Insurance Council of New Zealand
40 Bowen Street
Pipitea, Wellington
6011
Email: icnz@icnz.org.nz
Website: www.icnz.org.nz

25 June 2025

Capability & Guidance Team
Office of the Privacy Commissioner

IPP3A@privacy.org.nz

ICNZ SUBMISSION ON THE DRAFT GUIDANCE ON IPP3A

Thank you for the opportunity to provide comments on the Office of the Privacy Commissioner's (**OPC**) Draft Guidance on Information Privacy Principle 3A (**IPP3A**).

Te Kāhui Inihua o Aotearoa | The Insurance Council of New Zealand (**ICNZ**) represents general insurers. Our members accept the risks of over NZ$2 trillion of New Zealand's assets and liabilities. ICNZ's members provide insurance products ranging from those usually purchased by individuals (such as home and contents insurance, travel insurance, and motor vehicle insurance) to those purchased by small businesses and larger organisations (such as product and public liability insurance, professional indemnity insurance, cyber insurance, commercial property insurance, and directors and officers insurance).

ICNZ has the following feedback on the questions raised in the OPC's consultation.

1. Is the Guidance Fit for Purpose? If not, how could it be improved?

The draft Guidance and the examples provided are a good starting point. However, in its current form we consider that the Guidance does not address significant operational challenges that IPP3A will present to general insurers. While the intent of enhancing transparency is welcomed, the Guidance does not sufficiently account for the range of indirect collection in the insurance industry which is required to facilitate the efficient and timely processing of policies and claims. ICNZ members seek clarification on key aspects of IPP3A through the Guidance to support implementation and compliance. Greater certainty through guidance will help mitigate insurers' compliance costs which will ultimately benefit customers.

As the IPP3A is proposed to come into force on 1 May 2026, it is important that insurers have a clear understanding of their obligations so that they can implement the required changes to their systems and processes effectively and within the relatively short timeframe.

ICNZ would like to meet with you to discuss our submission further and to explain the insurance industry and the practical issues we will face if the Guidance does not provide further clarity.

Reasonable steps

IPP3A provides that the collecting agency must take any steps that are, in the circumstances, reasonable to notify the individual of certain matters when the agency collects information about the individual indirectly. The OPC has acknowledged that it has not provided guidance on what constitutes "reasonable steps". We note that what might be considered reasonable in the circumstances may be open to interpretation and many different factors may be taken into account when making this assessment. In some circumstances an agency may determine that it is reasonable to take no steps to notify individuals. It would be useful to have guidance on what factors should be taken into account when assessing what is "reasonable" in the circumstances and when not taking any steps might be acceptable. Additional practical examples in the Guidance for large organisations that provide scalable and proportionate solutions for notification would be useful.

2. **Are there any parts of the guidance that need more clarification, or are hard to understand?**

Notification steps – Reference to multiple entities

It is inappropriate and impractical to require an insurer to specifically and individually provide the name (and address) of the entities where information may be collected from or transferred to (e.g. brokers, repairers, tow companies, suppliers and subcontractors, plumbers, assessors and investigators, reinsurers etc). Most agencies use a Privacy Policy to communicate to the public how they collect, use and share personal information and to satisfy the notification obligations under the Privacy Act:

Requiring the name and address of individual third parties in a Privacy Policy may:

- Be impractical due to the volume and dynamic nature of these relationships – also noting in major events that insurers need to act quickly and often require an expanded list of agents and suppliers;
- Create an unmanageable administrative burden and workable notification fatigue;
- Disclose commercially sensitive information;
- Contradict international privacy practices (e.g., Office of the Australian Information Commissioner, UK Information Commissioner's Office), which support the use of class-based descriptions.

We therefore do not support the current approach set out in the Guidance that individual third parties must be named.[1]

[1] Page 8 of the Guidance: *"It's not enough to say the type or class of agency, such as we may share your information with a reporting agency".* Page 11: *"If the disclosing agency is going to be responsible for the notification requirements, they will need to be specific about who is indirectly collecting the personal information. It's not enough to say, 'we may share your information with a credit reporting agency'".*

The Guidance should be amended to make clear that referencing classes of third parties (e.g., "insurance brokers" or "claims service providers") can be adequate, i.e. reasonable in the circumstances, particularly if the information is not sensitive and individuals are offered the option to request more specific information if desired.

We note the Australian Information Commissioner has taken a sensible approach to their guidance where an "entity collects information from a wide variety of entities and it would not be practicable to give a separate notice in relation to each entity, the APP entity should instead indicate the kinds of entities from which it collects information"[2]

We recommend the following text on page 11 of the Guidance should be amended as indicated:

> "If the disclosing agency is going to be responsible for the notification requirements, they will need to be specific as possible about who is indirectly collecting the personal information. ~~It's not enough to say, "we may share your information with a credit reporting agency".~~ However, if you know that in certain situations you will always share information with specific agencies, you could tell individuals the circumstances in which you would always send to these agencies. Using categories of organisations may be appropriate if the agency is as specific as possible about the categories."

Similar amendments should be made to 'The intended recipients of the information' section on page 8 of the Guidance.

We would also like to see scenarios in the Guidance that provide a practical approach for insurers and similar large organisations that collect information from many sources.

Evidencing notification by the collecting agency

The Guidance implies on page 11 that an entity must ensure notification has occurred on a case-by-case basis when personal information is collected by third parties:

> "The collecting agency should still ensure it has reasonable grounds to believe that the disclosing agency is informing individuals as required. This could be achieved by receiving and *filing a copy of a form signed by an individual* or through regular contract reporting requirements." (emphasis added).

This is unnecessary and may extend beyond an entity's reasonable control and accountability.

Collecting agencies should be responsible for demonstrating how they meet their IPP3A obligations, including maintaining appropriate processes and controls. Contractual arrangements and conducting periodic (e.g. annual) reviews / attestations to confirm these

---

[2] Australian Privacy Principles guidelines, Chapter 5: APP 5 Notification of the collection of personal information, para 5.1 https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information

obligations are being met should be adequate to meet the expectations, rather than evidence of communication in every individual case.

We recommend that the Guidance is amended as follows:

> "This could be achieved via ~~by receiving and filing a copy of a form signed by an individual, or through regular~~ contractual arrangements and associated oversight or reporting requirements~~,~~ such as annual attestations."

Notification of the agency that is holding the information

We note IPP3A(1) sets out the matters that the collecting agency should notify an individual of when the individual's information is collected indirectly. IPP3A(1)(d) requires the collecting agency to notify the individual of the name and address of the agency that has collected the information and the name and address of the agency that is that is holding the information. We would welcome clarification of what is intended to be covered by the "agency that is holding the information". Our interpretation is that the collecting agency is not required to notify the name and address of the agency that was the original source of the information. We would welcome guidance confirming this.

Individual has already been made aware

The Ministry of Justice's Departmental Report on the Privacy Amendment Bill[3] stated (pp 13–14):

> "If personal information is routinely passed on to another agency, and the individual has been made aware of the agency's identity in a recent notice relating to a similar collection, it is not necessary to notify again".

The report also indicated that the OPC would provide confirmation of this approach in the Guidance. It would be helpful for the Guidance to provide further examples that include this scenario.

It is common for insurance policies to be held in joint names, in a business name or trust and/or for individuals to appoint a nominated representative to act on their behalf. Often an insurer will only issue their Privacy Policy to the main person insured, e.g. it is delivered to one email address and the insurer expects that other individuals have been, or will be made aware, of the Privacy Policy terms. In the OPC's recent webinar it was indicated that this approach was acceptable given the contract is set up so all parties can act jointly and information being told to one is treated as being told to both. It would be helpful if this could be documented in the Guidance.

[3] Ministry of Justice, Departmental Report for the Justice Committee, Privacy Amendment Bill, August 2024 https://www.parliament.nz/resource/en-NZ/54SCJUST_ADV_56e3fbe7-1f3d-464e-b54d-08dbae8917ae_JUST25117/486e13dffec774048ebebef3ee37e3d94a81307e

Non-compliance will not prejudice the interests of the individual

The collecting agency is not required to notify the individual where non-compliance would not prejudice the interests of the individual concerned (IPP3A(4)(a)).

The Guidance suggests this exception applies to low-risk situations, with a "no surprises" test which is helpful and illustrated by the emergency contact example. Other examples that could be included in the Guidance that would rely on this exception are powers of attorney, executors, trustees, or authorised representatives.

In the general insurance industry policies are often obtained by one person who provides information about other individuals, such as other policyholders, insured parties or named drivers on the policy. We expect that these individuals are aware their information has been collected by the insurer and that non-compliance would not prejudice their interests, allowing insurers to rely on this exemption. This would be a further relevant example to include in the Guidance.

Example Two 'City Property Management' on page 14 of the Guidance is unhelpful as it implies that agencies cannot rely on the exception "no prejudice to the interests of the individual concerned" when appointing contractors to assist their customers and/or customers' tenants. We consider that the "no surprises" test and the application of common sense would mean that this exception should apply in the context of insurance claims, where the tenant will have generally raised an issue with the landlord, who then lodges a claim and provides the tenant's contact details to enable an assessor and/or repairer to make contact to assess the issue and effect repairs.

It would also be beneficial for many sectors if the Guidance could include an example involving a vulnerable customer. There are sometimes circumstances where insurers and other providers, such as banks and energy companies, are informed about an individual's vulnerability by a third party for the purposes of providing that individual with an additional level of support in the future e.g. when advised indirectly of factors such as hearing impairments, mobility or cognitive issues, no ability to access email etc. We see this as a good example where non-compliance would not prejudice the interests of the individual as the service provider would be acting in their best interest. Guidance on this would be appreciated, noting that the information collected is often sensitive in nature and will in many cases be unsolicited, so often not within the Privacy Act definition of "collect".

In some instances, insurers will indirectly collect information about an individual but not need to contact that individual again. For example, a policyholder provides details of their neighbour who they suspect caused damage to their property but there is no proof, to the insurer does not intend to contact the neighbour or pursue recovery. Guidance would be helpful to establish if the insurer is still required to notify the neighbour that their information was indirectly collected and why, even if there is no other reason to contact them.

The Guidance states that "The collection may be for the benefit of the individual, but this doesn't mean you shouldn't tell them about it". This makes it difficult to interpret when this exception should apply and so we consider this should be revised.

Telling the individual would prejudice the purposes of the collection

The internal fraud investigation example on page 14 of the Guidance is helpful and we expect further examples relevant to sectors such as insurance can be provided here that would strengthen understanding. We suggest including cases involving insurance fraud investigations where notification of indirect collection may undermine the investigation.

Telling the individual is not reasonably practicable in the circumstances

IPP3A(4)(e) provides:

(4) It is not necessary for an agency to comply with subclause (1) if the agency believes, on reasonable grounds,—

(e) that compliance is not reasonably practicable in the circumstances of the particular case;

The Guidance uses the phrase "not reasonably *practical*" (emphasis added). The Guidance should be amended to reflect the statutory language and the use of "practicable".

Large agencies, like insurers, will need to adopt a systemic approach to complying with their IPP3A obligations. It would be helpful for the OPC to provide further guidance on what might be considered "reasonably practicable" when notifications are considered on a use case basis. We note the Ministry of Justice's Departmental Report on the Privacy Amendment Bill stated (at para 34):

> "Where the transfer of similar personal information is routine, it is intended that agencies will be able to make an assessment about whether notification is reasonable on a use-case by use-case assessment rather than strict case-by-case assessment. Business rules or policy directives (for public sector agencies) can be used to set up the criteria and parameters for sharing so that approaches for particular classes of information can be streamlined."

Duration of exceptions

The Guidance suggests that notification may be required at the conclusion of an activity where an exception was previously relied upon (pages 26 and 27). While this will be valid in some situations, in scenarios such as litigation or fraud investigations, this could expose whistleblowers to potential health and safety issues (psychological and/or physical – possibly covered by the 4(h)(ii) exception) or compromise sensitive processes.

The Guidance should clarify that notification is not required (at any time) where the basis for the exception is ongoing, for example where it would prejudice the willingness of future whistleblowers to come forward or create a risk of harm, particularly in sensitive or high-risk scenarios, such as following an investigation involving fraud.

The Guidance should therefore include another example that shows where an exception would be ongoing, perhaps an example where disclosure would create a health a safety risk for another individual or where the risk would be difficult to assess.

Trusted Insurance Co and Mater's Motors example on page 4

We appreciate the inclusion of insurance specific examples but we do not consider the example accurately reflects practice. Typically, when an insurer interacts with the repairer it is the insurer's customer's vehicle, so the insurer would already know their name and contact details etc, – so it is only really details of the loss that the repairer would be sharing with the insurers – e.g. which elements of damage to the vehicle related to the accident being claimed for vs pre-existing damage, wear and tear etc. Further, the relationship between the insurer and their customer will be subject to a Privacy Policy. For third parties, the insurer would typically be dealing with the third party's repairer.

In addition, to provide detailed disclosure in this scenario would create a significant administrative and cost burden and does not increase transparency for individuals, who would reasonably expect their information to be disclosed for the purposes of completing their claim.

3. **Are there more key terms we need to define or concepts that need more clarity?**

Please see our responses to questions 1 and 2 above.

4. **Are the examples provided meaningful to you? If not, what kinds of examples would you want to see instead?**

The Swiftstart NZ example involves an agency that does not collect and use the information for its own purposes and is not obliged to notify as it holds information on behalf of its client. The expectation that a cloud-based provider would impose standard disclosure wording and contractual clauses on its clients is not practical and does not appear to be a requirement under IPP3A. A large company with a high volume of third-party suppliers of this nature could not include bespoke disclosures for each in its Privacy Policy or directly to their customers. This example requires reconsideration.

5. **Any other relevant feedback or comment**

Insurers rely on being able to indirectly collect information to ensure only valid claims are paid. It is important that information can be provided freely and without consequences to insurers. Practical guidance would be helpful assist insurers to balance the need to be able to indirectly collect information with the privacy rights of the individuals providing the information. For example, a policyholder is unlikely to provide information about a person suspected of property damage or arson if the policyholder knows that the suspect may later be informed that the policyholder provided the suspect's information to the insurer once the investigation is complete.

We welcome clarity on the issues raised above to ensure the insurance industry can apply new IPP3A correctly. Such clarity will help insurers mitigate their compliance costs which will ultimately benefit consumers and will assist insurers to implement their new obligations within a relatively short timeframe (1 May 2026).

As noted above, ICNZ would like to meet with you to discuss our submission further.

Ngā mihi,

Susan Ivory
Regulatory Affairs Manager
Insurance Council of New Zealand