Privacy Commissioner
Te Mana Mātāpono Matatapu

Office of the Privacy Commissioner

Compliance Notice Guidelines

Privacy Act 2020

Version 1.0, 23 November 2020

Introduction

1. The Privacy Commissioner, an independent Crown entity, is New Zealand's privacy and data protection regulator under the Privacy Act 2020.

2. The Privacy Commissioner monitors compliance with the Privacy Act from a variety of channels including public enquiries to OPC, media reports, privacy complaints, Commissioner initiated inquiries and investigations, the exercise of the Commissioner's oversight and monitoring functions, privacy breach reporting to OPC, and referrals to OPC from other regulators, both within New Zealand and internationally. The Privacy Commissioner also monitors compliance with the Privacy Act codes of practice and with other specific codes and statutory provisions within the Commissioner's oversight.

3. Compliance issues can arise from a specific incident or from repeated or systemic issues. A systemic privacy issue can be identified from an incident that is brought to the Commissioner's attention, or from multiple complaints about the same agency, industry or sector that are of a similar nature. A systemic compliance issue can also be identified from other channels such as news media commentary or discussion on social media.

4. On becoming aware of a compliance issue, the Privacy Commissioner may consider issuing a compliance notice. To do so, the Commissioner must reach the view, in the circumstances, that there has been a breach of the Privacy Act or another relevant breach.[1]

5. The Commissioner is empowered to bring regulatory action under Part 6(2) of the Privacy Act by issuing a compliance notice to an agency in breach of its obligations.[2] This is in addition to other regulatory action available to the Privacy Commissioner under the Privacy Act.[3]

What is a compliance notice?

6. A compliance notice is a written notice from the Privacy Commissioner to a public or private sector agency that the agency is in breach of its statutory obligations under the Privacy Act or a code of practice, or under another relevant Act or instrument. It is a direction to an agency requiring it to take certain action, or to desist from taking certain action, in order to comply with

[1] Privacy Act, section 123. This includes breaches of other Acts that are treated as a breach of an information privacy principle or an interference with privacy – see the table in Appendix 1.
[2] Privacy Act, s 123(1).
[3] Privacy Act, s 123(3). For example, the Privacy Commissioner may issue a compliance notice as well as investigate a privacy complaint relating to the same matter.

the requirements of the Privacy Act, the code of practice or another specific code or provision.

7. The notice will specify the nature of the breach and require the agency to remedy the breach so that it complies with its statutory obligations. It may require that agency to take particular steps to comply with its statutory obligations within a specified timeframe.[4]

Who can be issued with a compliance notice?

8. The Privacy Commissioner can issue a compliance notice to any individual, person or entity that the Privacy Act applies to[5] – either a New Zealand agency,[6] an overseas agency[7] or individual[8], if that person or entity is in breach of their obligations under the Privacy Act, a code of practice or another specific code or provision.[9]

What is the threshold for issuing a compliance notice?

9. The Privacy Commissioner can issue a compliance notice at any time, if satisfied that an agency is in breach of its obligations.

10. A compliance notice can be issued in relation to a specific breach (a one-off incident) or a systemic breach. A systemic breach is a privacy issue that may have ongoing implications or effects and may relate to the adequacy of an agency's compliance practices, procedures or systems, adherence to those compliance practices, procedures or systems or attitudes to privacy compliance by personnel within the agency.

11. Not every breach or compliance issue will result in the issue of a compliance notice. The Privacy Commissioner will take certain considerations into account before issuing a compliance notice – these are set out below. The Privacy Commissioner must also provide an agency with a prior written notice about the breach and provide a reasonable opportunity to comment, before proceeding to issue a compliance notice.[10]

12. The Privacy Commissioner may (but is not required to) use other means for dealing with an identified breach such as a complaint investigation, referral

[4] Privacy Act, s 125.
[5] Privacy Act, s 4(1).
[6] Privacy Act, s 8.
[7] Privacy Act, s 9.
[8] Privacy Act, s 4(1)(c).
[9] Privacy Act, s 123.
[10] Privacy Act, s 124(3).

of a matter to the Director of Human Rights Proceedings,[11] or to another oversight body such as the Ombudsman,[12] a compliance advice letter, Privacy Commissioner own motion inquiry or investigation, naming the agency concerned under the Commissioner's naming policy, prosecution[13] or any other available means for dealing with the matter.

13. The Privacy Commissioner is not limited from issuing a compliance notice in conjunction with or in addition to exercising other functions or powers in relation to a matter such as a complaint investigation, making an access direction, responding to an enquiry or representation from any person on any matter affecting the privacy of the individual, carrying out the Commissioner's statutory oversight and monitoring functions, an own motion inquiry or investigation, or any other available functions or powers.

What sort of breaches could result in a compliance notice?

14. A compliance notice can respond to different kinds of breaches of an agency's privacy obligations.

15. A compliance notice can relate to breaches of an information privacy principle, [14] including:

    a) one or more of the collection principles 1- 4;
    b) the security principle 5;
    c) the correction principle 7 (failing to correct a person's personal information or to attach a statement of correction);
    d) the use and disclosure principles 10, 11 and 12; [15]
    e) the unique identifier principle 13.

16. A compliance notice is also a potential response by the Privacy Commissioner to breaches relating to information privacy principle 6 (providing individuals with access to their personal information). While the Commissioner has a power to make an access direction;[16] or to take other action;[17] this does not limit the Commissioner from issuing a compliance

[11] Privacy Act, s 78, 84, 91.
[12] Privacy Act, ss 75-76.
[13] Privacy Act, s 123(2)(b).
[14] Privacy Act, s 22.
[15] Note that in relation to cross border transfers of personal information, the Privacy Commissioner has a statutory power to issue a notice under Part 8 in certain circumstances (known as a transfer prohibition notice): Privacy Act, s 193.
[16] Privacy Act, s 92. Following investigation of a complaint under principle 6, the Privacy Commissioner may exercise a statutory power to direct an agency to provide an individual with confirmation of whether the agency holds personal information and access to any specified personal information (known as an access direction).
[17] Privacy Act, s 91.

notice in relation to specific breaches of Part 4(1) of the Privacy Act[18] or Part 5(2) of the Privacy Act.[19]

17. A compliance notice can relate to notifiable privacy breaches and require an agency to notify affected individuals, and to take any other specified steps as a result of the breach.[20]

18. A compliance notice can relate to breach of an information sharing agreement or an information matching agreement that might be identified from the Privacy Commissioner's routine statutory monitoring of, and reporting on, these programmes from an individual's complaint, or from any other source of information.[21]

19. A notice can also relate to breach of any other statutory obligation under the Privacy Act, for example, the obligation to appoint a Privacy Officer,[22] and the obligation to provide information to the Privacy Commissioner on request.[23]

20. Further, a compliance notice may be issued if an agency is in breach of its obligations under a code of practice[24] or code of conduct.[25]

Privacy Commissioner's powers to obtain information and examine on oath

21. The Privacy Commissioner may investigate before issuing a compliance notice and may use investigation powers available under Part 5 of the Privacy Act to do so.

22. The Commissioner has statutory powers under the Privacy Act to summons and examine persons on oath, and to require any person to provide relevant information. To enable the Commissioner to determine whether to issue a compliance notice, the Commissioner may hear or obtain information from any person considered to have relevant information.[26]

[18] Part 4(1) of the Privacy Act sets out the obligations of an agency in relation to requests made by an individual under IPP 6.
[19] Part 5(2) of the Privacy Act relates to the Commissioner's investigations and sets out the obligations of an agency in relation to an investigation, as required.
[20] Privacy Act, Part 6(1).
[21] Privacy Act, Part 7(1) and (4).
[22] Privacy Act, s 201.
[23] Privacy Act, s 87.
[24] Privacy Act, Part 3(2).
[25] This refers to a code of conduct issued under another Act that gives the Privacy Commissioner jurisdiction to investigate complaints for breaches of that code - see the attached table in Appendix 1.
[26] Privacy Act, s 128.

What will the Privacy Commissioner take account of?

23. The issue of a compliance notice is not automatic and will depend on the circumstances. The Privacy Commissioner will consider each identified compliance issue on a case-by-case basis, including all relevant factors. The Privacy Commissioner will act in accordance with the Compliance and Regulatory Action Framework (CARAF) in making decisions about compliance notices. This means that education and voluntary compliance may be preferred before enforcement action such as a compliance notice is issued. However, in some circumstances, the Commissioner may issue a compliance notice promptly following investigation of a compliance issue, in accordance with the CARAF.

24. The following are factors that **must** be taken into consideration by the Commissioner to the extent they are relevant in the circumstances (the mandatory factors). These include:[27]

    a) Whether there is another means under the Privacy Act or another Act for dealing with the breach – for example, if a complaint investigation or other regulatory response is sufficient to address the issue;
    b) The seriousness of the breach - for example, is the information particularly sensitive in the circumstances, or does the breach create a real or significant privacy risk to individuals;
    c) The likelihood of a repeat of the breach – for example, is there a systemic vulnerability that creates a risk that the breach could be repeated;
    d) The number of people who may be or are affected by the breach – that is, how big is the class of people potentially affected;
    e) Whether the agency has been cooperative in all dealings with the Commissioner – for example, has the agency been responsive to the Privacy Commissioner's requests for information, and addressed issues raised on previous occasions, or has the agency attempted to conceal relevant information from the Commissioner or obstructed the Commissioner's inquiries;
    f) The likely costs to the agency of complying with the notice – for example, the extent to which measures to remedy a breach will require additional resources or expertise and the reasonableness of those measures in all the circumstances.

25. The Commissioner **may** (but is not necessarily required to) take account of the extent to which any person has been adversely affected by the identified breach – for example whether the breach has or may:[28]

    a) cause loss, detriment, damage or injury to an individual;

[27] Privacy Act, s 124(1).
[28] Privacy Act, s 123(2)(a).

b) adversely affect an individual's rights, benefits or privileges, obligations or interests; or
c) result in significant humiliation, loss of dignity or significant injury to feelings.

26. The Commissioner is also required to take account of certain matters when exercising functions under the Privacy Act.[29] These include:

a) Cultural perspectives on privacy;
b) The desirability of facilitating the free flow of information;
c) Government and business efficiency in achieving their objectives;
d) New Zealand's international obligations, including international technology of communications;
e) Developing international guidelines relevant to the better protection of individual privacy.

What does a compliance notice include?

27. A compliance notice **must** include the following information:[30]

a) the name of the agency the compliance notice is issued to;
b) a description of the breach;
c) the relevant statutory provision or provisions;
d) the right to appeal the notice;
e) any other relevant information prescribed by regulations.[31]

28. The compliance notice **must** also inform the agency of the right to appeal the compliance notice.[32]

29. In addition, a compliance notice **may** include the following information:[33]

a) any particular steps the Privacy Commissioner considers need to be taken by the agency to comply with the relevant statutory provisions;
b) any conditions that the Commissioner considers are appropriate;
c) the date or dates by which the agency must comply, and report back to the Commissioner about the steps taken;
d) any other information that the Commissioner considers useful.

30. The Commissioner can subsequently vary a compliance notice at any time if the Commissioner considers that any of the information in the notice

[29] Privacy Act, s 21.
[30] Privacy Act, s125(1).
[31] No regulations have been made under s 215(1)(c).
[32] Privacy Act, s 125(1)(d).
[33] Privacy Act, s 125(2).

needs to be added to or changed, or part of the notice is no longer needed.[34]

31. If a compliance notice is varied, the written notice advising the agency must inform the agency of the right to appeal the varied notice.[35]

Does an agency have the right to comment?

32. Yes, the Privacy Commissioner must provide the agency concerned with a reasonable opportunity to comment.[36] The Commissioner will determine an appropriate period for comment, taking account of the relevant circumstances.[37]

33. The Commissioner will provide the agency with a written notice to the agency for their comment (a draft notice).

34. The draft notice **must** include the following information:

    a) a description of the identified breach;
    b) the relevant statutory provision or provisions;
    c) a summary of the Commissioner's conclusions about the mandatory factors the Commissioner has considered;
    d) the particular steps the Commissioner considers the agency needs to take to remedy the breach and any conditions the Commissioner considers appropriate; and
    e) the date or dates by which the Commissioner proposes that the agency must remedy the breach and report to the Commissioner (if any).

How should an agency respond to a compliance notice?

35. Unless the agency lodges an appeal, it must take steps to comply with the notice – including taking any particular action set out in the notice.[38] Alternatively, the agency may take some steps to comply, while appealing part of the compliance notice.

[34] Privacy Act, s 127.
[35] Privacy Act, s 127(3).
[36] Privacy Act, s 124(3).
[37] Privacy Act, s 124(4).
[38] Privacy Act, ss 126, 131.

36. The steps to comply with the notice must be taken as soon as practicable after receiving it. The compliance notice itself may set a date by which the breach must be remedied (unless that date is varied or modified, or the notice is cancelled or suspended).

37. If an agency disagrees with the compliance notice, or part of the notice, it can appeal the notice in the Human Rights Review Tribunal (within 15 working days from issue of the compliance notice).

Will the compliance notice be made public?

38. The Commissioner has a discretion to publish details about a compliance notice including the identity of the agency concerned, if the Commissioner considers it is desirable to do so in the public interest.[39] For example, it may be instructive for details of the compliance notice to be published to inform and guide other agencies about their compliance obligations.

39. If publishing details of the compliance notice would be adverse to the agency concerned, the Commissioner must first give the agency an opportunity to be heard.[40]

Can a compliance notice be varied or cancelled?

40. Yes, the Privacy Commissioner has the discretion to vary or cancel a compliance notice at any time.[41]

41. The Commissioner can vary a compliance notice at any time if any of the information in the notice needs to be added to or changed, or part of the notice is no longer needed.

42. The Commissioner can cancel a compliance notice at any time if satisfied that all or part of the notice has been complied with, or the notice is no longer needed.

43. If the Commissioner decides to vary or cancel a compliance notice, written notice of the decision must be given to the agency, and the variation or cancellation takes effect on the first working day after the day the decision is given to the agency.

44. An agency can appeal all or any part of a compliance notice that has been varied.

[39] Privacy Act, s 129.
[40] Privacy Act, s 210.
[41] Privacy Act, s 127.

Can a compliance notice be appealed?

45. Yes, the agency may appeal all or any part of a compliance notice. An appeal must be lodged in the Human Rights Review Tribunal within 15 working days.[42]

How is a compliance notice enforced?

46. If an agency does not comply with a notice or appeal it, the Privacy Commissioner may bring enforcement proceedings in the Human Rights Review Tribunal to enforce the notice.[43]

47. The Tribunal may make an order that the agency comply with the notice by a specified date.[44]

48. Failure to comply with Tribunal order is an offence, and if prosecuted, the agency could be fined for non-compliance.[45]

How will compliance notices be reported on?

49. The Commissioner is required to report at least annually on the activities of the Office. It is likely that compliance notices issued will form part of future reporting by the Commissioner.

[42] Privacy Act, s 131.
[43] Privacy Act, s 130.
[44] Privacy Act, s 133(1)(a).
[45] Privacy Act, s 133(3).

APPENDIX 1

Actions that are treated as a breach of an information privacy principle (IPP) or an interference with the privacy of the individual for purposes of section 123(1)(b) of the Privacy Act

Auditor Regulation Act 2011, s 44
Electoral Act 1993, s 204X
Family Violence Act 2018, s 245
Financial Markets Conduct Act 2013, Sch 2, cl 12
Financial Service Providers (Registration and Dispute Resolution) Act 2008, s 33
Insolvency Act 2006, s 456
Limited Partnerships Act 2008, s 66
Motor Vehicle Sales Act 2003, ss 59, 81
Personal Property Securities Act 1999, s 174
Plumbers, Gasfitters and Drainlayers Act 2006, s 87
Policing Act 2008, s 95B
Real Estate Agents Act 2008, s 70
Summary Proceedings Act 1957, s 92F

Codes of conduct providing for complaints to the Privacy Commissioner for purposes of section 123(1)(c) of the Privacy Act.

Social Security Act 2018, Sch 6, cl 12
Public and Community Housing Management Act 1992, s 89

APPENDIX: 2 TEMPLATE COMPLIANCE NOTICE

COMPLIANCE NOTICE

Issued by the Privacy Commissioner

under section 123 of the Privacy Act 2020

on [*date*]

Served on:	[*name of Agency and contact details*] (the "Agency")
Compliance Notice number:	[*CN/2020XYZ*]
Means of service:	[*post/email/delivery, noting applicable Privacy reg*]

PRELIMINARY MATTERS

The Privacy Commissioner considers the Agency is in breach of its obligations under the [Privacy Act / Privacy Code of Practice / other statutory obligation] and has provided prior written notice to the Agency and a reasonable opportunity to comment on that notice under section 124(3) of the Privacy Act.

The Agency [has/ has not] provided comment to the Privacy Commissioner on that written notice.

BREACH THIS NOTICE RELATES TO

The Privacy Commissioner has taken account of any comment received from the Agency, and the issue of this notice confirms that the Privacy Commissioner considers that the Agency is in breach of the following statutory provision/s (the "breach"):

[*specify privacy principle/s or other provisions of the Privacy Act, code of practice or other statutory provision*]

The basis for the Commissioner's view is the following:

1. [*Summary of high level facts and nature of the breach*]
2. [*Nature of investigation by Privacy Commissioner or information considered*]
3. [*refer to previous relevant correspondence between Privacy Commissioner and Agency*]
4. [*Commissioner's conclusion as to breach*]

FACTORS CONSIDERED BY THE PRIVACY COMMISSIONER

A summary of the Privacy Commissioner's conclusions on the following matters under section 124(1) of the Privacy Act to the extent relevant is as follows:

[provide summary of conclusions on the s 124(a) factors:

a) Whether there is another means under the Privacy Act or another act for dealing with the breach;
b) The seriousness of the breach;
c) The likelihood of a repeat of the breach;
d) The number of people who may be or are affected by the breach;
e) Whether the agency has been cooperative in all dealings with the Commissioner;
f) The likely costs to the agency of complying with the notice.

[include summary of any other matters such as:

a) [harm considerations under s 69(2)(b)]
b) [additional relevant considerations, including s 21]

REQUIREMENTS OF THIS COMPLIANCE NOTICE

The Agency is required to comply with this notice as soon as practicable and to remedy the breach described in this notice by [*specify date if applicable*].

The Agency is required to take the following steps in order to remedy the breach in order to comply with [*privacy principle or statutory provision*]:

[*specify particular step/s needed to remedy the breach, including any appropriate conditions]*

[The Agency is required to report to the Office of the Privacy Commissioner in writing no later than [date] on steps it has taken to remedy the breach.]

If the Agency complies with this notice by [date] the Commissioner may cancel the notice in accordance with section 127.

If the Agency partially complies with this notice by [date] the Privacy Commissioner may vary the notice in accordance with section 127.

[*Add any further details considered useful*]

AGENCY'S RIGHT TO APPEAL THIS NOTICE

The Agency has the right to appeal this notice to the Human Rights Review Tribunal under section 131 of the Privacy Act 2020. The appeal can relate to the whole or part of this compliance notice.

An appeal must be lodged in the Human Rights Review Tribunal within 15 working days of service of this notice.

ENFORCEMENT OF THIS NOTICE

The Privacy Commissioner may bring enforcement proceedings in the Human Rights Review Tribunal if there is reason to believe that the Agency has not remedied the breach or will not remedy the breach, or if the Agency fails to report on steps taken to remedy the breach as required by this notice, provided that no appeal has been lodged within the statutory time limit.

PUBLICATION OF DETAILS OF THIS NOTICE

The Privacy Commissioner may publish details about the compliance notice or the breach that is the subject of the notice, including the identity of the Agency if the Commissioner believes it is desirable to do so in the public interest.

The Privacy Commissioner may publish a statement or comment about the breach if considered appropriate in the circumstances.

Issued at Wellington, New Zealand

by the Privacy Commissioner on [*date*]

_____

John Edwards
Privacy Commissioner

Contact Information

Office of the Privacy Commissioner: compliance@privacy.org.nz
Human Rights Review Tribunal: hrrt@justice.org.nz