Comparing the Data Protection and Use Policy (DPUP) to the information privacy principles (IPPs)

What this guidance covers

This guidance describes:

- how the DPUP Principles and Guidelines address the Privacy Act 2020's IPPs
- where they contain good practice guidance that goes beyond IPP requirements
- what that additional good practice guidance is.

The guidance addresses how DPUP recognises that other laws can modify or override the IPPs and provides key examples of where that happens. It also links to other government guidance on such laws. It summarises aspects of DPUP that are beyond the scope of the Privacy Act 2020 as they relate to nonpersonal information.

Who this guidance is for

This guidance is designed for people who want a detailed comparison of DPUP against the Privacy Act 2020's IPPs. This may include people advising on privacy or legal considerations and those training others on DPUP.

Privacy Act 2020

The DPUP Guidelines were drafted before the Privacy Act 2020 was finalised and enacted. The Guidelines have been updated to accommodate changes in the 2020 Act that are material to DPUP. The Privacy Act 2020 came into force from 1 December 2020.

Read the IPPs on the Office of the Privacy Commissioner's website: privacy.org.nz/privacy-act-2020/privacy-principles/

Read DPUP's Guidelines at digital.govt.nz/dpup/guidelines

Table 1: Mapping the IPPs to DPUP and explaining where DPUP good practice guidance goes beyond the IPPs

Information privacy principle – addressed in which DPUP Guideline(s)	Where and how Guidelines' good practice guidance goes beyond the IPP requirements
Principle 1: Purpose of collection of personal information An agency can only collect personal information if it is collected for a lawful purpose connected with a function or activity of the agency, and the collection of the information is necessary for that purpose. If the lawful purpose for collecting the personal information about an individual does not require their identifying information to be collected, then the agency may not require it. **Addressed in which Guideline** • Purpose Matters Guideline	The Purpose Matters Guideline goes beyond the IPP1 requirements in the following areas: • De-identified information: emphasises the importance of considering purpose even where personal information has been de-identified. • Specific statutory power: explains why assessing purpose is relevant when collecting, using or disclosing personal information under a specific statutory power. • Recording purposes of collection: provides guidance on importance of documenting purposes of collection. • Methodology: suggests an approach to defining / assessing purposes of collecting / using personal information. • What people may think: considers what people providing the information will think about the proposed use of their information. • Evolving purpose statements: provides guidance on care to be taken with evolving statements of purpose. • Different analytical techniques: provides guidance on considering whether there are different analytical techniques or processes that affect how much information is collected.

Information privacy principle – addressed in which DPUP Guideline(s)	Where and how Guidelines' good practice guidance goes beyond the IPP requirements
	• Is information required from all service users?: provides guidance on considering whether personal information needs to be collected from every service user or whether some can opt out. • Broader privacy interests: considers broader groups' legitimate privacy interests. • Sensitivities and adverse consequences: provides guidance on considering sensitivities and possible adverse consequences even where collection is lawful. • Trust relationships: provides guidance on considering, when collecting personal information from another agency, the potential impact on trust relationships between the other agency and its service users. • Checks and balances: checklists that can be worked through to carefully consider proposed purposes, including consulting service users, agencies, Māori groups, external experts and others as needed. • Identifying information for insights: provides guidance on identifying what the most useful information will be to support developing insights, including qualitative and interpretative information.
Principle 2: Source of personal information Agencies are required to collect personal information directly from the individuals concerned, unless an exception applies. **Addressed in which Guidelines** • Purpose Matters Guideline (in the context of an IPP2 purpose-related exception) • Transparency and Choice Guideline	The Guidelines do not contain good practice guidance going beyond, or that could be seen as extending, the IPP2 requirement. However, the Manaakitanga Principle does recognise that service users should be included and involved whenever possible. They may be able to offer greater value than just their information, and their ideas and views should be included when developing or testing proposals to collect and use data or information to improve wellbeing.
Principle 3: Collection of information The collecting agency must take any steps that are, in the circumstances, reasonable to ensure that the individual concerned understands what information will be collecting and why, and what their rights are. **Addressed in which Guidelines** • Purpose Matters Guideline (in the context of purpose and transparency-related discussions) • Transparency and Choice Guideline (comprehensively addresses a wide	Providing purpose-related information to other agencies: IPP3's focus is on what individuals are to be told when an agency collects personal information from them. The Privacy Act 2020 is silent on what an agency should tell another agency when collecting personal information from that other agency. The Purpose Matters Guideline emphasises the importance of providing purpose-related information to such agencies and explains why. How information will not be used: where appropriate, agencies should consider telling people how their information will not be used. Perceptions of linking: provide guidance on considering how people could perceive their data being linked with other data and what they should be told about it.

Information privacy principle – addressed in which DPUP Guideline(s)	Where and how Guidelines' good practice guidance goes beyond the IPP requirements
range of transparency and choice-related issues)	Use of de-identified information: the Transparency and Choice Guideline recommends that agencies are transparent about what they are doing with people's information even when it has been de-identified. Telling people about more than IPP3 requires: provides guidance on making people aware of matters beyond the IPP3 requirements, including more granular guidance than the wording of IPP3 on informing people about who will see their personal information, whether inside or outside of the collecting agency. Helping frontline staff understand: provides guidance on helping frontline staff to fully understand the reasons for collection to enable them to be transparent with service users. Methods of helping people understand: provides guidance on considering how information may be communicated to service users in a manner that works for them, providing multiple opportunities for understanding if needed, and providing a safe and responsive environment. Choice: provides guidance on giving people choices, where an agency can, about whether personal information needs to be provided (exceeding IPP3 requirements) or how the information is captured or who is able to see the information.
Principle 4: Manner of collection of personal information Agencies must not collect personal information by unlawful means, or means that are unfair or intrude unreasonably on the personal affairs of the person concerned. Agencies need to take particular care when collecting personal information from children and young people. **Addressed in which Guideline** • Transparency and Choice Guideline	This Guideline goes beyond the IPP requirements by considering how the information is captured, for example “by a member of an agency’s staff writing down what a person says versus giving someone a paper or online form to fill out”.
Principle 5: Storage and security of personal information An agency holding personal information must ensure there are reasonable safeguards against loss, misuse or disclosure, and that if it's necessary to give information to another person, such as someone working on contract, everything reasonable is done to prevent unauthorised use or unauthorised disclosure. **Addressed in which Guideline(s)** • Purpose Matters Guideline (when considering potential information	The Guidelines do not contain good practice guidance going beyond, or extending, IPP5 requirements. However, the Kaitiakitanga Principle does recognise that, as a kaitiaki, agencies need to protect people’s stories and information and keep them safe and secure.

Information privacy principle – addressed in which DPUP Guideline(s)	Where and how Guidelines' good practice guidance goes beyond the IPP requirements
access problems if different kinds of personal information are being collected through a single channel or repository) • Transparency and Choice Guideline (in the context of making people aware of additional matters beyond those in IPP3).	
Principle 6: Access to personal information When someone's personal information can be accessed or found readily, that person is entitled to know information is held about them and to have access to it. When a person is given access to their information, the agency holding it must advise the person they have the right to request corrections to their information. An agency may refuse to disclose personal information if a ground set out in Part 4 of the Act applies. **Addressed in which Guideline** • Access to Information Guideline	The Guideline goes beyond the IPP6 requirements in the following areas: • Informing and reminding people of access and correction rights: explains why it can be important to inform and remind people of their access and correction rights. • Recording people's information: provides guidance on the importance, when recording information about people, to ensure it is accurate, clear and well-written. • Helping people ask: provides guidance on helping people to ask for their information more than simply informing people of their right to access and request correction of their personal information as required by IPP3. • Making it easy: provides guidance on making it easy to access and request corrections of people's personal information. • Acting as agent or representative: provides guidance on acting as an agent or representative for a service user in relation to Privacy Act requests.
Principle 7: Correction of personal information Everyone is entitled to request corrections to their personal information. If denied and corrections are not made, they can ask for a statement to be placed with the information saying what they wanted correcting. If agencies have already passed on personal information that is later corrected, they should tell the recipients about the correction. **Addressed in which Guideline** • Access to Information Guideline	This Guideline goes beyond the IPP requirements in IPP6. Access and correction are often treated together.
Principle 8: Accuracy of personal information to be checked before use An agency must not use or disclose personal information without taking reasonable steps to check it is accurate,	The Guidelines go beyond the IPP8 requirements in the following areas: • Helping people access and request correction can help agencies with IPP8: the Transparency and Choice Guideline notes that: "Helping service users to have a good understanding of what's being collected and the purposes of collection, while proactively providing them with means to

Information privacy principle – addressed in which DPUP Guideline(s)	Where and how Guidelines' good practice guidance goes beyond the IPP requirements
complete, relevant, up to date, and not misleading. **Addressed in which Guideline** • Transparency and Choice Guideline • Sharing Value Guideline	access and request correction of their information (or to correct it themselves), can help agencies meet their own obligations under IPP8. Service users may be more likely to request corrections of their personal information (or, if possible, update it themselves) if they think it's inaccurate or incomplete." Consulting people with experience on matters relevant to information quality and context: the Sharing Value Guideline recommends that people with relevant experience are consulted to ensure that knowledge on such things as the availability and quality of information, what is involved in collecting the information, and cultural context informs the collection and use of the information.
Principle 9: Personal information not to be kept for longer than necessary An agency holding personal information must not keep it for longer than needed for the information's lawful purpose.	This is not addressed in DPUP. There is no guidance beyond IPP9.
Principle 10: Limits on use of personal information An agency that holds personal information obtained in connection with one purpose must not use the information for another purpose, unless an exception applies. **Addressed in which Guidelines** • Purpose Matters Guideline (when discussing the purpose of collecting information and how it's going to be used)	The Guideline does not go beyond the IPP10 requirements.
Principle 11: Limits on disclosure of personal information An agency must not disclose personal information it holds if one of the listed exceptions applies. **Addressed in which Guideline(s)** • Purpose Matters Guideline (about being clear about purpose and sharing, and statutory overrides of IPP11)	The Guideline does not go beyond the IPP11 requirements. For general recognition in the Guidelines that specific statutory provisions can override certain IPPs, see 'How the Guidelines recognise the IPPS can be modified or overridden by other laws' below. Such provisions can override IPP11 as well.
Principle 12: Disclosure of personal information outside New Zealand IPP12 regulates the disclosure of personal information outside New Zealand. It seeks to ensure that, when information is disclosed offshore, there are comparable safeguards to those in	There is no guidance beyond IPP12.

Information privacy principle – addressed in which DPUP Guideline(s)	Where and how Guidelines' good practice guidance goes beyond the IPP requirements
the Privacy Act 2020. In essence, an agency can only disclose personal information to a foreign person or entity (that is, overseas), in reliance on certain listed IPP11 exceptions, if one of a number of conditions is satisfied. **Addressed in which Guideline** Purpose Matters Guideline ("If it will be shared with an agency overseas, the collecting agency needs to assess if sharing would be consistent with IPP12 — Disclosure of personal information outside New Zealand")	
Principle 13: Unique identifiers Unique identifiers (UIs) — such as IRD numbers and passport numbers — must not be assigned to individuals unless necessary for the agency to carry out its functions efficiently. UIs must be unique to each individual, except in some tax-related circumstances or for statistical or research purposes. The Privacy Commissioner states, "Principle 13 states that an organisation can only use unique identifiers when it is necessary. An organisation cannot assign a unique identifier to a person if that unique identifier has already been given to that person by another organisation. Organisations must take reasonable steps to protect unique identifiers from misuse. Unique identifiers are individual numbers, references, or other forms of identification allocated to people by organisations, such as driver's licence numbers, passport numbers, or IRD numbers." **Addressed in which Guideline** • This is not addressed in DPUP. UIs are referred to in the Purpose Matters Guideline but there is no reference to IPP13 itself.	The DPUP Guidelines do not contain good practice guidance that goes beyond the IPP13 requirements, other than a statement in the Purpose Matters Guideline that, "if the information you're collecting includes unique identifiers like a driver licence number, IRD number or passport number, you might want to tell people their number will not be used to match information you have about them with information another agency has about them".

The Privacy Act 2020 introduces, among other things, a new mandatory privacy breach notification regime, and a new compliance notice regime. Privacy breach notification is addressed briefly in DPUP's Kaitiakitanga Principle. Compliance notices are mentioned in the Purpose Matters and Transparency and Choice Guidelines.

Table 2: How DPUP Guidelines recognise that the IPPs can be modified or overridden by other laws

Statutory overrides of IPPs – addressed in which DPUP Guideline(s)	Key examples of statutory overrides and other applicable government guidance
The Privacy Act 2020's IPPs can be modified or overridden by: • other Acts of Parliament • legislative instruments, whether under the Privacy Act 2020 (such as an Approved Information Sharing Agreement under Part 7 of the Act) or other legislation • Codes of Practice under section 32 of the Privacy Act 2020 (such as the Health Information Privacy Code). (see sections 24 (Relationships between IPPs and other New Zealand law) and 38 (Effect of codes of practice) of the Privacy Act 2020). **Addressed in which Guideline(s)** Purpose Matters Guideline (where key concepts are listed, including: • clarity of purpose is required regardless of legal basis for correction • recognising that specific powers can override IPP2 • personal information can only be used for purpose of collection unless other uses permitted by law • purpose is still relevant when an alternative use appears to be authorised by a specific statutory provision • purpose is still relevant when disclosure appears to be authorised by a specific statutory provision) Transparency and Choice Guideline (where it recognises that sometimes people can be given no choice about providing information, that is, where a specific provision requires it)	These are some of the Acts and legislation that include various provisions that override certain IPPs: • Accident Compensation Act 2001 • Births, Deaths, Marriages, and Relationships Registration Act 1995 • Family Violence Act 2018 • Health Act 1956 • Kāinga Ora — Homes and Communities Act 2019 • Mental Health (Compulsory Assessment and Treatment) Act 1992 • Oranga Tamariki Act 1989 • Privacy (Information Sharing Agreement between Ministry of Social Development and New Zealand Customs Service) Order 2019 • Privacy (Information Sharing Agreement for Improving Public Services for At-risk Children) Order 2015 • Social Security Act 2018 • Substance Addiction (Compulsory Assessment and Treatment) Act 2017. For guidance on the: • Oranga Tamariki Act information sharing provisions, see orangatamariki.govt.nz/working-with-children/information-sharing/ • Family Violence Act information sharing provisions, see justice.govt.nz/justice-sector-policy/key-initiatives/reducing-family-and-sexual-violence/a-new-family-violence-act/information-sharing-guidance/

Table 3: Guidance beyond the scope of the Privacy Act

Areas where the DPUP Guidelines are beyond the scope of the Privacy Act	
Sharing Value Guideline	Provides guidance on developing and sharing the value of information and insights in an inclusive, useful, respectful and valuable way with those interested, for example, service users, frontline staff, funding partners and the community. It has a particular focus on sharing non-personal information, which does not identify and is not capable of identifying people.