

Incorporation of Information Privacy Principle 3A (IPP3A) into Sector Codes of Practice

**Submissions on behalf of The Law Association of
New Zealand by the Technology and Law
Committee**

INTRODUCTION

1. This submission is made on behalf of the Technology and Law Committee of The Law Association of New Zealand (TLANZ). The Committee comprises practitioners with specialist expertise in technology, law, and public policy, and provides informed commentary on issues at the intersection of legal regulation and technological innovation.
2. TLANZ is an independent membership organisation representing more than 8,600 legal professionals across Aotearoa New Zealand. Through its expert committees, the Association contributes to legislative and policy development across a broad range of areas, including privacy, cybersecurity, digital regulation, and emerging technologies.

EXECUTIVE SUMMARY

3. The Law Association of New Zealand (TLANZ) welcomes the enactment of the *Privacy Amendment Act 2025* and supports the incorporation of Information Privacy Principle 3A (IPP3A) into the relevant sector Codes of Practice — the Civil Defence National Emergencies (Information Sharing) Code 2020, the Credit Reporting Privacy Code 2020, the Health Information Privacy Code 2020, and the Telecommunications Information Privacy Code 2020.
4. IPP3A strengthens transparency by requiring agencies that collect personal information indirectly to take reasonable steps to notify individuals. TLANZ considers that the exceptions already set out in section 22(4) of the *Privacy Act 2020* (as amended by the *Privacy Amendment Act 2025*) are fit for purpose across these Codes and should not be expanded.
5. TLANZ supports a principled approach that emphasises clarity and consistency through guidance rather than additional exemptions. Deferred or alternative notification methods should be preferred where immediate notice is impracticable or would defeat the purpose of collection.

SUBMISSIONS

6. Health Information Privacy Code 2020 and Amendment No 1

- 6.1 The Health Information Privacy Code 2020 (HIPC) governs the collection and use of health information under Rules 3 and 11, which address collection from the individual and limits on disclosure. Health agencies routinely receive information indirectly through referrals, laboratories, pharmacies, and emergency services. Requiring notification for each indirect transfer would duplicate existing clinical communication and could delay treatment.
- 6.2 The exceptions in IPP3A(4)(a), (4)(e), and (4)(f) appropriately cover situations where notification would not prejudice the individual, is impracticable, or could endanger health or safety. TLANZ recommends that the HIPC cross-reference IPP3A explicitly and clarify that “impracticability” includes circumstances where notification would interfere with timely care. The HIPC should also clarify, that where possible, post-event notification should still occur once the clinical risk has passed. This approach aligns with the HIPC’s existing principles of necessity and proportionality.

7. Credit Reporting Privacy Code 2020

- 7.1 The Credit Reporting Privacy Code 2020 (CRPC) regulates credit reporters that collect information from lenders, courts, and public registers. Because these collections are almost entirely indirect, literal application of IPP3A would require individual notification for every credit update or default entry. Such a requirement would be unworkable and would offer

minimal privacy benefit. Transparency is already achieved through contractual disclosures at the time of credit application and through statutory rights of access and correction under IPP6 and IPP7.

- 7.2 The exceptions in IPP3A(3), (4)(a), and (4)(e) cover these arrangements adequately. Individuals are already aware that their information may be shared with credit reporters; non-notification does not prejudice them; and bulk data transfers make per-case notification impracticable. TLANZ therefore recommends that the CRPC acknowledge that existing industry practice meets the requirements of IPP3A and that credit reporters maintain internal records of instances where non-notification occurs. Aggregated reporting to the OPC could further enhance accountability.

8. Telecommunications Information Privacy Code 2020

- 8.1 The Telecommunications Information Privacy Code 2020 (TIPC) regulates the handling of subscriber and network data under Rule 2 (Source of Telecommunications Information). Telecommunications providers frequently collect information indirectly through roaming partners, fraud prevention systems, and emergency call routing. These activities are essential for network security and public safety.
- 8.2 TLANZ considers that the intent of IPP3A is already met by current practice. The existing exceptions in IPP3A(4)(a), (4)(c), (4)(e), and (4)(g) are sufficient to address law-enforcement co-operation, network integrity, and aggregate analytics. However, the Code should be updated to reference IPP3A and to recognise that notification may be deferred where immediate disclosure would prejudice security or investigations. Annual transparency statements on the use of these exceptions would strengthen public trust.

9. Civil Defence National Emergencies (Information Sharing) Code 2020

- 9.1 The Civil Defence National Emergencies (Information Sharing) Code 2020 applies during declared national emergencies and for twenty working days after their termination. It permits the indirect collection and sharing of personal information to protect life and property. Immediate notification in such circumstances is neither practicable nor appropriate.
- 9.2 The exceptions in IPP3A(4)(d), (4)(e), and (4)(f) provide ample coverage for these situations. TLANZ supports retaining the Code's broad flexibility but recommends that it explicitly refer to IPP3A to ensure statutory coherence. Once an emergency has ended, agencies should communicate how data was used and what protections applied. A post-event review requirement would enhance public confidence and demonstrate accountability.

10. Cross-Code Observations

- 10.1 The Committee recommends a uniform interpretation and application of IPP3A across all sector Codes to prevent fragmentation and maintain consistent privacy standards. Where direct notification is not practicable, agencies should adopt deferred notification as soon as the reason for delay no longer applies. Each agency should also maintain an internal record of any reliance on exceptions under IPP3A(4) and periodically review those decisions as part of its privacy management programme. The Office of the Privacy Commissioner (OPC) could further support this consistency by issuing examples of what constitutes "reasonable steps" and "impracticability" in sector-specific contexts.
- 10.2 The Committee also notes that the Electricity Industry Participation Code 2010, administered by the Electricity Authority, imposes binding Consumer Care Obligations under Part 11A which already require regulated participants to uphold clear standards of customer care, information management, and service continuity. These obligations reflect the same principles of transparency, accountability, and protection of personal information that underpin IPP3A.

- 10.3 Electricity retailers, distributors, and metering participants routinely handle personal information indirectly through interconnected operational systems—such as meter-data exchanges, retailer switching, network-fault coordination, and credit-risk assessment. These activities occur within a statutory compliance framework monitored and enforced by the Electricity Authority, with mandatory obligations and independent audit processes ensuring proper information governance.
- 10.4 The Committee considers that no additional or narrower exceptions are required for the electricity sector. The existing provisions in IPP3A(4)(a) (no prejudice to the individual), (4)(e) (impracticability), and (4)(g) (security or law-enforcement cooperation) are sufficient to accommodate operational realities. In many cases, immediate notification would be impracticable or could compromise network reliability or system security. Where notification is deferred, agencies should ensure it occurs as soon as the operational reason for delay has passed.
- 10.5 Accordingly, TLANZ recommends that the Privacy Commissioner recognise the Electricity Industry Participation Code 2010 as a comparable sectoral framework for the purposes of IPP3A, in the same way that the Telecommunications Information Privacy Code 2020 is treated. Explicitly cross-referencing the consumer-care obligations in OPC guidance would promote regulatory coherence across essential-service sectors and help avoid unnecessary duplication of compliance requirements.

CONCLUSION

11. The Law Association of New Zealand supports the incorporation of Information Privacy Principle 3A (IPP3A) into the Credit Reporting, Health, Telecommunications, and Civil Defence National Emergencies Codes of Practice. The Committee also endorses recognising the Electricity Industry Participation Code 2010 (Part 11A) as a sectoral instrument already consistent with IPP3A's intent.
12. The existing exceptions in section 22(4) of the Privacy Act 2020 are adequate and should not be broadened. The Committee emphasises the importance of clear OPC guidance, strong record-keeping practices, and targeted education within each sector to ensure effective implementation. This balanced approach will strengthen transparency, uphold public trust, and maintain the equilibrium between individual privacy rights and operational necessity as IPP3A takes effect on 1 May 2026.
13. Should any aspect of this submission require further clarification, we would be pleased to discuss our views in more detail. Please contact Moira McFarland, Committee Executive, at moira.mcfarland@tlanz.nz to arrange a meeting or to address any queries.

Ngā mihi,



Lloyd Gallagher
Convenor
TLANZ Technology and Law Committee



Amy Kingston-Turner
Member
TLANZ Technology and Law Committee