Privacy Commissioner
Te Mana Matapono Matatapu

Intelligence and Security Act amendments to Privacy Act: FAQs

What changes have been made to the Privacy Act as a result of the Intelligence and Security Act 2017?

The Privacy Act exemption for the handling of personal information by the New Zealand Security Intelligence Service (NZSIS) and the Government Communications Security Bureau (GCSB) has been amended (s 57). The NZSIS and the GCSB are now subject to most of the information privacy principles. However principles 2, 3 and 4(b) do not apply to the collection of personal information by the NZSIS and the GCSB.

Voluntary disclosures of personal information to the NZSIS and the GCSB are also now subject to the Privacy Act (formerly these were exempted by s 57).

New exceptions have been added to principles 10 and 11 to provide for the use and disclosure of personal information by the NZSIS and the GCSB. The new exception to principle 11 also provides for non-compelled disclosures of personal information to the NZSIS and GCSB.

What are the consequences of these amendments?

The key consequences of the amendments to the Privacy Act include the following:

- The NZSIS and the GCSB must now comply with most of the privacy principles
- Agencies disclosing personal information to the NZSIS and the GCSB will now need to comply with principle 11 (where formerly they were exempt under s 57), unless the disclosure is compelled on another legal basis
- The NZSIS and the GCSB can use and disclose personal information for a secondary purpose, subject to certain limits
- Affected individuals may now make privacy complaints about the collection, security, use, and disclosure of their personal information (in addition to access and correction complaints that can already be made) where there is reason to believe that a breach of an applicable privacy principle is an interference with their privacy (and where the action complained about occurs on or after 28 September 2017).

What privacy principles now apply to the NZSIS and the GCSB?

The NZSIS and the GCSB will now be subject to principles 1, 4(a), 5, 8, 9, 10 and 11, in addition to principles 6, 7 and 12 that already apply to the NZSIS and the GCSB.

The NZSIS and the GCSB remain exempt from principles 2, 3 and 4(b).

When can personal information be used or disclosed by the NZSIS or the GCSB for a secondary purpose?

Privacy principle 10(2) allows the NZSIS and the GCSB to use personal information obtained for one purpose, for a different or secondary purpose, where the intelligence and security agency has reasonable grounds to believe that the use of the information for the secondary purpose is necessary to perform any of its functions.

However s 220 of the Intelligence and Security Act limits the use of information obtained by or disclosed to the NZSIS for the purpose of a security clearance assessment. Information obtained in that context can only be used for the security clearance assessment, any other security clearance assessment and for counter-intelligence. Counter-intelligence is defined in s 220(3) as intelligence activities to identify and counteract the threat or potential threat of unauthorised disclosure of official information by a person who holds or has held a New Zealand Government-sponsored national security clearance.

Privacy principle 11(fa) allows the NZSIS and the GCSB to disclose personal information where the intelligence and security agency has reasonable grounds to believe that the disclosure of the information is necessary to perform any of its functions.

When can personal information be disclosed to the NZSIS or the GCSB?

In addition to mandatory disclosures under a compulsory warrant, order or direction (e.g. an intelligence warrant or a business records direction), personal information can be disclosed to the NZSIS or the GCSB on a voluntary discretionary basis, where the holder of the personal information believes on reasonable grounds that the disclosure is necessary for the intelligence agency to perform any of their functions (principle 11(fa)). Other exceptions to principle 11 can also be used, where the necessary criteria are met, including to avoid prejudice to the maintenance of the law (principle 11(e)(i)) or where necessary to avoid a serious threat to health, life or safety (principle 11(f)).

These disclosures can be proactive disclosures (in the absence of any request but where the agency holding the information considers it necessary to make the disclosure) or disclosures in response to a request for personal information from the NZSIS of the GCSB.

Where the NZSIS or the GCSB request information, the request must provide details of the information that is sought, and confirm that the information is necessary to enable the requester to perform any of its functions (s 121 of the Intelligence and Security Act).

To enable an agency to decide whether to disclose the information sought, the Director-General of the intelligence agency may certify under s 122(3) of the Intelligence and Security Act that the disclosure sought is necessary for the performance of the agency's function.

Note that the relevant Privacy Act code of practice applies where the personal information is health information, telecommunications information or credit information.

Part 5(4) of the Intelligence and Security Act provides for the compelled disclosure of the business records of telecommunications network operators and financial service providers

(including customer information) in accordance with a business records direction issued by the Director-General of the NZSIS or the GCSB.

What changes have been made to the Privacy Codes of Practice as a result?

Three codes of practice have been updated to reflect the new exception in principle 11:

1. The Health Information Privacy Code now has a new rule 11(2)(da) that allows for health information to be disclosed, where a health agency believes, on reasonable grounds, that it would not be desirable or practicable to obtain the authorisation of the individual concerned, and that the disclosure is necessary to enable the NZSIS or the GCSB to perform any of their functions.

2. The Telecommunications Information Privacy Code now has a new rule 11(1)(ga) that allows for telecommunications information to be disclosed where a telecommunications agency believes, on reasonable grounds, that the disclosure is necessary to enable the NZSIS or the GCSB to perform any of their functions, except where the disclosure of the information may be sought in accordance with a business records direction under Part 5(4) of the Intelligence and Security Act.

3. The Credit Reporting Privacy Code now has two new sub-rules:

    a. New rule 11(1)(ca) allows for credit information to be disclosed where a credit reporter believes, on reasonable grounds, that the disclosure is necessary to enable the NZSIS or the GCSB to perform any of their functions, other than security clearance assessments, and
    b. New rule 11(1)(cb) allows for credit information to be disclosed by a credit reporter in accordance with an access agreement. An access agreement is a written agreement between the NZSIS and a credit reporter providing access to credit information to enable the NZSIS to perform security clearance assessments (defined in s 220 of the Intelligence and Security Act). New Schedule 3A sets out certain provisions that are to be included in any access agreement.

What are the functions of the NZSIS and the GCSB?

The functions of the NZSIS and the GCSB are set out in Part 2 of the Intelligence and Security Act 2017, and include:

- Collecting and analysing intelligence and providing advice and assistance to public authorities, and other persons where authorised (s 10).

- Providing protective security services, advice and assistance to a public authority, and other persons where authorised (s 11). This includes personnel security, information security and physical security and advice about national security risks. In addition, in relation to the GCSB, this includes providing information assurance and cybersecurity activities to a public authority or other person where authorised, and doing everything necessary or desirable to protect the security and integrity of important communications and information infrastructures (s 12).

- Co-operating with each other and with the New Zealand Police and the New Zealand Defence Force and to provide advice and assistance (s 10).

- Co-operating with other entities and providing advice and assistance to respond to an imminent threat to life or safety (s 14).

- Any other function conferred or imposed by another enactment (s 15).

The functions of the NZSIS and the GCSB do not generally include enforcement functions except in certain circumstances (s 16).

How does the Privacy Commissioner deal with complaints about the actions of the NZSIS and the GCSB?

The Privacy Commissioner receives complaints about alleged breaches of the information privacy principles under Part 8 of the Privacy Act. Matters giving rise to a Privacy Act complaint should first be raised with the intelligence agency concerned.

In handling any complaint, the Privacy Commissioner may consult with the Ombudsman or the Inspector-General of Intelligence and Security, in case a matter is more properly dealt with under their respective complaints jurisdiction (s 72, s 72B, s 117, s 117B).

The outcome of the Privacy Commissioner's investigation of a complaint concerning the actions of the NZSIS or the GCSB is subject to a special procedure (s 81). This provides that a complainant cannot bring proceedings in the Human Rights Review Tribunal following the Privacy Commissioner's investigation. If the Commissioner forms the opinion that there has been an interference with the privacy of the individual, the Commissioner must report to the intelligence agency concerned and make any recommendations as a result. The Commissioner may request a report back as to the steps taken by the intelligence agency to give effect to the recommendations made. The Commissioner may report to the Prime Minister if the agency concerned has not taken adequate and appropriate action, and the Prime Minister may present the Commissioner's report to the House of Representatives.

Can the privacy principles be enforced against the NZSIS and the GCSB?

Individuals have the right under section 67 of the Privacy Act to bring a complaint to the Privacy Commissioner where it appears there has been an interference with their privacy. However, the information privacy principles do not generally confer any legal right that is enforceable in a court (s 11(2)).

Principle 6(1) - the right to obtain confirmation of whether the agency holds personal information and the right to have access to that information - does however confer legal rights that are enforceable in a court. This would be interpreted in light of any available refusal grounds, including prejudice to the security of New Zealand (s 27(1)(a)), and s 32 of the Privacy Act that permits a "neither confirm nor deny" response to avoid prejudice to important interests.

As noted above, the Privacy Commissioner's investigation of complaints against the NZSIS and the GCSB is subject to a special procedure (s 81) and a complainant cannot bring proceedings in the Human Rights Review Tribunal following completion of the Privacy Commissioner's investigation.

Are there any other grounds to make a complaint about the NZSIS or the GCSB?

Complaints can be made to the Inspector-General of Intelligence and Security by any New Zealand person that has been affected by any act, omission, practice, policy, or procedure of the NZSIS or the GCSB (s 171(2) of the Intelligence and Security Act).

There is also a procedure for employees and former employees of the NZSIS and GCSB to make a complaint to the Inspector-General (s 171(3)) and Parliament's Speaker may complain on behalf of a Member or Members of Parliament about any act, omission, practice, policy or procedure of the NZSIS or the GCSB (s 171(4)).

Whistleblowing complaints by employees of the NZSIS and the GCSB and other public servants are covered by procedures required by the Protected Disclosures Act 2000.

Complaints about decisions of the NZSIS and the GCSB in relation to official information requests are investigated by the Office of the Ombudsman (Part 5 of the Official Information Act 1982). The Ombudsman can also investigate certain decisions made by the NZSIS and the GCSB under Parts 3 and 4 of the Official Information Act.

Has the Privacy Commissioner been consulted about the new legislation?

The Privacy Commissioner made a written submission on the Intelligence and Security Bill and appeared before the Foreign Affairs, Defence and Trade Committee to present his submission.

The Privacy Commissioner was consulted on direct access agreements issued under Part 5(2) of the Intelligence and Security Act.

The Privacy Commissioner has been consulted on draft ministerial policy statements prepared under s 206(a), (d), (e), (f), (g), and (h) of the Intelligence and Security Act.

Where can I find out more about these changes?

You can contact our enquiries line (on 0800 803 909 or enquiries@privacy.org.nz) if you have any specific questions about these changes to the Privacy Act. You can also use our online FAQs - AskUs – www.privacy.org.nz/Ask