to tick a box, as in the example above, may be due to the individual not reading that section of the form rather

[30] See IPP 1.1 and IPP 1.2.

[31] See IPP 10.1.

[32] See Schedule 1 of the *Health Records Act 2001* (Vic) available on austlii.com.

[33] *Complainant AU v Public Sector Agency* [2011] VPrivCmr 3.

than the person actively consenting to what is proposed.

Informed

K.72 The individual must have full knowledge of all relevant facts, including:

- the personal information to be collected, used or disclosed;
- the purpose(s) for the information;
- who will receive the information, who will be accessing the information, who it may be passed on to and what use the recipients will make of the information; and
- the consequences of giving, or failing to give, consent.

K.73 Incorrect or misleading information will likely render the consent invalid. Organisations should ensure an individual is properly and clearly informed about how their personal information will be handled.

K.74 In *JK v Department of Transport Infrastructure Development* [2009] NSWADT 307 at [78]-[79], the NSW Administrative Tribunal has observed:

> *'[u]nder the general law such consents must be both freely given and informed… Whether any given consent will operate to satisfy the consent requirements will depend on the construction of the consent itself, the circumstances in which it was given, and the understanding of the person giving consent, taking into account their particular vulnerabilities'.*

Current

K.75 Consent has an expiration date. Consent cannot be assumed to endure indefinitely. It is good practice to inform the individual of a specified period for which the consent will be relied on in the absences of a material change of circumstances that the organisation knows or ought reasonably to know. If consent was not sought at the time of collection or that consent did not cover a proposed use or disclosure, an entity should seek the individual's consent at the time of the use or disclosure.

K.76 A person is entitled to change their mind and choose to revoke consent later. It should be as easy for an individual to withdraw consent as it is to give consent. Individuals should be provided information on how to withdraw consent when consent is sought. Legislation may expressly deal with the revocability of consent. For example, a statute may state that consent is irrevocable, or the law may set conditions around the timing and effect of any withdrawal of consent.[34]

K.77 Whether consent that has been given in the past is still current depends on the circumstances in which consent was given, and the amount of time that has passed.

Specific

K.78 Consent must be specific to an identified purpose in all the circumstances. An organisation should not seek a broader consent than is necessary for its purposes. If the information given is too broad or vague, the consent may not be specific enough to be regarded as valid for the particular collection, use or disclosure that the organisation makes. Broadly worded consent statements may be problematic when demonstrating why it is necessary or lawful for personal information to be collected. The level of specificity will depend on factors including:

- The nature of the personal information;

[34] See, for example, *Crimes Act 1958* (Vic) ss 464ZGC-464ZGF; *Adoption Act 1984* (Vic) s 41.

- The proposed use or disclosure;
- The recipient and its proposed use or disclosure; and
- The recipient's level of accountability.

K.79 Generally, the more privacy invasive the proposed use or disclosure of information is, the more specific the required information and consent should be.[35]

Bundled consent

K.80 'Bundled consent' refers to the practice of bundling together multiple requests for consent to cover a wide range of uses and disclosures of personal information without giving individuals an opportunity to choose what uses and disclosures they do or do not agree to.

K.81 Bundled consents can be problematic as they have the potential to undermine the voluntary nature of the consent. 'Broad' or 'bundled' consent forms diminish individuals' freedom of choice. Effectively, they coerce individuals to hand over their personal information and to agree to a variety of uses and disclosures in exchange for a service.[36]

K.82 If the use of bundled consents is contemplated, organisations should consider whether individuals are:

- Given a reasonable opportunity to freely elect to refuse consent to one or more proposed uses or disclosures;
- Sufficiently informed about each of the proposed uses or disclosures, including the purpose for the use or disclosure, the identity or type of organisation who will receive the information and any further use or disclosure that the recipient is to make of the information;
- Informed of any law which requires the individual to consent to any one or more of the proposed uses or disclosures and which of these proposed uses and disclosures are not compulsory; and
- Advised of the consequences (if any) of failing to consent to any one or more of the proposed uses or disclosures.

Express and implied consent

K.83 'Consent' is defined in s 3 of the PDP Act as express or implied consent.

K.84 Express consent is where the individual has stated they provide consent for the specific purpose outlined by the organisation. As a general rule, it is preferable to seek express consent in writing to provide clarity and transparency for the individual and the organisation. Express consent can also minimise the potential for confusion or ambiguity between the individual and the organisation as to whether consent has been provided and for what purpose.

K.85 Implied consent can be obtained where consent can reasonably be inferred from a person's conduct or actions. The test is objective. Organisations must not make assumptions about implied consent. It is risky to infer consent from a person's failure to refuse consent. The person may not have heard, understood or had sufficient information on which to decide to refuse.

---

[35] ALRC, *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108) [62.81]-[62.82].

[36] *OPC v Employment Services Company* [2005] PrivCmrA 13.

K.86 Consent should not be inferred in a particular case just because:

- most people have consented to the same use or disclosure;
- the benefits of consenting, as the organisation sees them, mean the individual would probably consent if asked;
- the individual has given consent in the past; or
- the disclosure is to a spouse or family member.

K.87 Implied consent can be difficult to establish if a complaint arises. Express consent is preferred as it can help avoid the confusion and lack of transparency which can arise from reliance on implied consent. The nature of the personal information and the circumstances will also dictate the most practical form of consent.

Notice versus consent

K.88 A collection notice is a statement provided to an individual at or before the time an organisation collects personal information from them. Under IPP 1.3, organisations must provide notice of collection 'at or before the time (or as soon as practicable after)' that an individual's personal information is being collected. The notice explains to individuals the purpose for which the information is collected and how the organisation will use and handle the information.

K.89 Notice is not the same as consent. When seeking consent, providing details about the intended use of the requested information can help an individual decide whether to provide consent. Consent must be an affirmative action, part of a two-way communication where the individual can respond to the agency request to use their information.

K.90 Consent and collection notices describe the purpose of the collection and use of personal information. They must also inform the individual of the information relevant to the provision of their personal information. One of the main differences between consent and notice is that when consent is being sought, the individual has to actively express that they agree to provide the information for the purposes outlined in the information provided by the organisation. Also, there are differences as to when a collection notice is used and when consent is sought.

Seeking consent in practice

K.91 Although there is no requirement to record consent, OVIC suggests this should be done where possible. A written record of consent is preferred so the individual has adequate opportunity to understand and decide whether to provide consent and the organisation and the individual can have a record of specifically what consent was provided. Information related to a person providing consent may include a record of verbally provided consent or capacity assessments.

K.92 An organisation's contact information should always be provided to an individual so they may make enquiries at any stage about the consent they have provided or so consent can be withdrawn.

K.93 Legal advice may also ensure consent is sought where necessary and in a manner that meets the legal requirements of valid and meaningful consent.

Purpose

K.94 The purpose of an action is the reason for which it is done. 'Purpose' in the context of the IPPs refers to the reason for the collection, use and disclosure of personal information. The purpose for which personal information is handled should be clearly defined upfront and communicated to individuals.

K.95 Organisations should clearly define the purpose of collection upfront. Doing so will inform how the IPPs apply throughout the lifecycle of the information. The purpose for collection should be specific, with a clearly defined scope and communicated to individuals at the point of collection, via a collection notice.

K.96 Unless an organisation knows the purpose for the collection of personal information, it cannot readily assess or assert its necessity (IPP 1.1) or its lawfulness and fairness (IPP 1.2). Being unclear about the purpose will make assessing the use and disclosure of information difficult under IPP 2.1. Determining the purpose also helps an organisation ascertain the required standard of data quality (IPP 3) and whether additional steps should be taken to secure the data (IPP 4.1).[37]

K.97 Purpose is expressly referred to in IPPs 1, 2, 4, 5, 7 and 10.

K.98 In *Ng v Department of Education*[2005] VCAT 1054, the meaning of 'purpose' was defined narrowly by VCAT as synonymous with the intent with which personal information was collected.[38] This involves an enquiry into the motive behind collection, rather than an enquiry into the effect the collection practice would have. VCAT cautioned against taking a wide view of 'purpose'.

Function creep

K.99 'Function creep' refers to situations where personal information collected for one stated reason is later used for other purposes, perhaps quite unrelated to the original purpose of collection. The term usually arises where individuals might not have willingly provided their information or tolerated the introduction of a new potentially intrusive practice had they known what uses would eventually be made of their information. Particularly, this occurs where privacy invasive secondary uses were not originally envisaged or where assurances had been given that functions would not 'creep' or expand and the eventual uses would not occur. Function creep undermines the transparency objective of the PDP Act[39] and is destructive of public trust in government.

K.100 A privacy impact assessment (**PIA**) can help prevent function creep. As part of the PIA process, organisations can identify the potential uses of the information, including those outside of the immediate identified purpose for collection. It is also useful to think about who might be involved in providing personal information or affected by the use of their personal information. Identifying these individuals and their reasons for interacting with an organisation can help identify other possible purposes which may differ from those communicated to the individual by the organisation at the point of collection. For example, the individual may interact with an organisation for a specific reason which may lead to their information being used or collected for additional purposes not envisaged by the organisation. In addition to helping avoid function creep, a PIA helps help prevent potential privacy breaches, particularly in relation to IPPs 1 and 2.

K.101 There are many good reasons for making secondary use of information already collected. However,

---

[37] For example, information collected for a financial or delicate purpose may indicate tighter security requirements.

[38] *Ng v Department of Education* [2005] VCAT 1054 at [88]-[89].

[39] Under s 5(d) of the PDP Act.

transparency and proper limits maintain individuals' willingness to supply their information fully and accurately and maintain trust that personal information is used responsibly and legitimately.

Necessary

K.102 'Necessary' is referred to in IPPs 1, 2, and 7. The term is not defined in the PDP Act, so it is useful to refer to case law.

K.103 In *Jurecek v Director, Transport Safety Victoria*, 'necessary' was interpreted according to 'reasonable proportionality'.[40] To understand what is necessary, organisations should balance 'the nature and importance of a legitimate purpose and the extent of the interference'.[41] In *Ng v Department of Education*,[42] VCAT held 'necessary' means 'subjected to the top scale of reasonableness'.[43]

K.104 Under the Victorian Charter, issues of necessity and proportionality are relevant to the conduct of public sector organisations where their acts and practices have an impact on privacy and other human rights recognised under the Charter.[44]

K.105 In *Hogan v Hinch* [2011] HCA 4 and *Mulholland v Australian Electoral Commission* [2004] HCA 41, the High Court of Australia stated that what is 'necessary' in the human rights field should be proportionate to legitimate aims and competing interests.[45] 'Necessary' does not mean 'essential' or 'unavoidable' but it does involve 'close scrutiny' and a 'compelling justification'.[46] Further, 'necessity' is the availability of no other obvious, compelling and equally effective means of achieving the legislative object which has a less restrictive effect on the freedom.[47]

K.106 'Necessary' requires more than what may be administratively convenient or desired. Government administration has access to powerful information and communications technologies which deal with individuals' personal information. This means it is important to guard against a temptation – however understandable it may be – to read down the test of necessity.

K.107 Necessity is discussed further in these Guidelines as it arises in the context of each of the relevant IPPs.

Reasonable, reasonably

K.108 What is considered 'reasonable' will differ according to the context in which it is applied. This means that it will depend on the particular organisation and the circumstances surrounding the personal

---

[40] *Jurecek v Director, Transport Safety Victoria* [2016] VSC 285 [70].

[41] *Jurecek v Director, Transport Safety Victoria* [2016] VSC 285 [70].

[42] *Ng v Department of Education* [2005] VCAT 1054.

[43] *Ng v Department of Education* [2005] VCAT 1054 [77] citing *Pelechowski v Registrar Court of Appeal (NSW)* (1999) 198 CLR 435 [452].

[44] See the *Charter of Human Rights and Responsibilities 2006* (Vic), especially s 7 (when human rights may be limited), s 32 (interpreting laws in manner compatible with human rights) and s 38 (obligations on public authorities to consider relevant human rights).

[45] *Mulholland v Australian Electoral Commission* [2004] HCA 41 [36]-[37]. See also *Hogan v Hinch* [2011] HCA 4 [72].

[46] *Mulholland v Australian Electoral Commission* [2004] HCA 41 [39]. See also *Hogan v Hinch* [2011] HCA 4 [72].

[47] *McCloy v New South Wales* [2015] HCA 34 [81].

information. Reasonableness as it applies to privacy should be viewed through a human rights lens. That is, an assessment of whether an action is reasonable should take account of its impact on the human right to privacy.

K.109 Variations of 'reasonableness' appear in the definition of 'personal information' and throughout several of the IPPs.

K.110 To be reasonable is to be fair, proper and moderate. The High Court of Australia considers what is reasonable to be a judgment of fact. What is reasonable will depend on each particular case,[48] and may be influenced by current standards.[49] A reasonableness test applies a reasoned and objective judgment to the circumstances. It implies taking a balanced view.

Reasonableness and human rights

K.111 Decisions involving personal information affect individuals' human rights as they expose individuals to a greater or lesser risk of their privacy being interfered with. As such, when assessing what is 'reasonable', organisations must view decisions through a human rights lens. This involves giving due consideration to any impacts on the right to privacy. When making decisions regarding personal information, organisations should balance any potential interference on individuals' right to privacy against the broader purposes of the decision and other organisational objectives.

K.112 This is reflected in Justice Bell's comments in *Jurecek v Director, Transport Safety Victoria* [2016] VSC 285. In that case, the Supreme Court of Victoria made the following statement about what constitutes 'reasonable steps'.

> *To a greater or lesser extent, matters of fact and degree are involved, which requires consideration of what is at stake for the individual (including the nature of the personal information in question) and balancing, in a reasonably proportionate way, the nature and importance of any legitimate purpose and the extent of the interference.*[50]

K.113 Decisions about how an organisation should secure personal information should be informed by the possible adverse impacts for an individual if the information is compromised. Decisions are 'reasonable' when the security measures are proportionate to the potential consequences – to both the organisation and to individuals – if the information were to be compromised.

Practicable

K.114 The IPPs refer to the term 'practicable' in IPPs 1, 2, 6, 8, 9 and 10.

K.115 'Practicable' means feasible or able to be done.[51] The word also incorporates an element of reasonableness. When the reasonableness or practicability of doing something is examined, cost is one consideration. Like other pieces of legislation which impact Victorian public sector agencies, the PDP Act may require an organisation to change its practices to ensure obligations under the IPPs are upheld. Processes and procedures need to be assessed and where necessary amended, time spent,

---

[48] See, for example, *Jones v Bartlett* [2000] HCA 56 [57]-[58].

[49] *Bankstown Foundry Pty Ltd v Braistina* [1986] HCA 20 [12].

[50] *Jurecek v Director, Transport Safety Victoria* [2016] VSC 285 [70].

[51] *CNK v R* [2011] VSCA 228 [8].

attention given, and costs incurred.

K.116 The Commonwealth Administrative Appeals Tribunal has said 'what amounts to reasonably practicable steps must be assessed on a case by case basis'.[52] Organisations should consider the particular circumstances.

> Please send any queries or suggested changes to privacy@ovic.vic.gov.au. We will respond to privacy enquiries and consider your suggestions when we next update the Guidelines to the Information Privacy Principles.

Version control table

Version	Description	Date published
Key Concepts 2019.B	Edits following consultation.	14 November 2019
Key Concepts 2019.A	Consultation draft.	28 February 2019
Key Concepts (2011)	2011 pdf version.	2011

[52] *TYGJ and Information Commissioner* [2017] AATA 1560.