New Zealand Banking Association
Te Rangapū Pēke

Submission

to the

Office of the Privacy Commissioner – Te Mana Mātāpono Matatapu

on the

Draft guidance on IPP3A

25 June 2025

NEW ZEALAND BANKING ASSOCIATION – TE RANGAPŪ PĒKE
PO Box 3043, Wellington 6140, New Zealand
www.nzba.org.nz

About NZBA

1. The New Zealand Banking Association – Te Rangapū Pēke (**NZBA**) is the voice of the banking industry. We work with our member banks on non-competitive issues to tell the industry's story and develop and promote policy outcomes that deliver for New Zealanders.

2. The following seventeen registered banks in New Zealand are members of NZBA:

- ANZ Bank New Zealand Limited
- ASB Bank Limited
- Bank of China (NZ) Limited
- Bank of New Zealand
- China Construction Bank (New Zealand) Limited
- Citibank N.A.
- The Co-operative Bank Limited
- Heartland Bank Limited
- The Hongkong and Shanghai Banking Corporation Limited
- Industrial and Commercial Bank of China (New Zealand) Limited
- JPMorgan Chase Bank N.A.
- KB Kookmin Bank Auckland Branch
- Kiwibank Limited
- Rabobank New Zealand Limited
- SBS Bank
- TSB Bank Limited
- Westpac New Zealand Limited

Contact details

3. If you would like to discuss any aspect of this submission, please contact:

Antony Buick-Constable
Deputy Chief Executive & General Counsel
antony.buick-constable@nzba.org.nz

Sam Schuyt
Policy Director & Legal Counsel
sam.schuyt@nzba.org.nz

Introduction

4. NZBA welcomes the opportunity to provide feedback to the Office of the Privacy Commissioner – Te Mana Mātāpono Matatapu (**OPC**) on the draft guidance on IPP3A (**Guidance**). NZBA commends the work that has gone into developing the Guidance.

5. We appreciate the OPC taking proactive steps to assist organisations with compliance, and for seeking feedback from the public on its interpretation.

6. Overall, NZBA is supportive of having the Guidance in place to support compliance with IPP3A legislative requirements. However, we consider that:

    6.1. The Guidance's interpretation of the requirements of IPP3A would make its application impractical and would overburden customers with information;

    6.2. The Guidance goes beyond what is required under the Privacy Act 2020 (**Act**), with a notably higher standard imported for indirect collection than direct collection (see further below, including at Appendix A our comparison of the disclosure expectations for IPP3 versus the IPP3A Guidance);

    6.3. The Guidance sets a standard that is significantly higher than international standards which, in its current form, would create a significant hurdle for compliance for all organisations looking to operate in New Zealand;

    6.4. The Guidance's interpretation of the scope of IPP3A(3) and the other exceptions is not practicable or pragmatic in its current form; and

    6.5. There are a number of parts of the Guidance that, in our view, would benefit from greater clarity or refinement.

7. We are also concerned that the Guidance as currently drafted could undermine the Government's intended path for innovation and growth, including open banking. The Minister of Commerce and Consumer Affairs has repeatedly emphasised the need to remove blockers for growth, including creating modern fit for purpose regulation that enables innovation and enhances competition. We are concerned that the approach taken to IPP3A in the Guidance will create a regulatory burden on both financial services participants and their customers, similar in nature to issues experienced in relation to the Credit Contracts and Consumer Finance Act.

8. We have identified below a number of aspects of the Guidance that would benefit from amendments to enable the practical implementation of IPP3A in a way that is suitable and proportionate for both organisations and individuals. In addition, we would welcome the opportunity to engage further with the OPC to consider how to address matters which may not be resolved through the final Guidance, including through consideration of a new Code of Practice.

Is the guidance fit for purpose? If not, how could it be improved?

Guidance's interpretation of IPP3A(1) would make its application impractical

9. The Guidance interprets the requirement to notify the customer of the "intended recipients" of the indirect collection as being a requirement to provide the specific name of every intended recipient (as opposed to providing information regarding the type or class of intended recipients).

10. This interpretation would make the application of the Bill impractical and unpragmatic and would risk overburdening customers with information. For context, indirect collection is very common in the banking industry. Examples include:

- Information provided by a joint account holder about another joint account holder e.g. co-borrowers
- Customer information provided by agents / authorised signatories / solicitors / parents / guardians / guarantors, etc
- Customer information provided by external financial advisers (distributors) / solicitors / custodians / mortgage advisers / valuation agencies
- Instances where a potential customer's details are provided to a bank from a mortgage broker / financial advisers
- Instances where we provide customer information to organisations we work with such as insurance partners/card partners
- When we receive credit ratings from the credit bureaus, such as Equifax
- Identification checking, for example, confirmation of a customer's passport details or driver licence details from the New Zealand Transport Authority and Department of Internal Affairs through Centrix or other DIA Confirmation Service partners.
- When we receive payroll deduction information from the Inland Revenue
- Information provided by the Police regarding information requests or financial crimes
- Job applicant information including references from a recruitment agent
- Criminal record check information from the Ministry of Justice
- Customer complaint details shared by any financial dispute resolution schemes
- Customer details provided by other banks for fraud, payments and transaction processing purposes, such as Anti-Scam Centre data sharing
- Cookies collection, for example, third party web platform provider informs us of internet preferences.

11. These types of examples would likely apply similarly to other types of financial services businesses, including insurance companies and mortgage brokers / financial advisers.

12. Large organisations sit on both sides of this activity: they act not just as the collecting agency, but also as the disclosing agency. There are countless examples where a bank chooses to, or is required to, disclose a customer's personal information to a third party, many of them included in the list above (e.g. banks will share information to and from agents, brokers, other account holders, credit agencies, government departments etc). As a result, it is important we are cognisant of the impact of this law change both from a disclosure and a collection perspective.

13. Banks' privacy policies and/or statements set out examples of where they can collect personal information from, or disclose information to, third parties. Therefore, banks already take steps to inform their customers of indirect collection from other agencies and who they disclose information to.

14. To illustrate the impact the new IPP3A might have in a common scenario, and where it could happen via multiple routes in parallel, consider how it could apply where a couple is interested in obtaining a home loan:

    14.1. The couple opts to use a mortgage adviser. The adviser might approach that couple's current bank and three alternative banks for loan options. The adviser provides information relating to those individuals to the four banks.

    14.2. The adviser and/or the banks, in turn, might also collect relevant information from a credit agency, the individual's current bank, the IRD, a valuer and the joint account owner.

    14.3. The couple's solicitor is then later in contact with the bank separately to arrange for loan documents to be reviewed.

15. Under the draft Guidance, it is unclear how IPP3A is intended to apply to this situation. The couple will likely be aware of the information exchange as a result of discussions with their mortgage adviser. As a result:

    15.1. Receiving notification from each bank confirming the receipt of information from the adviser seems unnecessary. We consider the banks should be able to rely upon the authorisation and / or prior notification by the advisor and apply one of the IPP3A(3), (4)(a) or (e) exceptions to not provide direct notification.

    15.2. Further information has been collected from other sources. This has presumably occurred with authorisation from the applicants who require this information application to be assessed. Again, the banks should be able to rely upon the authorisation and/or prior notification by the advisor and apply IPP3A(3), (4)(a) or (e) (see our submissions below at paragraphs 30-36).

15.3. If the above exceptions cannot be relied on, each bank will need to provide notification to both applicants that they have collected information from the other sources such as credit agencies, other banks, the IRD, the other loan applicant involved, etc. On the basis of the draft Guidance, this could not be achieved by a standard form disclosure, but would require specificity as to the relevant credit agency, the other applicant's details, etc. This will create a significant compliance burden.

15.4. Only the bank that eventually advances a loan will provide its full terms and conditions (accompanied by its privacy policy / statement). It is unclear under the Guidance whether the belated notification would be sufficient, and whether this would be considered "as soon as reasonably practicable".

15.5. When the loan is being processed, banks often ask the customer who their solicitor is, and then send that solicitor all of the loan and security documents to act on both the bank's and the customer's behalf. Again, the bank should be entitled to presume authorisation and/or notification has occurred as part of the lawyer / client relationship. The banking industry has dealings with thousands of law firms annually, so it is not practical to have disclosure dealt with via contractual terms.

16. This example gives some indication of the large number of notifications that might be generated in practice from a relatively simple transaction, and the issues that arise from any business activity done at scale. It also illustrates the potential of negative customer experiences associated with those notifications when the customers would already be confronted with a lot of paperwork. Banks can enter hundreds of home loans per day. This is one small example within the framework of the bank's functions.

17. We do not consider an outcome of notification for this indirect collection by the collecting agency a sensible one – and so, as expanded upon below, the ability to practically rely upon the exceptions, through clear and practical explanations and examples in the Guidance, becomes critical.

18. The approach taken in the Guidance that an agency should provide specific information for each of these notifications also potentially imposes a risk on the discloser or collector to maintain personalised, living documents of all sources, uses and contact details for individuals. This would be a significant undertaking which could create unfeasible and inefficient resourcing demands on entities. In the scenario described above, we consider the individual involved would already expect the information sharing to be taking place.

19. We consider that the costs involved, if such a register was considered a way to comply, would not be proportionate to the benefit such specificity would provide. The highly specific information sought in the Guidance (e.g. specific names and addresses of agencies) also risks individuals not engaging with notification:

19.1. The specific information is likely to become redundant more quickly than less specific information, leading to additional notices and potentially notification fatigue; and

19.2. The level of detail required in the notice increases the risk that individuals may not engage with it, particularly when they are receiving several notifications at the same time.

20. The Guidance's approach to specificity is inherently problematic for banks, which typically include details of indirect collection and disclosures in bank privacy policies and statements but do not include information regarding the specific entities to which indirect collection and disclosures are made. Banks connect daily with a vast number of third-party information sharing services. As drafted, the Guidance would require extensive notification lists and frequent updates to individual notifications as third-party information sharing relationships change. In practice this is not workable for either a disclosing / collecting agency, or individuals who may suffer from notification fatigue.

Guidance goes beyond what is required under the Privacy Act 2020

21. We have concerns that the Guidance suggests a more demanding interpretation of IPP3A (indirect collection) compared to IPP3 (direct collection) which, in our view, goes too far and is out of step with the intent of the legislation.

22. We have set out at Appendix A a comparison of IPP3A requirements as interpreted by the draft Guidance against understood disclosure requirements under IPP3 to illustrate the significantly higher standards proposed by the Guidance, despite the relevant wording in IPP3 and IPP3A being similar.

23. We submit that OPC should refine the draft Guidance to correct this apparent inconsistency to align with the interpretation of IPP3 where relevant.

Guidance sets a standard that is significantly higher than international standards and usual contractual terms

24. The Guidance's interpretation of the scope of the exceptions is inconsistent with international practice in the European Union and Australia and requires further consideration. For example:

24.1. There are exceptions under Australia's Privacy Principle 5 for third party collection of information in certain instances, including that agencies have flexibility and are only required to "disclose such matters as are reasonable in the circumstances" and that in some cases it is, therefore, not necessary to ensure awareness of the APP5 matters. This provides organisations with the flexibility to notify about the "types of any other ... entities, bodies or persons, to which the … entity usually discloses" to, i.e. there is no requirement to provide details such as names of each third party.

24.2. Article 14 of the GDPR requirements allow recipient names or “categories of recipients” to be given. Again, there is no requirement to provide details such as names of each third party and providing high level information is satisfactory.

25. Further, in our view the Guidance’s proposed standard for relying on the exception that an “individual has already been made aware” is high and incompatible with usual contractual terms.

25.1. Under the draft Guidance, notification requirements documented in contractual terms are not sufficient to meet 'reasonable grounds' for reliance. Proposed solutions such as sharing and filing signed documents do not appear to align with principles of minimal data collection and dissemination. We would welcome clarification that verification is not legally required (albeit helpful in evidencing compliance), and an expansion to other alternative modes of verification.

25.2. The need for “good evidence” on an individual rather than group basis is too high a bar.

26. The Guidance suggests that this type of notification requirement might be included as part of the contractual arrangements between the disclosing and collecting agencies. This could involve a substantial amendment of all contractual arrangements, which – for larger organisations in particular – could be time and cost intensive.

27. From the perspective of a disclosing agency, a bank would need to maintain a list of all the names and addresses of entities it discloses to. This would be both administratively difficult to manage, and risk disclosing confidential commercial arrangements while providing minimal benefit from a customer perspective.

28. An alternative would be for the OPC to confirm that banks may rely on the current exception in IPP3 which states it is not necessary for an agency to comply if the agency believes, on reasonable grounds that non-compliance would not prejudice the interests of the individual concerned. It would be preferable for the Guidance to include an express confirmation that this exception can be used and relied upon when the other entity has already been notified. Please see our discussion below in this regard.

29. We would welcome the opportunity to engage with the OPC on other alternative solutions for this issue which both promotes privacy, and does not overload individuals with notifications – for example, a Code of Practice may be an appropriate mechanism to ensure the right balance is struck.

Guidance’s interpretation of the scope of IPP3A(3) makes its application impracticable for large organisations like banks

30. We understand that the new IPP3A will provide for a number of practical legislative exceptions to ensure the efficient administration of certain public functions, and to protect against other unintended consequences. However, the exceptions are, in our view, too narrowly interpreted in the Guidance and do not sufficiently address the practical implications of the new principle.

31. Banks rely on the large-scale sharing of information to offer and provide their products and services. This will only increase with the impending designation of banks under the Customer and Product Data Act and the general shift towards 'open banking'. Having appropriate exemptions from IPP3A will be critical to delivering financial services effectively and efficiently, while supporting innovation.

32. Exception IPP3A(3) permits an organisation to not notify for indirect collection where the individual has already been made aware of the prescribed information. The example provided in the Privacy Amendment Bill is somewhat unclear, but one interpretation is that it would suffice, as long as the disclosing agency had previously notified the individual of information regarding the collection needed under IPP3.

33. However, the Guidance suggests this prescribed information needs to include the specific name of the collecting agency, rather than a general description.

Guidance's interpretation of the scope of IPP3A(4)(a) is too narrow

34. IPP3A(4)(a) provides that an agency need not undertake indirect collection notification if the collecting agency believes on reasonable grounds that to not do so would not prejudice the interests of the individual concerned. The indication in the Guidance is that this exception is for common, low risk cases.

35. The example given is emergency contact information. We agree that this is not a situation where indirect notification needs to be given. It would be helpful if the Guidance elaborated on what an agency might consider when determining whether collection is low risk.

    35.1. For example, if there are reasonable grounds for an entity to believe that someone is acting as an individual agent or representative (e.g. in the case of a solicitor), we consider it reasonable for an agency to assume that collection "would not prejudice the interests of the individual concerned". Another example is where a dispute resolution scheme contacts a bank and shares information about a complaint with them. It would not be pragmatic for the bank to notify the individual that information is being shared with the bank. A member of that dispute scheme should be able to engage in a complaint. This would not prejudice the interests of the individual concerned.

    35.2. We think these examples fall within the Guidance's suggestion of being common scenarios, and would be instances where it would be reasonable for

parties to understand information would be shared. It would be helpful if the Guidance could more clearly reflect this.

36. Another possible scenario is that this exception could apply to those scenarios where authorisation or notification have already occurred to a degree that this exception applies (i.e. the interests of the individual concerned would not be prejudiced). We envisage this could apply to scenarios where there has been sufficient notification of third-party disclosure by the disclosing agency such that further specific indirect collection notification is not necessary. We address this in our example on fraud and scams as set out further below. It would be helpful if the Guidance included an express confirmation that this exception can be used and relied upon when the other entity has already been notified and / or authorised. It becomes particularly important in the open banking context.

White labelled products

37. Banks sometimes provide financial products that are 'white labelled' through intermediaries and retailers where, as agreed in contract between those parties, the bank is not visible to the end customer. One interpretation of IPP3A is that it is reasonable to break the confidentiality of those arrangements by requiring disclosure of the indirect collection of personal information to the customer. If this interpretation is correct, it would have a significant adverse impact on the legitimate commercial interests of many businesses.

38. For context, the white labelling of products and services is not specific to banking, it is also common in sectors such as the energy and telecommunications sectors. Businesses across multiple sectors employ this approach for reasons including, to:

    38.1. access new customers a business may not otherwise attract, or are outside of their geographical reach;

    38.2. leverage reliable brands and loyalty schemes that a retailer may have in place;

    38.3. avoid the costs of developing new distribution channels, and providing customer service; and

    38.4. enhance the customer experience by, for example, embedding financial services into a retailer's website or online payment process.

39. Noting these commercial interests which we believe hold value for both consumers and businesses, it is not clear from the Guidance how IPP3A applies to white-labelled services that involve the in-direct collection of personal information. We request that the OPC:

    39.1. clarify this issue in its Guidance to provide banks and other businesses with clarity before IPP3A comes into force;

39.2. engage with the banking industry as soon as possible to help inform banks as they prepare to comply with this new law; and

39.3. clarify whether it anticipates making changes to the Credit Reporting Privacy Code 2020 as a consequence of IPP3A.

Are there any parts of the guidance that need more clarity, or are hard to understand?

40. We have listed below a number of parts of the Guidance that, in our view, would benefit from greater clarity or refinement.

Indirect Collection

41. It is not entirely clear what does and does not constitute indirect collection, and where it begins. We consider the two scenarios below would fall under the "not reasonably practicable" exception, for example.

41.1. If someone (who is not an agency) sets up an automatic payment using another person's personal details in the reference line etc, there is currently no clear exception relieving the bank of the obligation to notify the individual that their information is held. However, such notification would be impractical and in our view of no benefit. Banks can process millions of transactions every day, and implementing measures to comply with this disclosure obligation in these circumstances would not be practical.

41.2. If an individual informs a bank of concerns about their parent's health and ability to manage their banking independently, is the bank required to notify the parent that their health information has been collected via a call recording? Does this obligation change if the information is inadvertently captured (e.g. during hold music on a recorded call)? Banks may also hold information about individuals who form part of a client's family or business when carrying out credit assessments. Again, this may be an issue that could be addressed through a new Code of Practice.

Expiration of exceptions:

42. *Confidentiality & maintenance of the law exceptions:* Information collected under an expectation of confidentiality may qualify for an exception if disclosure would compromise the purpose of the collection. However, the Guidance indicates this must be reassessed over time. This raises questions regarding the longevity of such exceptions. We submit that the Guidance should include a statement to the effect that where reasonable, an exception may not expire.

42.1. For example, if authorities receive a tip-off and investigate, but ultimately finding no risk of money laundering, the original purpose for collection may no

longer apply. Disclosure to the individual however may discourage future tip-offs and expose the disclosing party to safety risks.

43. *Won't prejudice exception:* The OPC states agencies should apply a subjective 'no surprises' test, i.e. would the person be surprised that you collected their personal information? Conducting this assessment individually is impractical due to resource constraints and could also lead to unintentional discrimination.

Subjective assessments:

44. The Guidance suggests assessments should be subjective to the individual. For organisations with large customer bases and products this is infeasible with existing resources. Likewise, the requirement for continuous evaluation of exceptions is a highly manual and resource-intensive task.

Cross-border data transfer interplay (IPP12):

45. Since data may be collected overseas and transferred to New Zealand, it would be helpful to include a paragraph clarifying how IPP3A notification requirements align with IPP12 and overseas disclosure notices.

Contact detail gaps:

46. Banks often obtain beneficial-owner information indirectly but may not have contact details for that person. Further guidance on direct and indirect contact would be of assistance.

Group structures and outsourcing:

47. Many organisations operate via multiple legal entities and offshore service hubs. It is unclear whether a group-wide notification satisfies the requirement when collection and holding agencies differ. We submit that the OPC consider how the Guidance aligns with BS11 Outsourcing Policy and the Reserve Bank of New Zealand's data location expectations.

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

48. We note the IPP3A(3) example in the Privacy Amendment Bill is unclear. The example includes Agency A being the party who originally collects the information with Agency B being the agency who receives it indirectly. However, the IPP has been written in reverse – namely, that Agency B who collects information indirectly needs to comply unless there is an exception. We suggest the OPC considers clarifying this and aligning the terminology used in the Guidance for clarity and consistency.

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

49. We have set out below some comments on specific examples:

***Swiftstart example**: "any company or organisation that's contracting with Swiftstart is responsible for meeting any IPP3A requirements"*

49.1. In our view, Swiftstart would be a processor / agent in this example. As a result, we consider there is no disclosure of personal information requiring notification.

49.2. NZBA also recommends deleting the final paragraph of this example or clarifying that the actions described are potential risk management measures only.

Reach High (second example, p 7):

49.3. This example is confusing, as it does not appear to take into account that the information sharing might be authorised by the individual, and would not prejudice the individual.

Bank example (p 8)

49.4. This example makes the assumption that the financial services company is not a processor to the bank, however, each scenario might be different.

Green Gardens (first example, p 12)

49.5. Where large-scale information sharing practices are needed to run banks, a tick-box approach is not viable.

'No surprises' test (p 13)

49.6. Use of the word "consent" is unhelpful as it is not a term in the Privacy Act. We submit this should be replaced with "authorisation".

49.7. We also consider that some more large-scale bank-customer examples would be beneficial.

Out of date information (p 15-16)

49.8. This is arguably an IPP8 breach at the point of disclosure.

'[I]t wouldn't prejudice the interests of the individual concerned' (p 22)

49.9. A related example is given where we can 'reasonably presume' an individual who has provided the emergency contact details of someone else has made them aware they are their emergency contact. We can see parallels with this

example in the banking industry. For example, when an individual collects ID on behalf of staff and provides it to their bank when organising staff banking credit cards for example. Consideration should be given to providing more examples where agencies can 'reasonably presume' an individual would have been made aware that their information was being collected and shared.

49.10. A common related example of indirect collection will be where someone or an agency is acting on behalf of an individual and they are authorised to do so. For example, solicitors acting for clients, mortgage brokers / financial advisers acting for potential customers, appointed roles such as powers of attorney or other representatives. Is it intended that this scenario would fall within the new IPP3A(4)(a), i.e. that it would not prejudice the interests of the individual? If so, this should be clarified and used as an example.

Add fraud and scams example given broad ranging measures being taken

49.11. It would also be useful to include a specific example showing how information shared for the benefit of frauds and scam investigation/prevention could fall within an exemption. The sharing of information between financial institutions is critical and expected as part of the fight against fraud and scams, so noting this as an active example would assist. We presume banks can rely on IPP3A(4)(c)(i) or (d), depending on the context.

49.12. We note that it is vital to ensure banks can fully and frankly share information with other banks, and often this must take place as a matter of urgency. Accordingly, it is not desirable to be manage additional compliance burden in these circumstances.

49.13. There may also be tensions with other legislation, like AML, where information is shared between banks for fraud and scam prevention, but is done under an exemption from AML tipping off provisions. Disclosing information about who is involved in that information sharing may prejudice the terms of those exemptions and create challenges. Essentially, we believe it would be extremely beneficial to include a clear example that covers the scam and fraud information and fraud recovery processes.

Other relevant feedback

50. As currently framed, the Guidance would require significant time and resource to implement. There is already a tight timeframe for compliance (May 2026), and the Guidance appears to have a broader scope than what is captured in the incoming legislation, which poses significant practical challenges.

51. Some of the time-intensive tasks required to comply with the Guidance include:

51.1. When relying on the disclosing party to inform the individual of all matters, contract templates will likely need to be updated and existing contracts may need to be reviewed / re-written / renegotiated out of cycle. New Zealand-based parties may have insufficient negotiating power to implement these clauses (including on behalf of their overseas counterparts) with large inter/multi-national third parties.

51.2. Wide-scale process uplift across all indirect collection processes to consider whether authorisation can be collected via T&Cs, or alternatively, individual forms.

51.3. Disclosing parties who share among multiple collecting agencies within the same industry may wish to negotiate identical expectations, requiring pan-bank negotiations and agreements before entering into contract negotiation. This is likely to lead to significant difficulties in implementation if the Guidance is issued in its current form.

52. Given the tight timing, there is a need for certainty on the OPC's requirements as soon as possible, to ensure that compliance timeframes can be met. Similarly, we note some of the issues raised in this submission may require solutions that sit outside of the Guidance, and seek prompt engagement on those matters to ensure we achieve positive outcomes for the banking sector, customers and OPC.

New Zealand Banking Association
Te Rangapū Pēke

APPENDIX A: Comparison of IPP3 and IPP3A compliance requirements

What you need to tell people	Disclosure under draft IPP3A Guidance	Disclosure under IPP3 (Government commentary / generally accepted practice)	Commentary and Questions
The fact that the information has been collected	Specify exactly what kind of information you are collecting and the source.	Categories of PI / processes that lead to the collection of PI are outlined in Privacy Policies and Statements.	Broad categories should, similarly, be sufficient for IPP3A.
The purpose of the collection	Specific enough so the individual can understand what their information is being used for e.g. “to confirm that you are a member of x organisation to check that you are eligible for this discount”.	Broad categories i.e. comply with domestic and international laws, rules and regulations, including any that are reasonably expected to be implemented.	The requirement for a specific purpose does not, in our view, align with the allowance under IPP10 to use personal information for directly related purposes. We consider disclosure of the purpose should align with IPP3.
The intended recipients of the information	Expectation that recipients are named.	Broad categories i.e. authorities such as regulators, government agencies, courts or the police; brokers, referrers, distributors and financial advisers.	Specific listing of recipients may lead to a high compliance burden and notification fatigue for individuals (particularly if the addition of new recipients would require continuous monitoring and notification to the individual). We submit this requirement too should align with IPP3.

The name and address of the agency that is collecting information and the agency that holds the information	Tell people who has collected their information and provide address of the holding company.	N/A (addressed via requirements for direct collection, or otherwise under the naming of recipients per the above).	This may import an obligation to maintain a source of truth from all potential sources of PI – i.e. a disclosing agency may need to update this information if a recipient's details change. This information may also not always be readily available or appropriate to share (e.g. for an individual, or sole trader operating from a home office). As above, we recommend this aligns with the general, broad category approach to recipients under IPP3.