

Comparing privacy laws:
GDPR v.
The Privacy Acts



About the authors

OneTrust DataGuidance™ provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

The OneTrust DataGuidance™ platform includes focused guidance around core topics (i.e. GDPR, data transfers, breach notification, among others), Cross-Border Charts which allow you to compare regulations across multiple jurisdictions at a glance, a daily customised news service and expert analysis.

These tools, along with our in-house analyst service to help with your specific research questions, provide a cost-effective and efficient solution to design and support your privacy programme.

Image production credits:

Cover/p.5/p.51: LysenkoAlexander / Essentials collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com

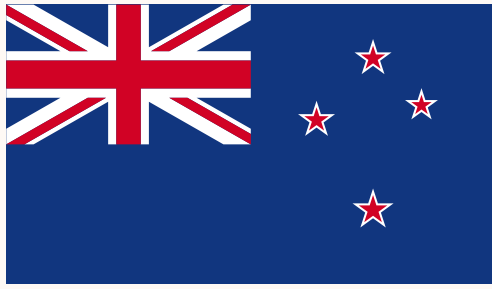
Scale key p6-49: enisaksoy / Signature collection / istockphoto.com

Icon p.33-40: AlexeyBlogoodf / Essentials collection / istockphoto.com

Icon p.47-51: cnythzl / Signature collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com

Table of contents

Introduction	5
1. Scope	
1.1. Personal scope	7
1.2. Territorial scope	11
1.3. Material scope	14
2. Key definitions	
2.1. Personal data	17
2.2. Pseudonymization	19
2.3. Controller and processors	20
2.4. Children	23
2.5. Research	24
3. Legal basis	26
4. Controller and processor obligations	
4.1. Data transfers	29
4.2. Data processing records	33
4.3. Data protection impact assessment	36
4.4. Data protection officer appointment	38
4.5. Data security and data breaches	40
4.6. Accountability	48
5. Individuals' rights	
5.1. Right to erasure	50
5.2. Right to be informed	56
5.3. Right to object	60
5.4. Right of access	63
5.5. Right not to be subject to discrimination	68
5.6. Right to data portability	69
6. Enforcement	
6.1. Monetary penalties	71
6.2. Supervisory authority	75
6.3. Civil remedies for individuals	84



Introduction

The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') came into effect on 25 May 2018, and governs the protection of personal data in EU and EEA Member States. Personal data protection in New Zealand is currently primarily regulated through the Privacy Act 1993 ('Privacy Act') and its 12 Information Privacy Principles ('IPPs'). However, on 26 June 2020, Parliament passed the Privacy Act 2020 ('Privacy Act 2020') which has a commencement date set for 1 December 2020. Amendments to the Privacy Bill on 3 June 2020 clarified matters such as liabilities, the potential for class action, enforcement powers, as well as mechanisms for data transfers such as binding schemes and prescribed countries. The Privacy Act established the Office of the Privacy Commissioner of New Zealand ('OPC'), which acts as the data protection authority in New Zealand, and is referred to as 'the Commissioner' within the Privacy Act and the Privacy Act 2020.

In a broad sense, the GDPR, the Privacy Act, and the Privacy Act 2020 provide similar approaches to personal data protection in terms of regulating, among other things, data collection and use, data subject rights, and data transfers. Nonetheless, neither the Privacy Act nor the Privacy Act 2020 establish consent as a main principle like the GDPR, nor do they address matters such as rights to erasure, object, data portability, sensitive data, children's data, or Data Protection Impact Assessments ('DPIA'). However, the Privacy Act and the Privacy Act 2020 both consider information sharing with public agencies and information matching agreements in much more detail than the GDPR. Overall, the Privacy Act 2020 will move the personal data protection framework in New Zealand into closer alignment with the GDPR by, for example, introducing data breach notification requirements.

This overview organises provisions from the GDPR, the Privacy Act, and the Privacy Act 2020 into key topics and sets them alongside each other to enable analysis and comparison. Each section begins with a detailing of principal information and a general introduction, as well as two consistency ratings comparing the GDPR against the Privacy Act and the GDPR against the Privacy Act 2020.


Structure and overview of the Guide


This Guide provides a comparison of the two legislative frameworks on the following key provisions:


1. Scope
2. Key definitions
3. Legal basis
4. Controller and processor obligations
5. Individuals' rights
6. Enforcement


Each topic includes relevant provisions from the two legislative legal frameworks, a summary of the comparison, and a detailed analysis of the similarities and differences between the GDPR and the Privacy Acts.

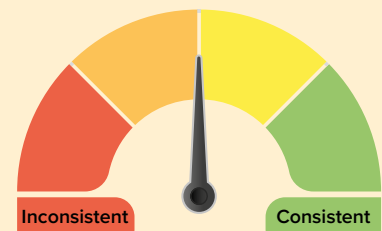
Key for giving the consistency rate

 **Consistent:** The GDPR and the Privacy Acts bear a high degree of similarity in the rationale, core, scope, and the application of the provision considered.

 **Fairly consistent:** The GDPR and the Privacy Acts bear a high degree of similarity in the rationale, core, and the scope of the provision considered, however, the details governing its application differ.

 **Fairly inconsistent:** The GDPR and the Privacy Acts bear several differences with regard to the scope and application of the provision considered, however, its rationale and core presents some similarities.

 **Inconsistent:** The GDPR and the Privacy Acts bear a high degree of difference with regard to the rationale, core, scope, and application of the provision considered.

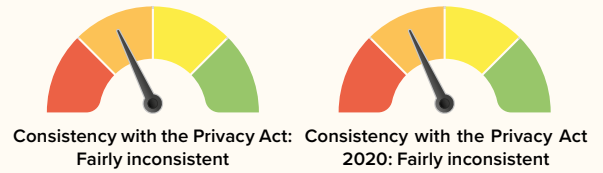


Usage of the Guide

This Guide is general and informational in nature, and is not intended to provide, and should not be relied on as a source of, legal advice. The information and materials provided in the Guide may not be applicable in all (or any) situations and should not be acted upon without specific legal advice based on particular circumstances.

1. Scope

1.1. Personal scope



While the GDPR, the Privacy Act, and the Privacy Act 2020 regulate the processing of personal information by private organisations and public bodies, there are significant differences between the pieces of legislation. For instance, unlike the GDPR, neither the Privacy Act nor the Privacy Act 2020 set out specific requirements for data processors. The Privacy Act 2020 would also introduce several new sections to clarify the personal scope of the Privacy Act, and particularly in relation to the location of individuals.

GDPR	Privacy Act	Privacy Act 2020
Data Controller		
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.	The Privacy Act applies to 'agencies' which, under Section 2(1), means 'any person or body of persons, whether corporate or unincorporate, and whether in the public sector or the private sector' with certain exceptions.	<p>The Privacy Act 2020 applies to 'agencies' which, under Section 8 means, with certain exceptions, '(i) an individual who is ordinarily resident in New Zealand; or (ii) a public sector agency; or (iii) a New Zealand private sector agency; or (iv) a court or tribunal, except in relation to its judicial functions'</p> <p>Under Section 7(1) a 'New Zealand private sector agency' means, 'a private sector agency that is an incorporated or unincorporated body and that — (a) is established under New Zealand law; or (b) has its central management and control in New Zealand.' Section 7 defines an 'overseas agency' as meaning 'an overseas person, body corporate, or unincorporated body that is not (a) a New Zealand agency; (b) the Government of an overseas country; (c) an overseas government entity to the extent that the entity is performing any public function on behalf of the overseas Government; or (d) a news entity, to the extent that it is carrying on news activities.'</p>

Data Processor

Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Section 3(4): For the purposes of this Act, where an agency holds information:

- (a) solely as agent;
- (b) for the sole purpose of safe custody; or
- (c) for the sole purpose of processing the information on behalf of another agency, and does not use or disclose the information for its own purposes, the information shall be deemed to be held by the agency on whose behalf that information is so held or, as the case may be, is so processed.

Section 11: (1) This Section applies if an agency (A) holds information as an agent for another agency (B) (for example, the information is held by A on behalf of B for safe custody or processing).

(2) For the purposes of this Act, the personal information is to be treated as being held by B, and not A.

(3) However, the personal information is to be treated as being held by A, as well as B if A uses or discloses the information for its own purposes.

(4) For the purposes of this Section, it does not matter whether A:

- (a) is outside New Zealand; or
- (b) holds the information outside New Zealand.

(5) To avoid doubt, if, under subsection (2), B is treated as holding personal information:

- (a) the transfer of the information to A by B is not a use or disclosure of the information by B; and
- (b) the transfer of the information, and any information derived from the processing of that information, to B by A is not a use or disclosure of the information by A.

Data Subject

Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Section 2(1): an 'individual' means a natural person, other than a deceased natural person; 'individual concerned,' in relation to personal information, means the individual to whom the information relates.

Section 7(1): an 'individual' means a natural person, other than a deceased natural person; 'individual concerned,' in relation to personal information, means the individual to whom the information relates.

Public Bodies

Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body.

Section 2(1): 'agency (a) means any person or body of persons, whether corporate or unincorporate, and whether in the public sector or the private sector; and, for the avoidance of doubt, includes a department; but (b) does not include:

- (i) the Sovereign;
- (ii) the Governor-General or the Administrator of the Government;
- (iii) the House of Representatives; or
- (iv) a member of Parliament in his or her official capacity;
- (v) the Parliamentary Service Commission;
- (vi) the Parliamentary Service, except in relation to personal information about any employee or former employee of that agency in his or her capacity as such an employee;
- (vii) in relation to its judicial functions, a court;
- (viii) in relation to its judicial functions, a tribunal;
- (ix) an Ombudsman;
- (x) a Royal Commission;
- (xi) a commission of inquiry appointed by an Order in Council made under the Commissions of Inquiry Act 1908;
- (xii) a commission of inquiry or board of inquiry or court of inquiry or committee of inquiry appointed, pursuant to, and not by, any provision of an Act, to inquire into a specified matter;
- (xiii) in relation to its news activities, any news medium; or
- (xiv) an inquiry to which Section 6 of the Inquiries Act 2013 applies.

Section 8: In this Act, New Zealand agency — (a) means — (i) an individual who is ordinarily resident in New Zealand; or (ii) a public sector agency; or (iii) a New Zealand private sector agency; or (iv) a court or tribunal, except in relation to its judicial functions; but (b) does not include — (i) the Sovereign; or

- (ii) the Governor-General or the Administrator of the Government; or
- (iii) the House of Representatives; or
- (iv) a member of Parliament in their official capacity; or
- (v) the Parliamentary Service Commission; or
- (vi) the Parliamentary Service, except in relation to personal information about any employee or former employee of the Parliamentary Service in their capacity as an employee; or
- (vii) an Ombudsman; or
- (viii) an inquiry; or
- (ix) a board of inquiry or court of inquiry appointed under any Act to inquire into a specified matter; or
- (x) a news entity, to the extent that it is carrying on news activities.

GDPR	Privacy Act	Privacy Act 2020
------	-------------	------------------

Nationality of Data Subject

Recital 14: The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.

The Privacy Act does not explicitly refer to its applicability in relation to the nationality of individuals.

The Privacy Act 2020 does not explicitly refer to its applicability in relation to the nationality of individuals.

Place of Residence

Recital 14: The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.

The Privacy Act does not explicitly refer to the place of residence of individuals.

Section 4: (1) This Act (except Section 212) applies to - (a) a New Zealand agency (A), in relation to any action taken by A (whether or not while A is, or was, present in New Zealand) in respect of personal information collected or held by A; (b) an overseas agency (B), in relation to any action taken by B in the course of carrying on business in New Zealand in respect of personal information collected or held by B; [...] (2) For the purposes of subsection (1)(a) and (b), it does not matter [...] (c) where the individual concerned is, or was, located.

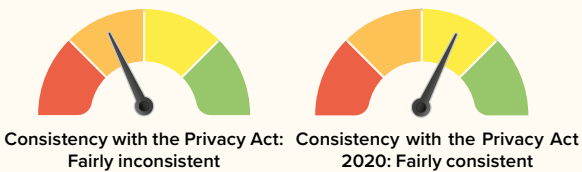
Deceased Individuals

Recital 27: This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.

Section 2(1): 'individual' means a natural person, other than a deceased natural person. 'Personal information' means information about an identifiable individual; and includes information relating to a death that is maintained by the Registrar-General pursuant to the Births, Deaths, Marriages, and Relationships Registration Act 1995, or any former Act (as defined by the Births, Deaths, Marriages, and Relationships Registration Act 1995).
Section 29(1): An agency may refuse to disclose any information requested pursuant to IPP 6 if (a) the disclosure of the information would involve the unwarranted disclosure of the affairs of another individual or of a deceased individual.

Section 7(1): 'individual' means a natural person, other than a deceased natural person.
Section 49: An agency may refuse access to any personal information requested if [...] (a) the disclosure of the information would involve the unwarranted disclosure of the affairs of [...] (ii) a deceased person.
Section 112: In this subpart, 'affected individual', in relation to personal information that is the subject of a privacy breach, [...] despite the definition of individual in section 7(1), includes a deceased person.

1.2. Territorial scope



The Privacy Act does not specify its territorial scope in the same level of detail as either the GDPR or the Privacy Act 2020. All three pieces of legislation do, however, apply to organisations within the jurisdiction while providing that some requirements may apply outside the jurisdiction. The Privacy Act 2020 is more aligned with the GDPR than the Privacy Act, and more explicitly addresses extraterritorial scope.

GDPR	Privacy Act	Privacy Act 2020
Establishment in Jurisdiction		
<p>Article 3: This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.</p> <p>Recital 22: Establishment implies the effective and real exercise of activity through stable arrangements.</p>	<p>The Privacy Act does not explicitly refer to agencies being established within New Zealand.</p>	<p>Section 4: (1) This Act (except Section 212) applies to (a) a New Zealand agency (A), in relation to any action taken by A (whether or not while A is, or was, present in New Zealand) in respect of personal information collected or held by A; (b) an overseas agency (B), in relation to any action taken by B in the course of carrying on business in New Zealand in respect of personal information collected or held by B; (c) an individual (C) who is not ordinarily resident in New Zealand, in relation to any action taken by C in respect of (i) personal information collected by C while present in New Zealand, regardless of where the information is subsequently held by C or where the individual to whom the information relates is, or was, located; (ii) personal information held by C while present in New Zealand (but not collected by C while present in New Zealand), regardless of where the individual to whom the information relates is, or was, located. [...] (3) For the purposes of subsection (1)(b), an agency may be treated as carrying on business in New Zealand without necessarily - (a) being a commercial operation; or (b) having a place of business in New Zealand; or (c) receiving any monetary payment for the supply of goods or services; or</p>

Establishment in Jurisdiction (cont'd)

(d) intending to make a profit from its business in New Zealand.

[Note: See Sections 7A and 7B in section 2.1. of this overview above.]

Extraterritorial

Recital 22: Establishment implies the effective and real exercise of activity through stable arrangements.

Section 10: (1) For the purposes of IPP 5 and IPPs 8 to 11, information held by an agency includes information that is held outside New Zealand by that agency, where that information has been transferred out of New Zealand by that agency or any other agency.
(2) For the purposes of IPPs 6 and 7, information held by an agency includes information held outside New Zealand by that agency.
(3) Nothing in this section shall apply to render an agency in breach of any of the IPPs in respect of any action that the agency is required to take by or under the law of any place outside New Zealand.

Section 4: (1) This Act (except Section 212) applies to [...] (b) an overseas agency (B), in relation to any action taken by B in the course of carrying on business in New Zealand in respect of personal information collected or held by B
For the purposes of subsection (1)(a) and (b), it does not matter — (a) where the personal information is, or was, collected by the agency; or (b) where the personal information is held by the agency; or (c) where the individual concerned is, or was, located.
(3) For the purposes of subsection (1)(b), an agency may be treated as carrying on business in New Zealand without necessarily — (a) being a commercial operation; or (b) having a place of business in New Zealand; or (c) receiving any monetary payment for the supply of goods or services; or (d) intending to make a profit from its business in New Zealand.

Goods and Services from Abroad

Recital 23: In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union

The Privacy Act does not refer to the provision of goods & services from abroad.

See Section 4A(3) above.

Goods and Services from Abroad (cont'd)

should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment.

Monitoring from Abroad

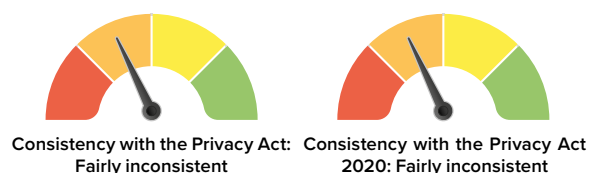
Recital 24: The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union.

The Privacy Act does not refer to monitoring from abroad.

The Privacy Act 2020 does not refer to monitoring from abroad.



1.3. Material scope



Unlike the GDPR, neither the Privacy Act nor the Privacy Act 2020 provide for special categories of data, such as sensitive data, address pseudonymised data or automated processing, or clearly define what types of data processing fall under their scope. The Privacy Act and the Privacy Act 2020, like the GDPR, however, provide general exemptions from obligations.

GDPR	Privacy Act	Privacy Act 2020
Personal Data/Personal Information		
Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Section 2(1): 'personal information' means information about an identifiable individual; and includes information relating to a death that is maintained by the Registrar-General pursuant to the Births, Deaths, Marriages, and Relationships Registration Act 1995, or any former Act (as defined by the Births, Deaths, Marriages, and Relationships Registration Act 1995).	Section 7(1): personal information (a) means information about an identifiable individual; and (b) includes information relating to a death that is maintained by the Registrar-General under the Births, Deaths, Marriages, and Relationships Registration Act 1995 or any former act (as defined in Section 2 of the Births, Deaths, Marriages, and Relationships Registration Act 1995).
Data Processing		
Article 4(2): 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.	The Privacy Act does not define data processing.	The Privacy Act 2020 does not define data processing.
Special Categories of Data		
Article 9(1): Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade	The Privacy Act does not differentiate special categories of data such as sensitive data.	The Privacy Act 2020 does not differentiate special categories of data such as sensitive data. However, Section 113(b) requires

Special Categories of Data (cont'd)

union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

that agencies that are assessing the potential harm of a privacy breach must consider 'whether the personal information is sensitive in nature.'

Anonymized Data

Recital 26: The principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

The Privacy Act does not explicitly refer to anonymised data. However, IPPs 2, 3, 10, and 11 on collecting information from individuals and limiting the use and disclosure of information, provide exceptions from general requirements where an agency believes, on reasonable grounds, that information 'will not be used in a form in which the individual concerned is identified.'

The Privacy Act 2020 does not explicitly refer to anonymised data. However, IPPs 2, 3, 10, and 11 on collecting information from individuals and limiting the use and disclosure of information, provide exceptions from general requirements where an agency believes, on reasonable grounds, that information 'will not be used in a form in which the individual concerned is identified.'

Pseudonymized Data

Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

The Privacy Act does not explicitly refer to pseudonymised data.

The Privacy Act 2020 does not explicitly refer to pseudonymised data.

Automated Processing

Article 2(1): This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

The Privacy Act does not differentiate automated and non-automated processing.

The Privacy Act 2020 does not differentiate automated and non-automated processing.

General Exemption

Article 2(2): This Regulation does not apply to the processing of personal data:

- (a) in the course of an activity which falls outside the scope of Union law;
- (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union; or
- (c) by a natural person in the course of a purely personal or household activity.

[See also Recital 26, above]

Section 54 provides an exemption from requirements for the OPC. Section 55 provides general exceptions to IPPs 6 and 7 on rights of access and correction.

Section 56: Nothing in the IPPs applies in respect of (a) the collection of personal information by an agency that is an individual; or (b) personal information that is held by an agency that is an individual, where that personal information is collected or held by that individual solely or principally for the purposes of, or in connection with, that individual's personal, family, or household affairs. (2) The exemption in subsection (1) ceases to apply once the personal information concerned is collected, disclosed, or used, if that collection, disclosure, or use would be highly offensive to an ordinary reasonable person. Section 57 exempts intelligence and security agencies from IPPs 2, 3, and 4(b).

Section 25: IPPs 1 to 4 apply only to personal information collected after 2 July 1993.

Section 26: (1) IPP 13(1) to (4)(a) does not apply to unique identifiers assigned before 1 July 1993. (2) However, IPP 13(2) applies to the assignment of a unique identifier on or after 1 July 1993 even if the unique identifier assigned is the same as that assigned by another agency before that date.

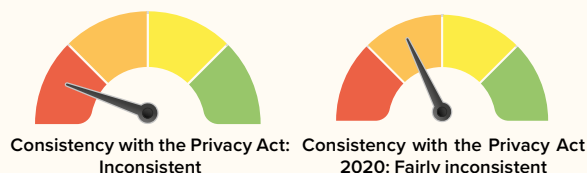
Section 27: (1) IPPs 1 to 3 and 4(b) do not apply to an agency if that agency (a) is an individual; and (b) is collecting personal information solely for the purposes of, or in connection with, the individual's personal or domestic affairs. (2) IPPs 5 to 12 do not apply to an agency if that agency (a) is an individual; and (b) is holding personal information that was collected by a lawful means solely for the purposes of, or in connection with, the individual's personal or domestic affairs. (3) However, the exemptions in subsections (1) and (2) do not apply if the collection, use, or disclosure of the personal information would be highly offensive to a reasonable person.

Section 28: IPPs 2, 3, and 4(b) 4(1)(b) do not apply to personal information collected by an intelligence and security agency.

Section 29: (1) IPPs 6 and 7 do not apply in respect of — (a) personal information during transmission by post, personal delivery, or electronic means. [Note: Sections 29 and 30 provide further exemptions in relation to administrative proceedings.]



2. Key definitions



2.1. Personal data

The Privacy Act 2020 provides a definition of 'personal information' that is closer to the GDPR's definition of 'personal data' than the Privacy Act. Neither the Privacy Act 2020 nor the Privacy Act, however, define special categories of data. While the Privacy Act 2020, the Privacy Act, and the GDPR all consider unique identifiers, they do so in different ways.

GDPR	Privacy Act	Privacy Act 2020
------	-------------	------------------

Personal Data/Personal Information

Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Section 2(1): 'personal information' means information about an identifiable individual; and includes information relating to a death that is maintained by the Registrar-General pursuant to the Births, Deaths, Marriages, and Relationships Registration Act 1995, or any former Act (as defined by the Births, Deaths, Marriages, and Relationships Registration Act 1995).

Section 7(1): personal information (a) means information about an identifiable individual; and (b) includes information relating to a death that is maintained by the Registrar-General under the Births, Deaths, Marriages, and Relationships Registration Act 1995 or any former act (as defined in Section 2 of the Births, Deaths, Marriages, and Relationships Registration Act 1995).

Special Categories of Data

Article 9(1): Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

The Privacy Act does not define special categories of data such as sensitive data.

The Privacy Act 2020 does not define special categories of data such as sensitive data. However, Section 113(b) requires that agencies that are assessing the potential harm of a privacy breach must consider 'whether the personal information is sensitive in nature.'

Online Identifiers

Recital 30: Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols,

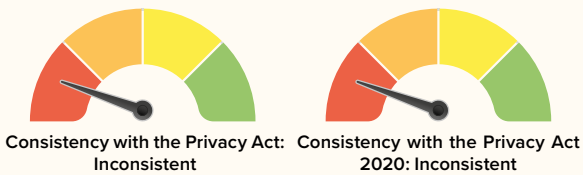
Section 2(1): 'unique identifier' means an identifier (a) that is assigned to an individual by an agency for the purposes of the operations of

Section 7(1): 'unique identifier', in relation to an individual, means an identifier other than the individual's name that uniquely identifies the individual.

Online Identifiers (cont'd)

such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.	the agency; and (b) that uniquely identifies that individual in relation to that agency; but, for the avoidance of doubt, does not include an individual's name used to identify that individual. [Note: See Section 6, IPP 12, for further information.]	[Note: See IPP 13, for further information.]
--	---	--

2.2. Pseudonymization



The GDPR defines anonymous information and pseudonymisation, while neither the Privacy Act nor the Privacy Act 2020 define either of these concepts.

GDPR	Privacy Act	Privacy Act 2020
Anonymization		

Recital 26: 'anonymous information' is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

The Privacy Act does not define 'anonymisation' or 'anonymous data.'

The Privacy Act 2020 does not define 'anonymisation' or 'anonymous data.'

Pseudonymization		
------------------	--	--

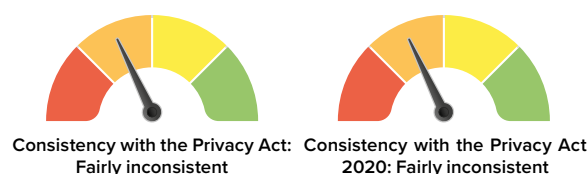
Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

The Privacy Act does not define 'pseudonymisation' or 'pseudonymised data.'

The Privacy Act 2020 does not define 'pseudonymisation' or 'pseudonymised data.'



2.3. Controllers and processors



Where the GDPR defines the concepts of 'data controllers' and 'data processors', the Privacy Act and the Privacy Act 2020 apply to the more broadly defined concept of 'agencies.' The Privacy Act and the Privacy Act 2020 do, however, establish where responsibility lies between parties.

GDPR	Privacy Act	Privacy Act 2020
Data Controller		
<p>Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.</p>	<p>The Privacy Act applies to 'agencies.'</p> <p>Section 2(1): (a) 'agency' means any person or body of persons, whether corporate or unincorporate, and whether in the public sector or the private sector; and, for the avoidance of doubt, includes a department; but (b) does not include (i) the Sovereign; (ii) the Governor-General or the Administrator of the Government; (iii) the House of Representatives; (iv) a member of Parliament in his or her official capacity; (v) the Parliamentary Service Commission; (vi) the Parliamentary Service, except in relation to personal information about any employee or former employee of that agency in his or her capacity as such an employee; (vii) in relation to its judicial functions, a court; (viii) in relation to its judicial functions, a tribunal; (ix) an Ombudsman; (x) a Royal Commission; (xi) a commission of inquiry appointed by an Order in Council made under the Commissions of Inquiry Act 1908; (xii) a commission of inquiry or board of inquiry or court of inquiry or committee of inquiry appointed, pursuant to, and not by, any provision of an Act, to inquire into a specified matter; (xiii) in relation to its news activities,</p>	<p>Section 7A: In this Act, New Zealand agency - (a) means — (i) an individual who is ordinarily resident in New Zealand; or (ii) a public sector agency; or (iii) a New Zealand private sector agency; or (iv) a court or tribunal, except in relation to its judicial functions; but (b) does not include - (i) the Sovereign; or (ii) the Governor-General or the Administrator of the Government; or (iii) the House of Representatives; or (iv) a member of Parliament in their official capacity; or (v) the Parliamentary Service Commission; or (vi) the Parliamentary Service, except in relation to personal information about any employee or former employee of the Parliamentary Service in their capacity as an employee; or (vii) an Ombudsman; or (viii) an inquiry; or (ix) a board of inquiry or court of inquiry appointed under any Act to inquire into a specified matter; or (x) a news entity, to the extent that it is carrying on news activities.</p> <p>Section 6B: In this Act, overseas agency means an overseas person, body corporate, or unincorporated body that is not (a) a New Zealand agency; (b) the Government of an overseas country;</p>

GDPR	Privacy Act	Privacy Act 2020
------	-------------	------------------

Data Controller (cont'd)

any news medium; or
(xiv) an inquiry to which Section 6 of the Inquiries Act 2013 applies.

(c) an overseas government entity to the extent that the entity is performing any public function on behalf of the overseas Government; or (d) a news entity, to the extent that it is carrying on news activities.

Data Processor

Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

The Privacy Act does not define 'data processor.'

The Privacy Act 2020 does not define 'data processor.'

Controller and Processor Contracts

Article 28(3): Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. [Article 28 goes on to stipulate necessary information to be included in such a contract.]

The Privacy Act does not directly refer to agency and processor agreements. Section 3(4): For the purposes of this Act, where an agency holds information (a) solely as agent; (b) for the sole purpose of safe custody; or (c) for the sole purpose of processing the information on behalf of another agency, and does not use or disclose the information for its own purposes, the information shall be deemed to be held by the agency on whose behalf that information is so held or, as the case may be, is so processed.

The Privacy Act 2020 does not directly refer to agency and processor agreements. Section 11: (1) This Section applies if an agency (A) holds information as an agent for another agency (B) (for example, the information is held by A on behalf of B for safe custody or processing). (2) For the purposes of this Act, the personal information is to be treated as being held by B, and not A. (3) However, the personal information is to be treated as being held by A, as well as B if A uses or discloses the information for its own purposes. (4) For the purposes of this section, it does not matter whether A (a) is outside New Zealand; or (b) holds the information outside New Zealand. (5) To avoid doubt, if, under subsection (2), B is treated as holding personal information, (a) the transfer of the information to A by B is not a use or disclosure of the information by B; and (b) the transfer of the information, and any information derived from the processing of that information, to B by A is not a use or disclosure of the information by A.

GDPR	Privacy Act	Privacy Act 2020
------	-------------	------------------

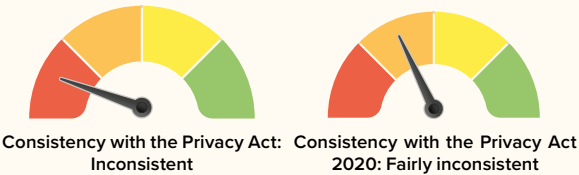
Data Protection Impact Assessment (DPIA)
--

DPIA is not specifically defined, however Article 35 sets out requirements for DPIAs (see section 4.3. for further information).	The Privacy Act does not refer to DPIA.	The Privacy Act 2020 does not refer to DPIA.
--	---	--

Data Protection Officer (DPO)

DPO is not specifically defined, however Article 37 sets out requirements related to DPOs (see section 5.4. below for further information).	DPO is not specifically defined, however Section 23 sets out requirements related to privacy officers (see section 5.4. below for further information).	DPO is not specifically defined, however Section 201 sets out requirements related to privacy officers (see section 5.4. below for further information).
---	---	--

2.4. Children



The Privacy Act does not refer to children's personal information. The Privacy Act 2020 would introduce a broad prescription to take children's and young person's vulnerability into account, but, unlike the GDPR, the Privacy Act 2020 does not provide more specific requirements.

GDPR	Privacy Act	Privacy Act 2020
Children definition		
<p>The GDPR does not specifically define 'child'. However, Article 8(1) provides: Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.</p>	<p>The Privacy Act does not refer to children.</p>	<p>The Privacy Act 2020 does not define or provide an age threshold for children. However, Section 22, IPP 4 provides: 'An agency may collect personal information only — (a) by a lawful means; and (b) by a means that, in the circumstances of the case (particularly in circumstances where personal information is being collected from children or young persons), — (i) is fair; and (ii) does not intrude to an unreasonable extent upon the personal affairs of the individual concerned'</p>
Consent for Processing Children's Data		
<p>Article 8(2): The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.</p>	<p>The Privacy Act does not refer to children.</p>	<p>The Privacy Act 2020 does not refer to children beyond IPP 4 as noted above.</p>
Privacy Notice		
<p>Recital 58: Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.</p>	<p>The Privacy Act does not refer to children.</p>	<p>The Privacy Act 2020 does not refer to children beyond IPP 4 as noted above.</p>

2.5. Research



Consistency with the Privacy Act: Fairly consistent Consistency with the Privacy Act 2020: Fairly consistent

While neither the Privacy Act nor the Privacy Act 2020 provide definitions of processing for research purposes, they do establish relevant exemptions that are comparable to the GDPR. In addition, all three pieces of legislation enable further processing for research purposes.

GDPR	Privacy Act	Privacy Act 2020
------	-------------	------------------

Scientific/Historial Research Definition

<p>Recital 159: Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research.</p> <p>Recital 160: Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.</p>	<p>While the Privacy Act does not provide definitions for 'research purposes' Section 6 does provide exemptions where an agency believes on reasonable grounds that information 'will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned' from IPPs 2, 3, 10, and 11 which regulate collecting information directly from a concerned individual, providing certain information to the individual, limits on the use of information, and limits on the disclosure of information, respectively.</p>	<p>While the Privacy Act 2020 does not provide definitions for 'research purposes' Section 22 does provide exemptions where an agency believes on reasonable grounds that information 'will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned' from IPPs 2, 3, 10, 11, and 13 which regulate collecting information directly from a concerned individual, providing certain information to the individual, limits on the use of information, limits on the disclosure of information, and assignment of unique identifiers respectively.</p>
--	---	--

Compatability with Original Purpose of Collection

<p>Article 5(1)(b): Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').</p>	<p>Section 6, IPP 10: (1) An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds, [...] (f) that the information [...] (ii) is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.</p>	<p>Section 22, IPP 10: (1) An agency that holds personal information that was obtained in connection with one purpose may not use the information for any other purpose unless the agency believes, on reasonable grounds, [...] (b) that the information [...] (ii) is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.</p>
---	--	---

Appropriate Safeguards

Article 89(1): Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner.

The Privacy Act does not refer to appropriate safeguards specifically in relation to processing for research purposes. [Note: Section 6, IPP 5 requires that agencies ensure that information is protected by 'security safeguards as it is reasonable in the circumstances to take.']

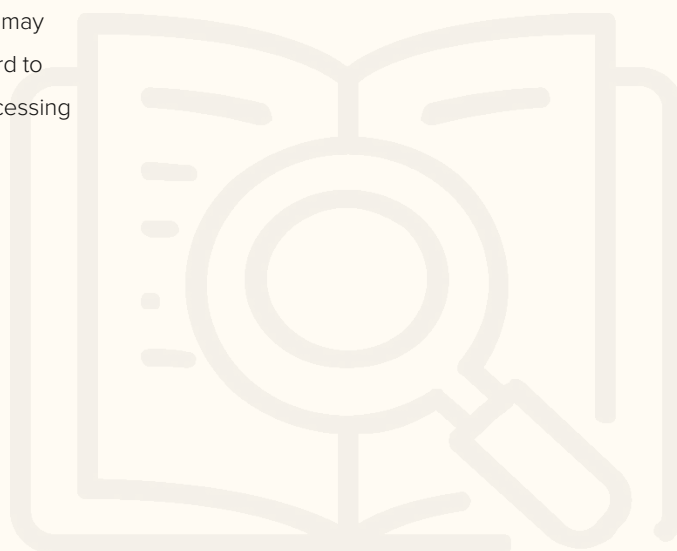
The Privacy Act 2020 does not refer to appropriate safeguards specifically in relation to processing for research purposes. [Note: Section 22, IPP 5 requires that agencies ensure that information is protected by 'security safeguards as are reasonable in the circumstances to take.']

Data Subject Rights (Research)

Under Article 17(3), the right to erasure may not apply in cases of scientific or historical research. Article 21(6), however, provides that data subjects may exercise the right to object to data processing for scientific or historical research purposes. In addition, Article 89 provides that Member States may derogate from the GDPR in regard to data subject rights and data processing for research purposes.

The Privacy Act does refer specifically to data subject rights in relation to processing for research purposes.

The Privacy Act 2020 does refer specifically to data subject rights in relation to processing for research purposes.



3. Legal basis



Consistency with the Privacy Act:
Fairly inconsistent



Consistency with the Privacy Act
2020: Fairly inconsistent

Rather than outlining a set of legal grounds for processing personal information, in the manner of the GDPR, the Privacy Act and the Privacy Act 2020 set out a series of IPPs that must be followed. These IPPs regulate purposes of information collection, sources of information, informing concerned individuals, the manner of collection, storage and security, access, correction, accuracy, and retention of information, limits on use and disclosure of information, and unique identifiers (see Section 6 of the Privacy Act and Section 22 of the Privacy Act 2020).

GDPR	Privacy Act	Privacy Act 2020
------	-------------	------------------

Legal Grounds

Article 6(1): Processing shall be lawful only if and to the extent that at least one of the following applies:

- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Section 6: IPP 1 Personal information shall not be collected by any agency unless

- (a) the information is collected for a lawful purpose connected with a function or activity of the agency; and
- (b) the collection of the information is necessary for that purpose.

Section 22, IPP 1: (1) Personal information shall not be collected by any agency unless:

- (a) the information is collected for a lawful purpose connected with a function or activity of the agency; and
- (b) the collection of the information is necessary for that purpose.

(2) If the lawful purpose for which personal information about an individual is collected does not require the collection of an individual's identifying information, the agency may not require the individual's identifying information.

GDPR	Privacy Act	Privacy Act 2020
------	-------------	------------------

Sensitive Data (Legal Basis)

There are specific requirements for processing special categories of data, see Article 9 of the GDPR for further information.	The Privacy Act does not specify alternative legal bases for processing sensitive data.	The Privacy Act 2020 does not specify alternative legal bases for processing sensitive data.
---	---	--

Conditions for Consent

<p>Article 7(3): The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.</p> <p>Article 4: (11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.</p>	<p>The Privacy Act does not define conditions for consent.</p>	<p>The Privacy Act 2020 does not define conditions for consent.</p>
---	--	---

Journalism/Artistic Purposes

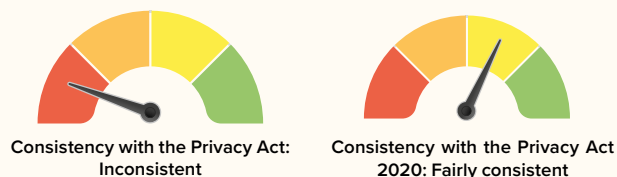
<p>Article 85(1): Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.</p>	<p>Section 2(1): agency [...] (b) does not include [...] (xiii) in relation to its news activities, any news medium. [...] 'news activity' means (a) the gathering of news, or the preparation or compiling of articles or programmes of or concerning news, observations on news, or current affairs, for the purposes of dissemination to the public or any section of the public; (b) the dissemination, to the public or any section of the public, of any article or programme of or concerning (i) news; (ii) observations on news; (iii) current affairs. 'news medium' means any agency whose business, or part of whose business, consists of a news activity;</p>	<p>Sections 7A and 7B (see section 3.3 above) note that the terms 'agency' and 'overseas agency' do not include 'a news entity, to the extent that it is carrying on news activities.'</p>
--	---	--

Journalism/Artistic Purpose (cont'd)

but, in relation to IPPs 6 and 7, does
not include Radio New Zealand Limited
or Television New Zealand Limited.



4. Controller and processor obligations



4.1. Data transfers

The Privacy Act differs from both the GDPR and the Privacy Act 2020 in that it provides relatively limited provisions on international data transfers and only broadly covers disclosure of personal information. The Privacy Act 2020 will introduce a new IPP that would establish alternative mechanisms for international data transfers, including binding schemes that are comparable with those under the GDPR.

GDPR	Privacy Act	Privacy Act 2020
Adequate Protection		
Article 45(1): A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.	Section 114B: (1) The Commissioner may prohibit a transfer of personal information from New Zealand to another State if the Commissioner is satisfied, on reasonable grounds, that (a) the information has been, or will be, received in New Zealand from another State and is likely to be transferred to a third State where it will not be subject to a law providing comparable safeguards to this Act; and (b) the transfer would be likely to lead to a contravention of the basic IPPs of national application set out in Part Two of the OECD Guidelines and set out in Schedule 5A.	Section 22, IPP 12: (1) An agency (A) may disclose personal information to a foreign person or entity (B) in reliance on IPP 11(1)(a), (c), (e), (f), (h), or (i) only if (a) the individual concerned authorises the disclosure to B after being expressly informed by A that B may not be required to protect the information in a way that, overall, provides comparable safeguards to those in this Act; (b) B is carrying on business in New Zealand and, in relation to the information, A believes on reasonable grounds that B is subject to this Act; (c) A believes on reasonable grounds that B is subject to privacy laws that, overall, provide comparable safeguards to those in this Act; (d) A believes on reasonable grounds that B is a participant in a prescribed binding scheme; (e) A believes on reasonable grounds that B is subject to privacy laws of a prescribed country; or (f) A otherwise believes on reasonable grounds that B is required to protect the information in a way that, overall, provides

Adequate Protection (cont'd)

comparable safeguards to those in this Act (for example, pursuant to an agreement entered into between A and B).

(2) However, subclause (1) does not apply if the personal information is to be disclosed to B in reliance on IPP 11(1)(e) or (f) and it is not reasonably practicable in the circumstances for A to comply with the requirements of subclause (1).

(3) In this principle IPP, - 'prescribed binding scheme' means a binding scheme specified in regulations made under Section 214

'prescribed country' means a country specified in regulations made under Section 214. Section 214: (1) The Governor-General may, by Order in Council made on the recommendation of the responsible Minister given after consultation with the Commissioner, make regulations prescribing countries for the purpose of IPP 12(1)(e).

(2) The Minister may recommend the making of regulations under subsection (1) only if the Minister is satisfied that the countries have privacy laws that, overall, provide comparable safeguards to those in this Act.

(3) A country may be prescribed subject to any specified limitation or qualification relating to —

- (a) the type of foreign person or entity in that country that personal information may be disclosed to;
- (b) the type of personal information that may be disclosed to a foreign person or entity in that country.

Other Mechanisms for Data Transfers

Article 46(1): In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

(2) The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

- (a) a legally binding and enforceable instrument between public authorities or bodies;
- (b) binding corporate rules in accordance with Article 47;
- (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
- (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
- (e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- (f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

Section 6, IPP 11: An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds, (a) that the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or

(b) that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to disclose the information; or

(c) that the disclosure is to the individual concerned; or

(d) that the disclosure is authorised by the individual concerned; or

(e) that non-compliance is necessary (i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences;

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(f) that the disclosure of the information is necessary to prevent or lessen a serious threat (as defined in Section 2(1)) to (i) public health or public safety; or

(ii) the life or health of the individual concerned or another individual; or

(fa) that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions;

See IPP 12 above.

Section 214: (1) The Governor-General may, by Order in Council made on the recommendation of the responsible Minister given after consultation with the Commissioner, make regulations prescribing binding schemes for the purpose of IPP 12(1)(d).

(2) The Minister may recommend the making of regulations under subsection (1) only if the Minister is satisfied that the binding schemes require a foreign person or entity to protect personal information in a way that, overall, provides comparable safeguards to those in this Act.

Section 22, IPP 11: (1) An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds, - (a) that the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or

(b) that the disclosure is to the individual concerned; or

(c) that the disclosure is authorised by the individual concerned; or

(d) that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to disclose the information; or

(e) that the disclosure of the information is necessary -

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution,

Other Mechanisms for Data Transfers (cont'd)

(3) Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

(g) that the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern; or

(h) that the information (i) is to be used in a form in which the individual concerned is not identified; or

(ii) is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(i) that the disclosure of the information is in accordance with an authority granted under Section 54.

and punishment of offences; or

(ii) for the enforcement of a law that imposes a pecuniary penalty; or

(iii) for the protection of public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(f) that the disclosure of the information is necessary to prevent or lessen a serious threat to —

(i) public health or public safety; or

(ii) the life or health of the individual concerned or another individual; or

(g) that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions; or

(h) that the information -

(i) is to be used in a form in which the individual concerned is not identified; or

(ii) is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(i) that the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern.

(2) This principle IPP is subject to IPP 12.

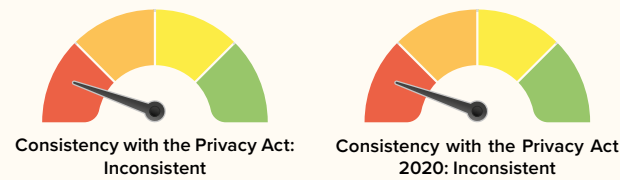
Data Localization

Not applicable.

Not applicable.

Not applicable.

4.2. Data processing records



Unlike the GDPR, neither the Privacy Act nor the Privacy Act 2020 set out clear data processing record requirements.

GDPR	Privacy Act	Privacy Act 2020
Data Controller Obligation		
<p>Article 30(1): Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:</p> <p>(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;</p> <p>(b) the purposes of the processing;</p> <p>(c) a description of the categories of data subjects and of the categories of personal data;</p> <p>(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;</p> <p>(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;</p> <p>(f) where possible, the envisaged time limits for erasure of the different categories of data; and</p> <p>(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).</p>	<p>The Privacy Act does not specify data processing record requirements. In general terms, it provides under Section 6, IPP 5:</p> <p>An agency that holds personal information shall ensure (a) that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against</p> <p>(i) loss; and</p> <p>(ii) access, use, modification, or disclosure, except with the authority of the agency that holds the information; and</p> <p>(iii) other misuse; and</p> <p>(b) that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.</p>	<p>The Privacy Act 2020 does not specify data processing record requirements. In general terms, it provides under Section 22, IPP 5:</p> <p>An agency that holds personal information shall ensure (a) that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against</p> <p>(i) loss; and</p> <p>(ii) access, use, modification, or disclosure, except with the authority of the agency that holds the information; and</p> <p>(iii) other misuse; and</p> <p>(b) that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.</p>

GDPR	Privacy Act	Privacy Act 2020
------	-------------	------------------

Data Processor Obligation

Article 30(2): Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

- (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
- (b) the categories of processing carried out on behalf of each controller;
- (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; and
- (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

The Privacy Act does not specify data processing record requirements.

The Privacy Act 2020 does not specify data processing record requirements.

Records Format

Article 30(3): The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

The Privacy Act does not specify data processing record requirements.

The Privacy Act 2020 does not specify data processing record requirements.

Required to Make Available

Article 30(4): The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

Section 91(4): The Commissioner may from time to time, by notice in writing, require any person who in the Commissioner's opinion is able to give information relevant to an investigation being conducted by the Commissioner under

Section 87: (1) At any time during an investigation, the Commissioner may, by notice, require any person to provide (a) any information in the person's possession, or under the person's control, that the

GDPR	Privacy Act	Privacy Act 2020
------	-------------	------------------

Required to Make Available		
----------------------------	--	--

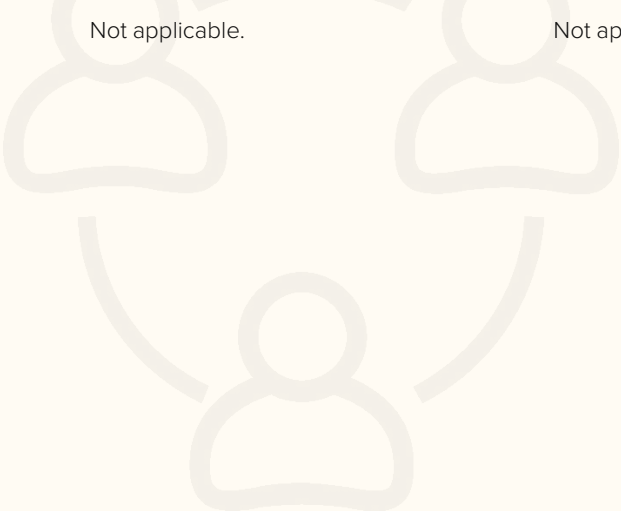
	<p>Part 8, or an inquiry being carried out by the Commissioner under Section 13(1) (m), to furnish such information, and to produce such documents or things in the possession or under the control of that person, as in the opinion of the Commissioner are relevant to the subject matter of the investigation or inquiry.</p>	<p>Commissioner considers may be relevant to the investigation; (b) any documents or things in the person's possession, or under the person's control, that the Commissioner considers may be relevant to the investigation.</p>
--	---	--

Exemptions		
------------	--	--

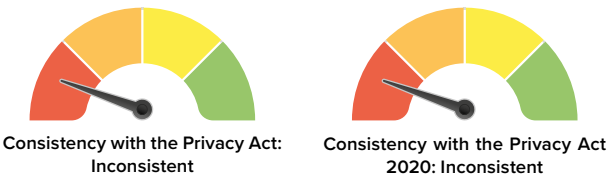
<p>Article 30(5): The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.</p>	<p>Not applicable.</p>	<p>Not applicable.</p>
---	------------------------	------------------------

General Data Processing Notification		
--------------------------------------	--	--

<p>Not applicable.</p>	<p>Not applicable.</p>	<p>Not applicable.</p>
------------------------	------------------------	------------------------



4.3. Data protection impact assessment



Neither the Privacy Act nor the Privacy Act 2020 provide for data protection or privacy impact assessments. The OPC has recommended such assessments in non-binding guidance. See New Zealand – Privacy Impact Assessment for further information.

GDPR	Privacy Act	Privacy Act 2020
------	-------------	------------------

When is a DPIA Required

Article 35(1): Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

[...] (3) A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

The Privacy Act does not refer to DPIA.

The Privacy Act 2020 does not refer to DPIA.

DPIA Content Requirements

Article 35(7): The assessment shall contain at least:

- (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
- (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

The Privacy Act does not refer to DPIA.

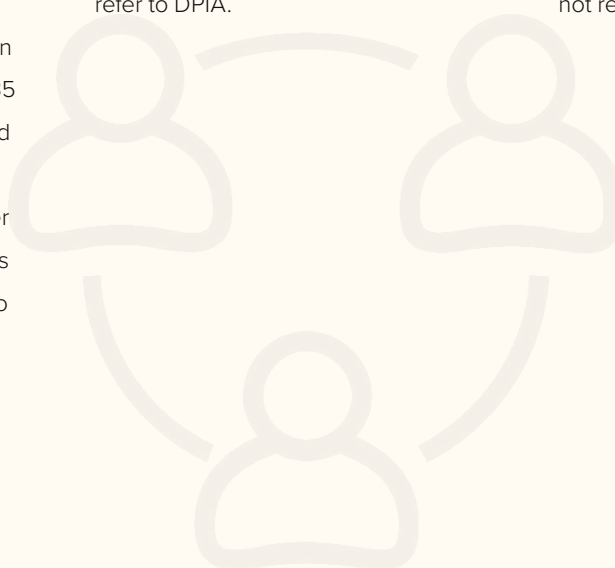
The Privacy Act 2020 does not refer to DPIA.

Consultation with Authority

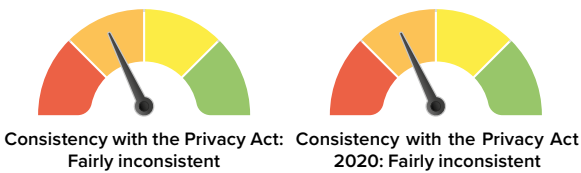
Article 36(1): The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. [Article 36 goes on to detail requirements related to such prior consultation].

The Privacy Act does not refer to DPIA.

The Privacy Act 2020 does not refer to DPIA.



4.4. Data protection officer appointment



While both the Privacy Act and the Privacy Act 2020 provide broad requirements for the appointment of privacy officers, this role and associated obligations are significantly less defined than under the GDPR. The OPC has released relevant, non-binding guidance (see New Zealand – Data Protection Officer Appointment).

GDPR	Privacy Act	Privacy Act 2020
DPO Tasks		
<p>Article 39(1): The data protection officer shall have at least the following tasks:</p> <p>(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;</p> <p>(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;</p> <p>(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;</p> <p>(d) to cooperate with the supervisory authority; and</p> <p>(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.</p>	<p>Section 23: It shall be the responsibility of each agency to ensure that there are, within that agency, 1 or more individuals whose responsibilities include (a) the encouragement of compliance, by the agency, with the IPPs;</p> <p>(b) dealing with requests made to the agency pursuant to this Act;</p> <p>(c) working with the Commissioner in relation to investigations conducted pursuant to Part 8 in relation to the agency;</p> <p>(d) otherwise ensuring compliance by the agency with the provisions of this Act.</p>	<p>Section 201: (1) An agency must appoint as privacy officers for the agency one or more individuals (within or outside the agency) whose responsibilities include (a) encouraging the agency to comply with the IPPs;</p> <p>(b) dealing with requests made to the agency under this Act;</p> <p>(c) working with the Commissioner in relation to investigations conducted under Part 5 in relation to the agency;</p> <p>(d) ensuring that the agency complies with the provisions of this Act.</p> <p>(2) Subsection (1) does not apply to an agency that is an individual who is collecting and holding personal information solely for the purposes of, or in connection with, the individual's personal or domestic affairs.</p>

When is a DPO Required

Article 37(1): The controller and the processor shall designate a data protection officer in any case where:

- (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

See Section 23 above.

See Section 201 above.

[Note: Section 3 of the Privacy Act 2020 provides that, 'Any person who immediately before the commencement day was a privacy officer under Section 23 of the Privacy Act continues on and after that day as a privacy officer under Section 201 of this Act.']

Group Appointments

Article 37(2): A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

The Privacy Act does not refer to group appointments of privacy officers.

The Privacy Act 2020 does not refer to group appointments of privacy officers.

Notification of DPO

Article 37(7): The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

The Privacy Act does not require notification of privacy officers to the OPC.

The Privacy Act 2020 does not require notification of privacy officers to the OPC.

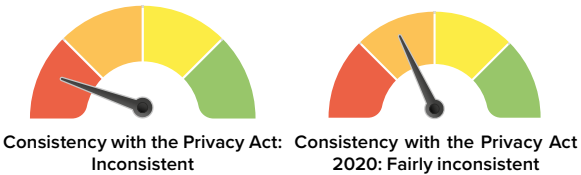
Qualifications

Article 37(5): The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

The Privacy Act does not refer to the qualifications of privacy officers.

The Privacy Act 2020 does not refer to the qualifications of privacy officers.

4.5. Data security and data breaches



Currently, there are currently no mandatory breach notification requirements in New Zealand under the Privacy Act, however the Privacy Act 2020 will introduce significant obligations. Although the Privacy Act 2020 is less specific than the GDPR on certain matters, such as a timeframe for notifying authorities of data breaches, in general terms, the Privacy Act 2020 sets out more comprehensive data breach-related provisions.

GDPR	Privacy Act	Privacy Act 2020
------	-------------	------------------

Security Measures Defined

<p>Article 32(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:</p> <p>(a) the pseudonymisation and encryption of personal data;</p> <p>(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;</p> <p>(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;</p> <p>(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.</p>	<p>Section 6, IPP 5: An agency that holds personal information shall ensure (a) that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against (i) loss; and</p> <p>(ii) access, use, modification, or disclosure, except with the authority of the agency that holds the information; and</p> <p>(iii) other misuse; and</p> <p>(b) that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.</p>	<p>Section 22, IPP 5: An agency that holds personal information shall ensure (a) that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against (i) loss; and</p> <p>(ii) access, use, modification, or disclosure, except with the authority of the agency that holds the information; and</p> <p>(iii) other misuse; and</p> <p>(b) that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.</p>
--	---	--

Data Breach Notification to Authority

<p>Article 33(1): In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after</p>	<p>The Privacy Act does not require mandatory data breach notifications.</p>	<p>Section 112(1): 'notifiable data breach' means (a) means a privacy breach that it is reasonable to believe has caused serious harm to an affected</p>
--	--	--

Data Breach Notification to Authority (cont'd)

having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

individual or individuals or is likely to do so (see Section 112A for factors that must be considered by an agency when assessing whether a privacy breach is likely to cause serious harm); but (b) does not include a privacy breach if the personal information that is the subject of the breach is held by an agency who is an individual and the information is held solely for the purposes of, or in connection with, the individual's personal or domestic affairs. Section 113: When an agency is assessing whether a privacy breach is likely to cause serious harm in order to decide whether the breach is a notifiable privacy breach, the agency must consider the following: (a) any action taken by the agency to reduce the risk of harm following the breach; (b) whether the personal information is sensitive in nature; (c) the nature of the harm that may be caused to affected individuals; (d) the person or body that has obtained or may obtain personal information as a result of the breach (if known); (e) whether the personal information is protected by a security measure; (f) any other relevant matters.

Timeframe for Breach Notification

See Article 33(1) above.

The Privacy Act does not require mandatory data breach notifications.

Section 114: An agency must notify the Commissioner as soon as practicable after becoming aware that a notifiable privacy breach has occurred.

Notifying Data Subjects of Data Breach

Article 34(1): When the personal data breach is likely to result in a high risk to the rights and freedoms of natural

The Privacy Act does not require mandatory data breach notifications to data subjects.

Section 115: (1) An agency must notify an affected individual as soon as practicable after becoming aware that a notifiable

Notifying Data Subjects of Data Breach (cont'd)

persons, the controller shall communicate the personal data breach to the data subject without undue delay.

privacy breach has occurred, unless subsection (2) or an exception in Section 116 applies or a delay is permitted under Section 116(4).
 (2) If it is not reasonably practicable to notify an affected individual or each member of a group of affected individuals, the agency must instead give public notice of the privacy breach, unless an exception in Section 116 applies or a delay is permitted under Section 116(4).
 (3) Public notice must be given (a) in a form in which no affected individual is identified; and (b) in accordance with any regulations made under Section 215(1)(a).
 (4) If subsection (2) or an exception in Section 120 is relied on, the agency must notify the affected individual or individuals at a later time if (a) circumstances change so that subsection (2) or the exception no longer applies; and (b) at that later time, there is or remains a risk that the privacy breach will cause serious harm to the affected individual or individuals.
 (5) A failure to notify an affected individual or give public notice under this section may be an interference with privacy under this Act (see Section 69(2)(a)(iv)).

Data Processor Notification of Data Breach

Article 33(2): The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

The Privacy Act does not require mandatory data breach notifications.

Section 121: [...] (3) Subsection (4) applies to processes and proceedings under this Act relating to the obligations under Section 114 or 115.
 (4) Anything relating to a notifiable privacy breach that is known by an agent is to be treated as being known by the principal agency.

Data Processor Notification of Data Breach (cont'd)

Section 120: (1) This Section applies to processes and proceedings under this Act relating to the obligations under Section 114 or 115.

(2) An employee or a member of an agency is not liable in those processes or proceedings if anything done or omitted by them results in the employer or agency failing to notify the Commissioner or an affected person (or their representative) or give public notice of a notifiable privacy breach.

(3) For the purpose of those processes and proceedings, anything done or omitted by an employee or a member of an agency is to be treated as being done or omitted by the employer or agency.

(4) For the purpose of those processes and proceedings, anything done or omitted by an agent of another agency is to be treated as being done or omitted by both the agent and the principal agency.

(5) However, the extent of liability of an agent is affected by whether they hold personal information that is the subject of a notifiable privacy breach. See the definition of privacy breach in Section 112 and see Section 11, which applies and which provides that information held by an agent is to be treated as being held by the principal agency unless Section 11(3) applies.

Exceptions

Article 34(3): The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were

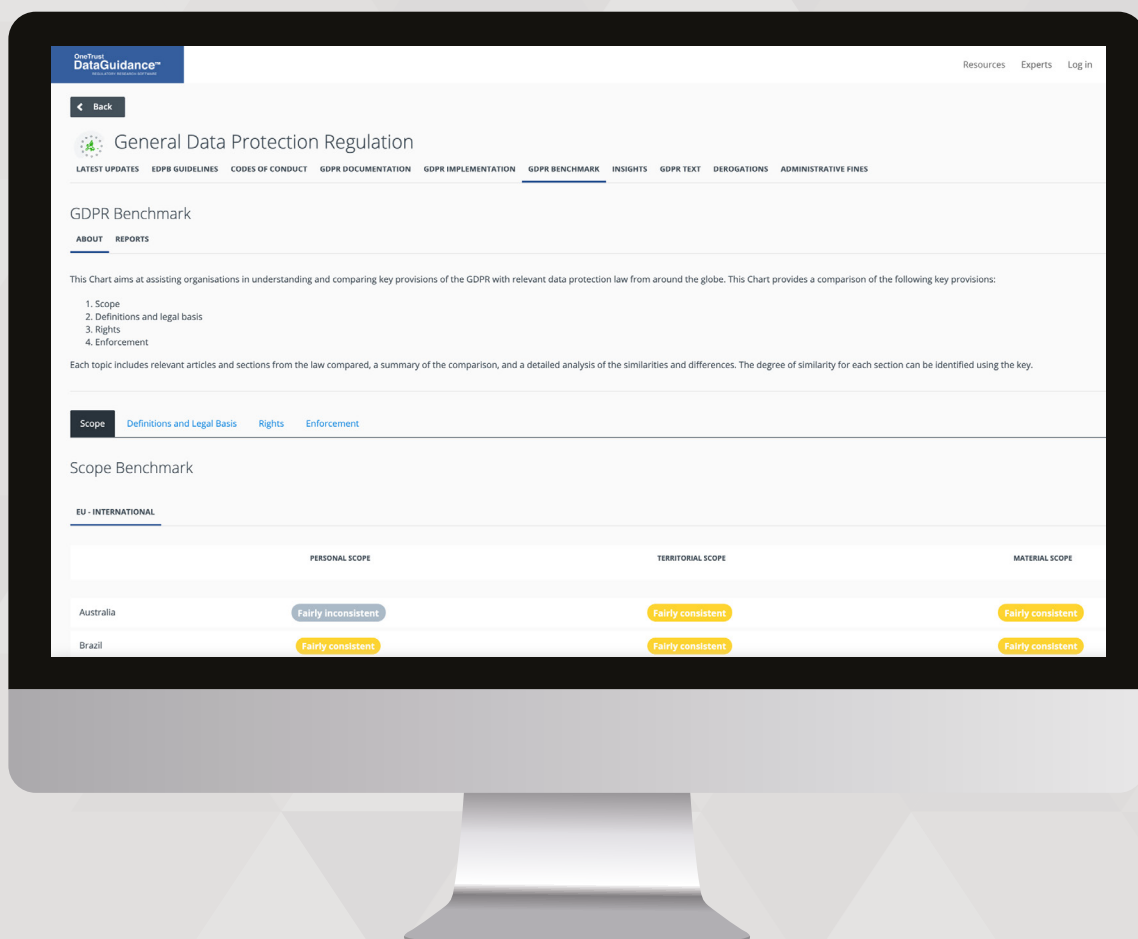
Not applicable.

Section 116: (1) An agency is not required to notify an affected individual or give public notice of a notifiable privacy breach if the agency believes that the notification or notice would be likely to (a) prejudice the security or defence of New Zealand or the international relations

Global Regulatory Research Software

40 In-House Legal Researchers, 500 Lawyers
Across 300 Jurisdictions

Monitor regulatory developments, mitigate risk,
and achieve global compliance



OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE

Build a global privacy program by comparing key legal frameworks against the GDPR

CCPA | Russia | Thailand | Brazil | Japan | China
and 20+ other global laws & frameworks

Understand and compare key provisions of the GDPR with relevant data protection laws from around the globe

The GDPR Benchmarking tool provides comparison of the various pieces of legislation on the following key provisions



Scope



Rights



Definitions and legal basis



Enforcement

- Employ topic specific guidance to develop your compliance activities
- Monitor news and access written opinion pieces on the most recent developments

Start your free trial at
www.dataguidance.com

Exemptions (cont'd)

applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

of the Government of New Zealand;

(b) prejudice the maintenance of the law by any public sector agency, including the prevention, investigation, and detection of offences, and the right to a fair trial;

(c) endanger the safety of any person; or

(d) reveal a trade secret.

(2) An agency is not required to notify an affected individual or give public notice (relating to a particular individual) of a notifiable privacy breach (a) if the individual is under the age of 16 and the agency believes that the notification or notice would be contrary to that individual's interests; or

(b) if, after consultation is undertaken by the agency with the individual's health practitioner (where practicable), the agency believes that the notification or notice would be likely to prejudice the health of the individual.

(3) If subsection (2) applies, the agency must (a) consider whether it would be appropriate to notify a representative instead of the individual (if a representative is known or can be readily identified); and

(b) before deciding whether to notify a representative, take into account the circumstances of both the individual and the privacy breach; and

(c) if the agency decides it is appropriate to notify a representative and has identified a representative, notify that person.

(4) An agency may delay notifying an affected individual or giving public notice of a notifiable privacy breach (but not delay notifying the Commissioner) only (a) if the agency believes that a delay is necessary

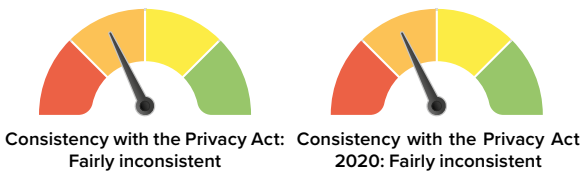
Exemptions (cont'd)

because notification or public notice may have risks for the security of personal information held by the agency and those risks outweigh the benefits of informing affected individuals; and (b) for a period during which those risks continue to outweigh those benefits.

(5) An agency may rely on an exception, or delay in notifying affected individuals or giving public notice, under this section and, in relation to a delay, do so for the period referred to in subsection (4)(b), only if the agency believes on reasonable grounds that the exception applies, the ground for delay exists, or the circumstances referred to in subsection (4)(b) continue to exist.



4.6. Accountability



Unlike the GDPR, neither the Privacy Act nor the Privacy Act 2020 define a principle of accountability, however they both contain relevant provisions and specify certain liabilities.

GDPR	Privacy Act	Privacy Act 2020
Principle of Accountability		
Article 5(2): The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability'). [Paragraph 1 details principles of: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality.]	While the Privacy Act does not contain a specific accountability principle, certain provisions may be considered to ensure the same, such as privacy officers ensuring compliance.	While the Privacy Act 2020 does not contain a specific accountability principle, certain provisions may be considered to ensure the same, such as privacy officers ensuring compliance.
Liability of Data Controllers and Data Processors		

Article 82 (2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

The Privacy Act does not explicitly define liabilities of data processors, but it does clarify other liabilities. Section 126: Subject to subsection (4), anything done or omitted by a person as the employee of another person shall, for the purposes of this Act, be treated as done or omitted by that other person as well as by the first-mentioned person, whether or not it was done with that other person's knowledge or approval. (2) Anything done or omitted by a person as the agent of another person shall, for the purposes of this Act, be treated as done or omitted by that other person as well as by the first-mentioned person, unless it is done or omitted without that other person's express or implied authority, precedent or subsequent. (3) Anything done or omitted by a person as a member of any agency shall, for the purposes of this Act, be treated as done or omitted by that agency as well as by the first-mentioned person, unless it is done or omitted without.

The Privacy Act 2020 refers to the liabilities of principals in relation to data breaches (see section 5.5. above), and also clarifies other liabilities for circumstances other than data breaches: Section 211: For the purpose of this Act, (a) anything done or omitted to be done by a person (A) as an employee of another person (B) is to be treated as being done or omitted by both A and B, whether or not it was done or omitted with B's knowledge or approval; (b) anything done or omitted to be done by a person (A) as an agent of another person (B) is to be treated as being done or omitted by both A and B, unless it was done or omitted without B's express or implied authority; (c) anything done or omitted to be done by a person as a member of an agency is to be treated as being done or omitted by both the person and the agency, unless it is done or omitted without the agency's express or implied authority. (2) In proceedings under this

Liability of Data Controllers and Data Processors (cont'd)

that agency's express or implied authority, precedent or subsequent.

(4) In proceedings under this Act against any person in respect of an act alleged to have been done by an employee of that person, it shall be a defence for that person to prove that he or she or it took such steps as were reasonably practicable to prevent the employee from doing that act, or from doing as an employee of that person acts of that description.

Act against any person (C) in respect of an act alleged to have been done by an employee of that person (D), it is a defence to prove that C took such steps as were reasonably practicable to prevent D from doing that or any similar act.

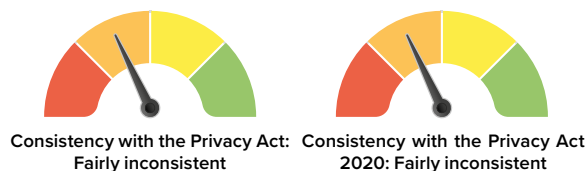
(3) Subsection (2) overrides subsection (1)(a).

(4) This section is subject to Sections 119 and 120 [on liabilities and data breaches].



5. Rights

5.1. Right to erasure



Neither the Privacy Act nor the Privacy Act 2020 provide for a clear right to erasure in the same manner as the GDPR. However, both define 'correction' as including 'deletion' and provide for a right to 'correct' information.

GDPR	Privacy Act	Privacy Act 2020
------	-------------	------------------

Grounds for Erasure

Article 17(1): The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing;
- (d) the personal data have been unlawfully processed;
- (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Section 6, IPP 7: (1) Where an agency holds personal information, the individual concerned shall be entitled (a) to request correction of the information; and (b) to request that there be attached to the information a statement of the correction sought but not made.

(2) An agency that holds personal information shall, if so requested by the individual concerned or on its own initiative, take such steps (if any) to correct that information as are, in the circumstances, reasonable to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.

(3) Where an agency that holds personal information is not willing to correct that information in accordance with a request by the individual concerned, the agency shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the information, in such a manner that it will always be read with the information, any statement provided by that individual of the correction sought.

Section 22, IPP 7: (1) An individual whose personal information is held by an agency is entitled to request the agency to correct the information.

(2) An agency that holds personal information must, on request or on its own initiative, take such steps (if any) that are reasonable in the circumstances to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.

(3) When requesting the correction of personal information, or at any later time, an individual is entitled to (a) provide the agency with a statement of the correction sought to the information (a statement of correction); and (b) request the agency to attach the statement of correction to the information if the agency does not make the correction sought.

(4) If an agency that holds personal information is not willing to correct the information as requested and has been provided with a statement of correction, the agency must take such steps (if any) that are reasonable in the circumstances to ensure that the statement of correction is attached to the information in a manner that ensures that it will always be read with the information.

(5) If an agency corrects personal information or attaches a statement of correction to personal

Grounds for Erasure (cont'd)

information, that agency must, so far as is reasonably practicable, inform every other person to whom the agency has disclosed the information.

(6) Subclauses (1) to (2B) are subject to the provisions of Part 4.

Section 7(1): 'correct', in relation to personal information, means to alter that information by way of correction, deletion, or addition, and 'correction' has a corresponding meaning.

Section 22, IPP 8: An agency that holds personal information must not use or disclose that information without taking any steps that are, in the circumstances, reasonable to ensure that the information is accurate, up to date, complete, relevant, and not misleading.

Inform Data Subject of Right

Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

Section 6, IPP 3(1): Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of [...] (g) the rights of access to, and correction of, personal information provided by these principles.

Section 22, IPP 3(1): Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of [...] (g) the rights of access to, and correction of, information provided by these principles.

Fees

Article 12(5): Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

- (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
- (b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Section 35: (2) Subject to subsection (4), an agency that is not a public sector agency shall not require the payment, by or on behalf of any individual who wishes to make an information privacy request, of any charge in respect of (a) the provision of assistance in accordance with Section 38; or (b) the making of the request to that agency; or (c) the transfer of the request to any other agency; or (d) the processing of the request, including deciding whether or not the request is to be granted and, if so, in what manner.

(3) An agency that is not a public sector agency may require the payment, by or on behalf of any individual who wishes to make a request pursuant to subclause (1)(a) or subclause (1)(b) of IPP 6 or pursuant to IPP 7, of a charge in respect of (a) the making available of information in compliance, in whole or in part, with the request; or (b) in the case of a request made pursuant to subclause (1) of IPP 7, (i) the correction of any information in compliance, in whole or in part, with the request; or (ii) the attaching, to any information, of a statement of any correction sought but not made.

Section 40(2): Where any charge is imposed, the agency may require the whole or part of the charge to be paid in advance.

Section 66: (1) In relation to an IPP 6 request, [...] (2)(b) a private sector agency may, subject to the provisions of any applicable code of practice, impose a charge for (i) providing assistance under Section 42; (ii) attaching a statement of correction to personal information. [...] (4) A charge imposed under subsection (1) or (2) must be reasonable [...] (5) An agency may require all or part of a charge to be paid in advance.

Response Timeframe

Article 12(3): The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one

Section 40(1): Subject to this Act, the agency to which an information privacy request is made or transferred in accordance with this Act shall, as soon as reasonably practicable,

Section 63: (1) As soon as is reasonably practicable after receiving a request under IPP 7(1), and in any case not later than 20 working days after receiving the request, an agency must (a)

Response Timeframe (cont'd)

month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

and in any case not later than 20 working days after the day on which the request is received by that agency, (a) decide whether the request is to be granted and, if it is to be granted, in what manner and, subject to Sections 35 and 36, for what charge (if any); and (b) give or post to the individual who made the request notice of the decision on the request.

Section 41: (1) Where an information privacy request is made or transferred to an agency, the agency may extend the time limit set out in section 39 or Section 40(1) in respect of the request if (a) the request is for a large quantity of information or necessitates a search through a large quantity of information, and meeting the original time limit would unreasonably interfere with the operations of the agency; or (b) consultations necessary to make a decision on the request are such that a proper response to the request cannot reasonably be made within the original time limit.

(2) Any extension under subsection (1) shall be for a reasonable period of time having regard to the circumstances.

decide whether to grant the request; and (b) notify the requestor that (i) the agency has corrected, or will correct, the personal information; or (ii) the agency will not correct the personal information.

Section 65: On receiving a correction request, an agency may extend the time limit set out in Section 62 or 63 in respect of the request if (a) the request necessitates a search through a large quantity of information, and meeting the original time limit would unreasonably interfere with the operations of the agency; (b) consultations necessary to make a decision on the request are such that a response to the request cannot reasonably be given within the original time limit; or (c) the processing of the request raises issues of such complexity that a response to the request cannot reasonably be given within the original time limit.

(2) Any extension under subsection (1) must be for a reasonable period of time, having regard to the circumstances.

Format of Response

Article 12(1): The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

The Privacy Act does not specify the format of a response to a request for correction.

The Privacy Act 2020 does not specify the format of a response to a request for correction. [Note: Section 63 of the Privacy Act 2020 outlines the decision process for providing a statement of correction.]

Publicly Available Data

Article 17(2): Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

The Privacy Act does not refer specifically to publicly available data, however Section 6, IPP 7 provides: (4) Where the agency has taken steps under subclause (2) or subclause (3), the agency shall, if reasonably practicable, inform each person or body or agency to whom the personal information has been disclosed of those steps.

The Privacy Act 2020 does not refer specifically to publicly available data, however Section 22, IPP 7 provides: (3) If an agency corrects personal information or attaches a statement of correction to personal information, that agency must, so far as is reasonably practicable, inform every other person to whom the agency has disclosed the information.

Exceptions

Article 17(3): Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

- (a) for exercising the right of freedom of expression and information;
- (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
- (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or (e) for the establishment, exercise or defence of legal claims.

Section 55: Nothing in IPP 6 or IPP 7 applies in respect of (a) personal information in the course of transmission by post, telegram, cable, telex, facsimile transmission, electronic mail, or other similar means of communication;

(b) evidence given or submissions made to

- (i) a Royal Commission; or (ii) a commission of inquiry appointed by Order in Council under the Commissions of Inquiry Act 1908; or (iii) an inquiry to which Section 6 of the Inquiries Act 2013 applies, at any time before the report of the Royal Commission, commission of inquiry, or inquiry, as the case may be, has been published or, in the case of evidence given or submissions made in the course of a public hearing, at any time before the report has been presented to the Governor-General or appointing Minister, as the case may be; (c) evidence given or submissions made to a commission of inquiry or board of inquiry or court of inquiry or committee of inquiry appointed, pursuant to, and not by, any provision of an Act, to inquire into a specified matter;

Section 29: IPPs 6 and 7 do not apply in respect of (a) personal information during transmission by post, personal delivery, or electronic means;

(b) personal information that is contained in any correspondence or communication between an agency and any of the following persons and that relates to an investigation conducted by that person under any Act, not being information that was in existence before the commencement of the investigation: (i) an Ombudsman; (ii) any officer or employee appointed by the Chief Ombudsman under section 11(1) of the Ombudsmen Act 1975; (iii) the Commissioner; (iv) any employee or delegate of the Commissioner;

(c) personal information held by the Auditor-General, the Deputy Auditor-General, or any employee of the Auditor-General in connection with the performance or exercise of the Auditor-General's functions, duties, or powers that is not personal information about any employee or former

Exceptions (cont'd)

Article 12(5): Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

(d) information contained in any correspondence or communication that has taken place between the office of the Ombudsmen and any agency and that relates to any investigation conducted by an Ombudsman under the Ombudsmen Act 1975 or the Official Information Act 1982 or the Local Government Official Information and Meetings Act 1987, other than information that came into existence before the commencement of that investigation; or

(e) information contained in any correspondence or communication that has taken place between the office of the Commissioner and any agency and that relates to any investigation conducted by the Commissioner under this Act, other than information that came into existence before the commencement of that investigation.

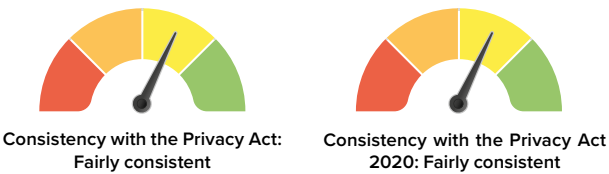
employee of the Auditor-General in their capacity as an employee;

(d) personal information contained in evidence given or submissions made to (i) a government inquiry, until the final report of that inquiry is presented to the appointing Minister; (ii) a public inquiry (including a Royal commission), until the final report of that inquiry is presented to the House of Representatives; (iii) a person or body appointed under any act to inquire into a specified matter; or (e) personal information contained in a video record made under the Evidence Regulations 2007 or any copy or transcript of the video record.

(2) IPP 7 does not apply to personal information collected by Statistics New Zealand under the Statistics Act 1975.



5.2. Right to be informed



The GDPR, the Privacy Act, and the Privacy Act 2020 all establish the right to be informed and set out similar information of which data subjects/concerned individuals need to be made aware. The Privacy Act and the Privacy Act 2020, however, differ from the GDPR in terms of detailing this right.

GDPR	Privacy Act	Privacy Act 2020
Informed Prior to/at Collection		
<p>Article 13(1): Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:</p> <p>(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;</p> <p>(b) the contact details of the data protection officer, where applicable;</p> <p>(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;</p> <p>(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;</p> <p>(e) the recipients or categories of recipients of the personal data, if any;</p> <p>(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available. (2) In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained,</p>	<p>Section 6, IPP 3: Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of (a) the fact that the information is being collected; and (b) the purpose for which the information is being collected; and (c) the intended recipients of the information; and (d) the name and address of (i) the agency that is collecting the information; and (ii) the agency that will hold the information; and (e) if the collection of the information is authorised or required by or under law, (i) the particular law by or under which the collection of the information is so authorised or required; (ii) whether or not the supply of the information by that individual is voluntary or mandatory; (f) the consequences (if any) for that individual if all or any part of the requested information is not provided; and (g) the rights of access to, and correction of, personal information provided by these principles.</p> <p>(2) The steps referred to in subclause (1) shall be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected.</p>	<p>Section 22, IPP 3: If an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of (a) the fact that the information is being collected; and (b) the purpose for which the information is being collected; and (c) the intended recipients of the information; and (d) the name and address of (i) the agency that is collecting the information; and (ii) the agency that will hold the information; and (e) if the collection of the information is authorised or required by or under law, (i) the particular law by or under which the collection of the information is so authorised or required; (ii) whether or not the supply of the information by that individual is voluntary or mandatory; (f) the consequences (if any) for that individual if all or any part of the requested information is not provided; and (g) the rights of access to, and correction of, personal information provided by these principles.</p> <p>(2) The steps referred to in subclause (1) shall be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected.</p>

Informed Prior to/at Collection (cont'd)

provide the data subject with the following further information necessary to ensure fair and transparent processing:

- (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- (c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- (d) the right to lodge a complaint with a supervisory authority;
- (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

What Information is to be Provided

See Article 13(1) and (2) above.

See Section 6, IPP 3 above.

See Section 22, IPP 3 above.

When Data is from Third Party

In addition to the information required under Article 13, Article 14(2) specifies that where information is not obtained directly from the data subject then the data subject must be provided with information on the legitimate interests pursued by the controller or by a third party where the processing is based on point (f) of Article 6(1). Furthermore, paragraph (e) of Article 13(2) is replaced with a requirement to inform data subjects of the source from which the personal data originate, and if applicable, whether it came from publicly accessible sources.

The Privacy Act does not specify what information must be provided to a concerned individual where personal information has been obtained indirectly, however Section 6, IPP 2 provides that, unless certain exceptions apply, 'Where an agency collects personal information, the agency shall collect the information directly from the individual concerned.'

The Privacy Act 2020 does not specify what information must be provided to a concerned individual where personal information has been obtained indirectly, however Section 22, IPP 2 provides that, unless certain exceptions apply, 'If an agency collects personal information, the information must be collected from the individual concerned.'

Intelligibility Requirements

Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

The Privacy Act does not refer to intelligibility requirements in relation to the right to be informed.

The Privacy Act 2020 does not refer to intelligibility requirements in relation to the right to be informed.

Format

See Article 12(1) above.

The Privacy Act does not address this matter.

The Privacy Act 2020 does not address this matter.

Exceptions

The requirements of Article 13 do not apply where the data subject already has the information. The requirements of Article 14 do not apply where:

- (a) the data subject already has the information;
- (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
- (c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
- (d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

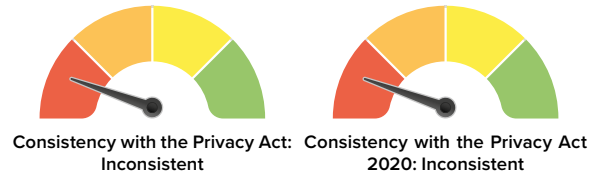
Section 6, IPP 3: (3) An agency is not required to take the steps referred to in subclause (1) in relation to the collection of information from an individual if that agency has taken those steps in relation to the collection, from that individual, of the same information or information of the same kind, on a recent previous occasion.

- (4) It is not necessary for an agency to comply with subclause (1) if the agency believes, on reasonable grounds, (a) that non-compliance is authorised by the individual concerned; (b) that non-compliance would not prejudice the interests of the individual concerned; (c) that non-compliance is necessary (i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; (ii) for the enforcement of a law imposing a pecuniary penalty; (iii) for the protection of the public revenue; or (iv) or the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); (d) that compliance would prejudice the purposes of the collection; or (e) that compliance is not reasonably practicable in the circumstances of the particular case; or (f) that the information (i) will not be used in a form in which the individual concerned is identified; or (ii) will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

Section 22, IPP 3: (3) An agency is not required to take the steps referred to in subclause (1) in relation to the collection of information from an individual if the agency has taken those steps on a recent previous occasion in relation to the collection, from that individual, of the same information or information of the same kind.

- (4) It is not necessary for an agency to comply with subclause (1) if the agency believes, on reasonable grounds, (a) that non-compliance would not prejudice the interests of the individual concerned; or (b) that non-compliance is necessary - (i) to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or (ii) for the enforcement of a law that imposes a pecuniary penalty; or (iii) for the protection of public revenue; or (iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or (c) that compliance would prejudice the purposes of the collection; or (d) that compliance is not reasonably practicable in the circumstances of the particular case; or (e) that the information - (i) will not be used in a form in which the individual concerned is identified; or (ii) will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

5.3. Right to object



Unlike the GDPR, neither the Privacy Act nor the Privacy Act 2020 provide for a right to object or address associated concerns such as withdrawal of consent.

GDPR	Privacy Act	Privacy Act 2020
------	-------------	------------------

Grounds for Right to Object/ Opt Out

Article 21(1): The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

The Privacy Act does not provide for a right to object.

The Privacy Act 2020 does not provide for a right to object.

Withdraw Consent

Article 7(3): The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

The Privacy Act does not provide for the withdrawal of consent.

The Privacy Act 2020 does not provide for the withdrawal of consent.

Restrict Processing

Article 18(1): The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: (a) the accuracy of the personal data is contested by the data subject, for a period enabling

The Privacy Act does not provide for restrictions on processing.

The Privacy Act 2020 does not provide for restrictions on processing.

Restrict Processing (cont'd)

the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

Object to Direct Marketing

Article 21(3): Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

The Privacy Act does not address this matter.

The Privacy Act 2020 does not address this matter.

Inform Data Subject of Right

See Article 12(1) in section 5.1. above. In addition, Article 21(4) provides: At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

The Privacy Act does not provide for a right to object.

The Privacy Act 2020 does not provide for a right to object.

Fees

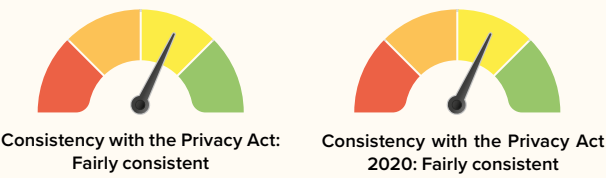
See Article 12(5) in section 5.1. above.

The Privacy Act does not provide for a right to object.

The Privacy Act 2020 does not provide for a right to object.

GDPR	Privacy Act	Privacy Act 2020
Response Timeframe		
See Article 12(3) in section 5.1. above.	The Privacy Act does not provide for a right to object.	The Privacy Act 2020 does not provide for a right to object.
Format of Response		
See Article 12(1) in section 5.1. above.	The Privacy Act does not provide for a right to object.	The Privacy Act 2020 does not provide for a right to object.
Exceptions		
See Article 12(5) in section 5.1. above.	Not applicable.	Not applicable.

5.4. Right of access



The GDPR, the Privacy Act, and the Privacy Act 2020 provide extensive rights of access, and detail matters such as informing data subjects/concerned individuals of the right, response timeframes, and reasons for refusing access. The specifics of these requirements, however, differ between the pieces of legislation.

GDPR	Privacy Act	Privacy Act 2020
------	-------------	------------------

Grounds for Right of Access

Article 15(1): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed.	Section 6, IPP 6: Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled (a) to obtain from the agency confirmation of whether or not the agency holds such personal information; and (b) to have access to that information.	Section 22, IPP 6: (1) An individual is entitled to receive from an agency upon request (a) confirmation of whether the agency holds any personal information about them; and (b) access to their personal information.
---	--	---

Information to be Accessed

Article 15(1): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal	See Section 6, IPP 6 above.	See Section 22, IPP 6 above.
--	-----------------------------	------------------------------



Information to be Accessed (cont'd)

data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source; and

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Inform Data Subject of Right

See Article 12(1) in section 5.1.

Section 6, IPP 3(1): Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of [...] (g) the rights of access to, and correction of, personal information provided by these principles.

Section 22, IPP 3(1): Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of [...] (g) the rights of access to, and correction of, information provided by the IPPs.

Fees

See Article 12(5) in section 6.1. above.

See Section 35 and 40(2) in section 6.1. above.

Section 66: (1) In relation to an IPP 6 request, [...] (b) a private sector agency may, subject to the provisions of any applicable code of practice, impose a charge for (i) providing assistance under Section 42, but only if the agency makes information available in compliance, in whole or in part, with the request; (ii) making information available in compliance, in whole or in part, with the request. [...] (4) A charge imposed under Subsection (1) or (2) must be

GDPR	Privacy Act	Privacy Act 2020
------	-------------	------------------

Fees (cont'd)

reasonable and, in the case of a charge imposed under Subsection (1) (a) or (b)(ii), regard may be had to (a) the cost of the labour and materials involved in making the information available; and (b) any costs involved in making the information available urgently (in the case of an urgent IPP 6 request received under Section 46). (5) An agency may require all or part of a charge to be paid in advance.

Verify Data Subject Request

Recital 64: The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

The Privacy Act does not specifically address this matter.

The Privacy Act 2020 does not specifically address this matter.

Response Timeframe

See Article 12(3) in section 6.1. above.

See Sections 40 and 41 in section 6.1. above.

Section 44: (1) If an agency does not transfer an IPP 6 request under Section 43, the agency must, as soon as is reasonably practicable, and in any case not later than 20 working days after the day on which the request is received, respond to the request. Section 48: (1) On receiving an IPP 6 request, an agency may extend the time limit set out in Section 43 or 44 in respect of the request if (a) the request is for a large quantity of information, or necessitates a search through a large quantity of information, and meeting the original time limit would unreasonably interfere with the operations of the agency; (b) consultations necessary to make a decision on the request

Response Timeframe (cont'd)

are such that a response to the request cannot reasonably be given within the original time limit; or

(c) the processing of the request raises issues of such complexity that a response to the request cannot reasonably be given within the original time limit.

(2) Any extension under subsection (1) must be for a reasonable period of time having regard to the circumstances.

Format of Response

See Article 12(1) in section 6.1. above.

Section 42: (1) Where the information in respect of which an information privacy request is made by any individual is comprised in a document, that information may be made available in 1 or more of the following ways:

(a) by giving the individual a reasonable opportunity to inspect the document;

(b) by providing the individual with a copy of the document; or

(c) in the case of a document that is an article or thing from which sounds or visual images are capable of being reproduced, by making arrangements for the individual to hear or view those sounds or visual images; (d) in the case of a document by which words are recorded in a manner in which they are capable of being reproduced in the form of sound or in which words are contained in the form of shorthand writing or in codified form, by providing the individual with a written transcript of the words recorded or contained in the document;

(e) by giving an excerpt or summary of the contents; or

(f) by furnishing oral information about its contents.

(2) Subject to Section 43, the agency shall make the information available

Section 56: If the personal information requested by an individual is in a document, that information may be made available in one or more of the following ways:

(a) by giving the requestor a reasonable opportunity to inspect the document;

(b) by providing the requestor with a hard copy or an electronic copy of the document;

(c) in the case of a document that is an article or a thing from which sounds or visual images are capable of being reproduced, by making arrangements for the requestor to hear or view the sounds or visual images;

(d) in the case of a document by which words are recorded in a manner in which they are capable of being reproduced in the form of sound or in which words are contained in the form of shorthand writing or in codified form, by providing the requestor with a written transcript of the words recorded or contained in the document;

(e) by giving, in any manner, an excerpt or a summary of the document's contents; or

(f) by giving oral information about the document's contents.

Format of Response (cont'd)

in the way preferred by the individual requesting it unless to do so would

(a) impair efficient administration;

(b) be contrary to any legal duty of the agency in respect of the document; or

(c) prejudice the interests protected by Section 27 or Section 28 or Section

29 and (in the case of the interests protected by Section 28) there is

no countervailing public interest.

(3) Where the information is not provided in the way preferred by the individual

requesting it, the agency shall, subject to Section 32, give to that individual (a) the

reason for not providing the information in that way; and (b) if that individual so

requests, the grounds in support of that reason, unless the giving of those grounds

would itself prejudice the interests

protected by Section 27 or Section 28

or Section 29 and (in the case of the

interests protected by Section 28) there

is no countervailing public interest.

(2) Subject to Section 55, the agency must make the information available

in the way preferred by the requestor

unless to do so would (a) impair the

efficient administration of the agency;

or (b) be contrary to any legal duty of

the agency in respect of the document;

or (c) prejudice an interest protected

by any of Sections 49 to 53.

(3) If the information is not provided in the way preferred by the requestor, the agency must give to the requestor

(a) the reason for not providing

the information in that way; and (b)

if the requestor so requests, the

grounds in support of that reason

Exceptions

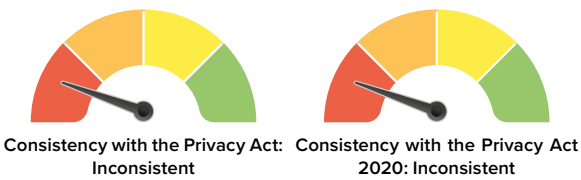
See Article 12(5) in section 6.1. above.

See Section 55 in section 6.1. above.

In addition, Part 4 of the Privacy Act sets out 'good reasons for refusing access,' including security, defence, international relations, and trade secrets, as well as general reasons such as the request being 'frivolous.'

Sections 49-53 consider reasons for refusing access, including protection of individuals, whether the information is evaluative material, security, defence, international relation, trade secrets, and general reasons such as the information cannot be found.

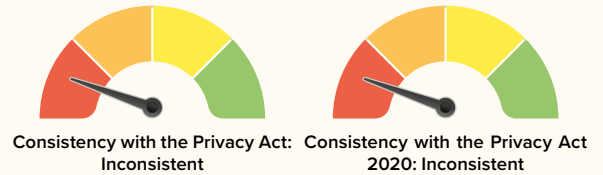
5.5. Right not to be subject to discrimination



Unlike the GDPR, neither the Privacy Act nor the Privacy Act 2020 address matters to do with discrimination through automated processing or for exercising rights.

GDPR	Privacy Act	Privacy Act 2020
Definition of Right		
<p>The GDPR only implies this right and does not provide an explicit definition for it.</p>	<p>The Privacy Act does not refer to this right. [Note: There are specific provisions relating to information matching agreements and 'adverse actions' (see Part 10 of the Privacy Act).]</p>	<p>The Privacy Act 2020 does not refer to this right. [Note: There are specific provisions relating to information matching agreements and 'adverse actions' (see Part 7 of the Privacy Act 2020).]</p>
Automated Processing		
<p>Article 22(1): The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. [Article 22 goes on to detail this right, including exceptions]</p>	<p>The Privacy Act does not refer to automated processing.</p>	<p>The Privacy Act 2020 does not refer to automated processing.</p>

5.6. Right to data portability



Unlike the GDPR, neither the Privacy Act nor the Privacy Act 2020 provide for a right to data portability.

GDPR	Privacy Act	Privacy Act 2020
Grounds for Portability		
Article 20(1): The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means.	The Privacy Act does not provide for the right to data portability.	The Privacy Act 2020 does not provide for the right to data portability.
Inform Data Subject of Right		
See Article 12(1) in section 5.1.	The Privacy Act does not provide for the right to data portability.	The Privacy Act 2020 does not provide for the right to data portability.
Fees		
See Article 12(5) in section 5.1. above.	The Privacy Act does not provide for the right to data portability.	The Privacy Act 2020 does not provide for the right to data portability.
Response Timeframe		
See Article 12(3) in section 5.1. above.	The Privacy Act does not provide for the right to data portability.	The Privacy Act 2020 does not provide for the right to data portability.
Format		
See Article 20(1) above.	The Privacy Act does not provide for the right to data portability.	The Privacy Act 2020 does not provide for the right to data portability.

GDPR	Privacy Act	Privacy Act 2020
------	-------------	------------------

Controller to Controller

Article 20(2): In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

The Privacy Act does not provide for the right to data portability.

The Privacy Act 2020 does not provide for the right to data portability.

Technically Feasible

See Article 20(2) above.

The Privacy Act does not provide for the right to data portability.

The Privacy Act 2020 does not provide for the right to data portability.

Exceptions

See Article 12(5) in section 5.1. above.

The Privacy Act does not provide for the right to data portability.

The Privacy Act 2020 does not provide for the right to data portability.

6. Enforcement



Consistency with the Privacy Act:
Fairly inconsistent



Consistency with the Privacy Act
2020: Fairly inconsistent

6.1. Monetary penalties

While the GDPR, the Privacy Act, and the Privacy Act 2020 all provide for monetary penalties, the potential fines under the GDPR are substantially higher. The Privacy Act 2020 will introduce some increases to sanctions in New Zealand, but these will still be significantly lower than those available under the GDPR.

GDPR	Privacy Act	Privacy Act 2020
Provides for Monetary Penalties		
The GDPR provides for monetary penalties.	The Privacy Act provides for monetary penalties.	The Privacy Act 2020 provides for monetary penalties.
Issued by		
Article 58(2) Each supervisory authority shall have all of the following corrective powers: [...] (i): to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case.	The OPC does not have the power to issue fines directly. The OPC may refer matters to the Human Rights Tribunal, which has the authority to issue fines.	The OPC does not have the power to issue fines directly. The OPC may refer matters to the Human Rights Tribunal, which has the authority to issue fines.
Fine Maximum		
Article 83(5): infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; (b) the data subjects' rights pursuant to Articles 12 to 22; (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant	Section 127: Every person commits an offence against this Act and is liable on conviction to a fine not exceeding \$2,000 [approx. €1,110]. [Note: Section 114F provides that, 'Every person who, without reasonable excuse, fails or refuses to comply with a transfer prohibition notice commits an offence and is liable on conviction to a fine not exceeding \$10,000 [approx. €5,540].']	Section 212: A person commits an offence against this Act and is liable on conviction to a fine not exceeding \$10,000 [approx. €5,540].

Fine Maximum (cont'd)

to Articles 44 to 49;

(d) any obligations pursuant to Member State law adopted under Chapter IX;

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

(6) Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Percentage of Turnover

Under Article 83(4), (5), and (6), fines may be issued that equate to 2% or 4% of the total worldwide annual turnover of the preceding financial year.

The Privacy Act does not provide for fines that are equivalent to a percentage of turnover.

The Privacy Act 2020 does not provide for fines that are equivalent to a percentage of turnover.

Mitigating Factors

Article 83(2): When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them; (b) the intentional or negligent character of the infringement; (c) any action taken by the controller

The Privacy Act does not directly refer to mitigating factors relating to monetary penalties. However, it does set out relevant considerations in relation to complaints.

Section 71: (1) The Commissioner may in his or her discretion decide to take no action or, as the case may require, no further action, on any complaint if, in the Commissioner's opinion, (a) the length of time that has elapsed between the date when the subject matter of the complaint arose and the date when the complaint was made is such that an investigation of the complaint is no longer practicable or desirable;

The Privacy Act 2020 does not directly refer to mitigating factors relating to monetary penalties. However, it does set out relevant considerations in relation to complaints.

Section 80: The Commissioner may decide not to investigate a complaint if, in the Commissioner's opinion, (a) the complainant has not made reasonable efforts to resolve the complaint directly with the agency concerned; or (b) there is an alternative dispute resolution process available to resolve the complaint because of the agency's membership of a

Mitigating Factors (cont'd)

or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

(b) the subject matter of the complaint is trivial;

(c) the complaint is frivolous or vexatious or is not made in good faith;

(d) the individual alleged to be aggrieved does not desire that action be taken or, as the case may be, continued;

(e) the complainant does not have a sufficient personal interest in the subject matter of the complaint; or

(f) where (i) the complaint relates to a matter in respect of which a code of practice issued under Section 46 is in force; and (ii) the code of practice makes provision for a complaints procedure, the complainant has failed to pursue, or to pursue fully, an avenue of redress available under that complaints procedure that it would be reasonable for the complainant to pursue; or

(g) there is in all the circumstances an adequate remedy or right of appeal, other than the right to petition the House of Representatives or to make a complaint to an Ombudsman, that it would be reasonable for the individual alleged to be aggrieved to exercise.

(2) Notwithstanding anything in subsection (1), the Commissioner may in his or her discretion decide not to take any further action on a complaint if, in the course of the investigation of the complaint, it appears to the Commissioner that, having regard to all the circumstances of the case, any further action is unnecessary or inappropriate.

particular profession or industry; or

(c) there is an adequate remedy or right of appeal, other than the right to petition the House of Representatives or to make a complaint to an Ombudsman, that it would be reasonable for the aggrieved individual to pursue;

(d) the complaint relates to a matter in respect of which a code of practice has been issued that includes a complaints procedure, and the complainant has not taken reasonable steps to pursue, or fully pursue, the redress available under that procedure;

(e) the aggrieved individual or aggrieved individuals knew about the action that is the subject of the complaint for 12 months or more before making the complaint was made;

(f) the time that has elapsed between the date on which the subject of the complaint arose and the date on which the complaint was made is such that an investigation of the complaint is no longer practicable or desirable;

(g) the aggrieved individual does or aggrieved individuals do not want the complaint pursued; or

(h) the complainant does not have a sufficient personal interest in the subject of the complaint; or

(i) the subject of the complaint is trivial; or

(j) the complaint is frivolous, vexatious, or not made in good faith.

(2) Despite anything in subsection (1), the Commissioner may, in the Commissioner's discretion, decide not to investigate a complaint if it appears to the Commissioner that, having regard to all the circumstances of the case, an investigation is unnecessary.

GDPR	Privacy Act	Privacy Act 2020
------	-------------	------------------

Imprisonment

Not applicable.

Not applicable.

Not applicable.

DPO Liability

Not applicable.

Section 126: (1) Subject to subsection (4), anything done or omitted by a person as the employee of another person shall, for the purposes of this Act, be treated as done or omitted by that other person as well as by the first-mentioned person, whether or not it was done with that other person's knowledge or approval.

(2) Anything done or omitted by a person as the agent of another person shall, for the purposes of this Act, be treated as done or omitted by that other person as well as by the first-mentioned person, unless it is done or omitted without that other person's express or implied authority, precedent or subsequent.

(3) Anything done or omitted by a person as a member of any agency shall, for the purposes of this Act, be treated as done or omitted by that agency as well as by the first-mentioned person, unless it is done or omitted without that agency's express or implied authority, precedent or subsequent.

(4) In proceedings under this Act against any person in respect of an act alleged to have been done by an employee of that person, it shall be a defence for that person to prove that he or she or it took such steps as were reasonably practicable to prevent the employee from doing that act, or from doing as an employee of that person acts of that description.

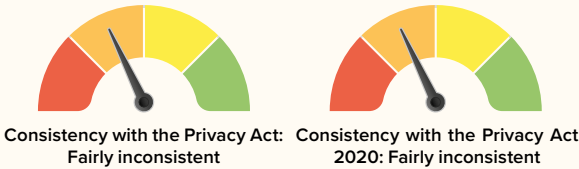
Section 211: For the purpose of this Act, (a) anything done or omitted to be done by a person (A) as an employee of another person (B) is to be treated as being done or omitted by both A and B, whether or not it was done or omitted with B's knowledge or approval; (b) anything done or omitted to be done by a person (A) as an agent of another person (B) is to be treated as being done or omitted by both A and B, unless it was done or omitted without B's express or implied authority; (c) anything done or omitted to be done by a person as a member of an agency is to be treated as being done or omitted by both the person and the agency, unless it is done or omitted without the agency's express or implied authority.

(2) In proceedings under this Act against any person (C) in respect of an act alleged to have been done by an employee of that person (D), it is a defence to prove that C took such steps as were reasonably practicable to prevent D from doing that or any similar act.

(3) Subsection (2) overrides subsection (1)(a).

(4) This Section is subject to Sections 119 and 120 [on liabilities and data breaches].

6.2. Supervisory authority



Although the supervisory authorities regulated by the GDPR, the Privacy Act, and the Privacy Act 2020 have broadly similar investigatory and advisory powers, there are notable differences in terms of corrective powers. The GDPR sets out more extensive corrective powers than the Privacy Act and the Privacy Act 2020, however the Privacy Act 2020 will introduce some limited corrective powers to the OPC.

GDPR	Privacy Act	Privacy Act 2020
------	-------------	------------------

Provides for Data Protection Authority

Article 51(1): Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

Section 12(1): There shall be a Commissioner called the Privacy Commissioner.

Section 13: (1) There continues to be a Commissioner called the Privacy Commissioner.

Investigatory Powers

Article 58(1): Each supervisory authority shall have all of the following investigative powers:

- (a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;
- (b) to carry out investigations in the form of data protection audits;
- (c) to carry out a review on certifications issued pursuant to Article 42(7);
- (d) to notify the controller or the processor of an alleged infringement of this Regulation;
- (e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;
- (f) to obtain access to any premises of the

Section 69: (1) The functions of the Commissioner under this Part shall be

- (a) to investigate any action that is or appears to be an interference with the privacy of an individual;
- (b) to act as conciliator in relation to any such action;
- (c) to take such further action as is contemplated by this Part.

(2) The Commissioner may commence an investigation under subsection (1)(a) either on complaint made to the Commissioner or on the Commissioner's own initiative.

Section 90: (1) Every investigation under Part 8 by the Commissioner shall be conducted in private.

(2) Subject to Section 120, –(a) the Commissioner may hear or obtain information from such persons as the Commissioner thinks fit; (b) the Commissioner may make such inquiries

Section 79: This subpart applies to investigations conducted by the Commissioner

- (a) into complaints received under Section 72(1); or the Commissioner's own initiative, into any matter in respect of which a complaint may be made under this Act.

Section 81: (1) The Commissioner must conduct an investigation in a timely manner.

(2) During an investigation, the Commissioner may

- (a) hear and obtain information from any person;
- (b) make any inquiries.

(3) At any time during an investigation, the Commissioner may decide to take no further action on a complaint or matter if the Commissioner

- (a) is satisfied of any of the matters set out in Section 80;
- (b) considers that any further action is unnecessary or inappropriate.

Investigatory Powers (cont'd)

controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

as the Commissioner thinks fit;

(c) it shall not be necessary for the

Commissioner to hold any hearing;

(d) subject to Section 73(b), no person shall be entitled as of right to be heard by the Commissioner.

(3) Subject to the provisions of this Act, the Commissioner may regulate his or her procedure in such manner as he or she thinks fit.

[Note: Part 9 of the Privacy Act goes on to further detail the proceedings of the OPC.]

(4) As soon as practicable after making a decision under subsection

(3), the Commissioner must notify the parties of (a) that decision; and (b) the reason for that decision.

(5) It is not necessary for the Commissioner to hold a hearing, and no person is entitled as of right to be heard by the Commissioner.

(6) Any investigation held by the Commissioner must be conducted in private.

Section 82: When conducting an investigation, the Commissioner may adopt any procedure the Commissioner considers appropriate that is not inconsistent with this Act or any regulations made Section 215(1)(a).

Corrective Powers

Article 58(2): Each supervisory authority shall have all of the following corrective powers:

- (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
- (b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
- (c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
- (d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
- (e) to order the controller to communicate a personal data

The Privacy Act does not provide the OPC with direct corrective powers.

Instead, the OPC may seek to secure settlements between parties or pass matters on to the Director of Human Rights Proceedings (see Section 77). See Section 87 of the Privacy Act on the powers of the Human Rights Tribunal.

Corrective powers are largely held by the Human Rights Tribunal under the Privacy Act 2020. However, the Privacy Act 2020 will introduce limited corrective powers for the OPC in the form of access directions and compliance notices.

Section 92: (1) The Commissioner may direct an agency to provide an individual access to the individual's personal information in any manner that the Commissioner considers appropriate.

(2) Without limiting subsection (1), the Commissioner may direct an agency to do any of the following before a specified date:

- (a) confirm whether the agency holds any specified personal information;
- (b) permit the individual access to any specified personal information;
- (c) make any specified information available to the individual in a particular way.

Corrective Powers (cont'd)

breach to the data subject;

(f) to impose a temporary or definitive limitation including a ban on processing;

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

(3) The Commissioner may, at any time, on the request of the individual or on the Commissioner's own initiative,

(a) amend an access direction; or

(b) cancel an access direction.

Section 123: The Commissioner may issue a compliance notice to an agency if the Commissioner considers that one or more of the following may have occurred: (a) a breach of this Act, including an action listed in Section 69(2)(a); (b) an action that is to be treated as a breach of an IPP or an interference with the privacy of an individual under another Act; (c) a breach of a code of practice issued under this Act or a code of conduct (or similar) issued under another Act (if a complaint about a breach of the code can be the subject of a complaint under Part 5 of this Act).

(2) Before issuing a compliance notice, the Commissioner may, but is not required to, (a) assess whether any person has suffered harm (for example, the types of harm listed in Section 69(2)(b)); (b) use other means under this Act or another act for dealing with the breach.

(3) A compliance notice may be issued at any time, including concurrently with the use of any other means for dealing with the breach.

[Note: Sections 125-135 go on to detail processes related to compliance notices, including the publication of such notices and potential fines imposed by the Human Rights Tribunal.]

Authorisation/Advisory Powers

Article 58(3): Each supervisory authority shall have all of the following authorisation and advisory powers:

Section 46(1): The Commissioner may from time to time issue a code of practice.

[Note: See Sections 47-53 for further

Section 32: (1) The Commissioner may at any time issue a code of practice in relation to the IPPs.

Authorisation/Advisory Powers (cont'd)

(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;

(b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

(c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;

(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);

(e) to accredit certification bodies pursuant to Article 43;

(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);

(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(h) to authorise contractual clauses referred to in point (a) of Article 46(3);

(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);

(j) to approve binding corporate rules pursuant to Article 47.

information on codes of practice.]

Section 54: (1) The Commissioner may authorise an agency to collect, use, or disclose personal information, even though that collection, use, or disclosure would otherwise be in breach of IPP 2 or IPP 10 or IPP 11, if the Commissioner is satisfied that, in the special circumstances of the case, (a) the public interest in that collection or, as the case requires, that use or that disclosure outweighs, to a substantial degree, any interference with the privacy of the individual that could result from that collection or, as the case requires, that use or that disclosure; or (b) that collection or, as the case requires, that use or that disclosure involves a clear benefit to the individual concerned that outweighs any interference with the privacy of the individual that could result from that collection or, as the case requires, that use or that disclosure.

(2) The Commissioner may impose in respect of any authority granted under subsection (1) such conditions as the Commissioner thinks fit.

(3) The Commissioner shall not grant an authority under subsection (1) in respect of the collection, use, or disclosure of any personal information for any purpose if the individual concerned has refused to authorise the collection or, as the case requires, the use or disclosure of the information for that purpose.

[In addition, see advisory powers in Section 13 of the Privacy Act below.]

[Note: See Sections 32-38 for further information on codes of practice.]

Section 30: (1) An agency may apply to the Commissioner for authorisation to do any of the following in the circumstances of a particular case: (a) collect personal information even if the collection of that information would otherwise be in breach of IPP 2; (b) keep personal information even if the keeping of that information would otherwise be in breach of IPP 9; (c) use personal information even if the use of that information would otherwise be in breach of IPP 10; (d) disclose personal information even if the disclosure of that information would otherwise be in breach of IPP 11 or 12.

(2) An application under subsection (1) must be made in the manner required by the Commissioner.

(3) If, on receiving an application, the Commissioner is not satisfied that the applicant has taken sufficient steps to give notice of the application to all individuals concerned, the Commissioner may require the applicant to give public notice of the application in a manner that the Commissioner specifies.

(4) If, on receiving an application, the Commissioner is not satisfied that the applicant has given sufficient opportunity to individuals concerned to object to the application, the Commissioner may require the applicant to give any further opportunity that the Commissioner specifies.

(5) In considering whether to grant an authorisation, the Commissioner must take into account any objections to the application received from individuals concerned.

(6) The Commissioner may grant an authorisation sought by an applicant

Authorisation/Advisory Powers (cont'd)

only if the Commissioner is satisfied that, in the special circumstances of the case, (a) the public interest in granting the authorisation outweighs, to a substantial degree, the possibility of (i) any loss, detriment, damage, or injury to the individuals concerned; or (ii) any adverse affect on the rights, benefits, privileges, obligations, or interests of the individuals concerned; or (iii) any significant humiliation, significant loss of dignity, or significant injury to the feelings of the individuals concerned; or (b) granting the authorisation would result in a clear benefit to the individuals concerned that outweighs the possibility of (i) any loss, detriment, damage, or injury to the individuals concerned; or (ii) any adverse effect on the rights, benefits, privileges, obligations, or interests of the individuals concerned; or (iii) any significant humiliation, significant loss of dignity, or significant injury to the feelings of the individuals concerned.

(7) The Commissioner may not grant an authorisation under subsection (6) in respect of any specified personal information if the individual concerned objected.

(8) An authorisation granted under subsection (6) may be subject to any conditions that the Commissioner considers appropriate.

(9) The Commissioner must maintain on the Commissioner's Internet site a list of current authorisations granted under this section.

[In addition, see advisory powers in Section 17 of the Privacy Act 2020 below.]

Tasks of Authority

Article 57(1): Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory: (a) monitor and enforce the application of this Regulation; (b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention; (c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing; (d) promote the awareness of controllers and processors of their obligations under this Regulation; (e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end; (f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary; (g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and

Section 13: (1) The functions of the Commissioner shall be (a) to promote, by education and publicity, an understanding and acceptance of the IPPs and of the objects of those principles; (b) when requested to do so by an agency, to conduct an audit of personal information maintained by that agency for the purpose of ascertaining whether or not the information is maintained according to the information privacy principles; (c) to monitor the use of unique identifiers, and to report to the Prime Minister from time to time on the results of that monitoring, including any recommendation relating to the need for, or desirability of taking, legislative, administrative, or other action to give protection, or better protection, to the privacy of the individual; (d) to maintain, and to publish, in accordance with Section 21, directories of personal information; (e) to monitor compliance with the public register IPPs, to review those IPPs from time to time with particular regard to the Council of Europe Recommendations on Communication to Third Parties of Personal Data Held by Public Bodies (Recommendation R (91) 10), and to report to the responsible Minister from time to time on the need for or desirability of amending those IPPs; (f) to examine any proposed legislation that makes provision for (i) the collection of personal information by any public sector agency; or (ii) the disclosure of personal information by one public sector agency to any other public sector agency, or both; to have particular regard, in the course of that examination, to the matters set out in Section 98, in any case where the Commissioner considers that the information might be used for the purposes

Section 17: (1) The functions of the Commissioner are: (a) to exercise the powers, and carry out the functions and duties, conferred on the Commissioner by or under this Act or any other enactment; (b) to provide advice (with or without a request) to a Minister, a Parliamentary Under-Secretary or an agency on any matter relevant to the operation of this Act; (c) to promote, by education and publicity, an understanding and acceptance of the IPPs and of the objectives of those principles; (d) to make public statements in relation to any matter affecting the privacy of individuals; (e) to receive and invite representations from members of the public on any matter affecting the privacy of individuals; (f) to consult and co-operate with other persons and bodies concerned with the privacy of individuals; (g) to examine any proposed legislation (including subordinate legislation) or proposed government policy that the Commissioner considers may affect the privacy of individuals, including any proposed legislation that makes provision for either or both of the following: (i) the collection of personal information by a public sector agency; (ii) the sharing of personal information between public sector agencies (including parts of public sector agencies); (h) to monitor the use of unique identifiers; (i) to inquire generally into any matter, including any other enactment or any law, or any practice, or

Tasks of Authority (cont'd)

enforcement of this Regulation;
 (h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;
 (i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;
 (j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);
 (k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);
 (l) give advice on the processing operations referred to in Article 36(2);
 (m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);
 (n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);
 (o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);
 (p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
 (q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification;

of an information matching programme; and to report to the responsible Minister the results of that examination;
 (g) for the purpose of promoting the protection of individual privacy, to undertake educational programmes on the Commissioner's own behalf or in co-operation with other persons or authorities acting on behalf of the Commissioner;
 (h) to make public statements in relation to any matter affecting the privacy of the individual or of any class of individuals;
 (i) to receive and invite representations from members of the public on any matter affecting the privacy of the individual;
 (j) to consult and co-operate with other persons and bodies concerned with the privacy of the individual;
 (k) to make suggestions to any person in relation to any matter that concerns the need for, or the desirability of, action by that person in the interests of the privacy of the individual; (l) to provide advice (with or without a request) to a Minister or an agency on any matter relevant to the operation of this Act;
 (m) to inquire generally into any matter, including any enactment or law, or any practice, or procedure, whether governmental or non-governmental, or any technical development, if it appears to the Commissioner that the privacy of the individual is being, or may be, infringed thereby;
 (n) to undertake research into, and to monitor developments in, data processing and computer technology to ensure that any adverse effects of such developments on the privacy of individuals are minimised, and to report to the responsible Minister the results of such research and monitoring; (o) to examine any proposed legislation

procedure, whether governmental or non-governmental, or any technical development, if it appears to the Commissioner that the privacy of individuals is being, or may be, infringed (for powers of the Commissioner in relation to inquiries, see Section 203);
 (j) to undertake research into, and to monitor developments in, data processing and technology to ensure that any adverse effects of the developments on the privacy of individuals are minimised;
 (k) to give advice to any person in relation to any matter that concerns the need for, or desirability of, action by that person in the interests of the privacy of individuals;
 (l) when requested to do so by an agency, to conduct an audit of personal information maintained by that agency for the purpose of ascertaining whether the information is maintained according to the IPPs;
 (m) to monitor the operation of this Act and consider whether any amendments to this Act are necessary or desirable;
 (n) to report to the responsible Minister on the results of (i) any examination conducted under paragraph (g); (ii) the monitoring undertaken under paragraph (h); (iii) the research and monitoring undertaken under paragraph (j); (iv) the monitoring and consideration undertaken under paragraph (la);
 (o) to report to the Prime Minister of (i) any matter affecting the privacy of individuals, including the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the privacy of individuals; (ii) the desirability of New Zealand accepting any international instrument relating to the privacy of

Tasks of Authority (cont'd)

body pursuant to Article 43;
 (r) authorise contractual clauses and provisions referred to in Article 46(3);
 (s) approve binding corporate rules pursuant to Article 47;
 (t) contribute to the activities of the Board;
 (u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and
 (v) fulfil any other tasks related to the protection of personal data.

(including subordinate legislation) or proposed policy of the Government that the Commissioner considers may affect the privacy of individuals, and to report to the responsible Minister the results of that examination;
 (p) to report (with or without request) to the Prime Minister from time to time on any matter affecting the privacy of the individual, including the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the privacy of the individual;
 (q) to report to the Prime Minister from time to time on the desirability of the acceptance, by New Zealand, of any international instrument relating to the privacy of the individual;
 (r) to report to the Prime Minister on any other matter relating to privacy that, in the Commissioner's opinion, should be drawn to the Prime Minister's attention;
 (s) to gather such information as in the Commissioner's opinion will assist the Commissioner in carrying out the Commissioner's functions under this Act;
 (t) to do anything incidental or conducive to the performance of any of the preceding functions;
 (u) to exercise and perform such other functions, powers, and duties as are conferred or imposed on the Commissioner by or under this Act or any other enactment.
 [...] (1A) Except as expressly provided otherwise in this or another Act, the Commissioner must act independently in performing his or her statutory functions and duties, and exercising his or her statutory powers, under (a) this Act; and (b) any other Act that expressly provides for the functions, powers,

individuals; (iii) any other matter relating to the privacy of individuals that, in the Commissioner's opinion, should be drawn to the Prime Minister's attention;
 (p) to gather any information that will assist in carrying out the functions in paragraphs (a) to (n).
 (2) The Commissioner may at any time, if it is in the public interest or in the interests of any person or body of persons to do so, publish (a) reports relating generally to the performance of the Commissioner's functions under this Act; (b) reports relating to any case or cases investigated by the Commissioner.
 (3) Subsection (2) applies regardless of whether the matters to be dealt with in a report under that subsection have been the subject of a report to the responsible Minister or the Prime Minister.
 Section 18: (1) The responsible Minister may, for any of the following purposes, request the Commissioner to provide advice on whether a binding scheme requires a foreign person or entity to protect personal information in a way that, overall, provides comparable safeguards to those in this Act: (a) to assist the Minister in deciding whether to recommend the making of regulations under Section 213 prescribing the binding scheme; (b) to assist the Minister in deciding whether any regulations made under Section 213 prescribing the binding scheme should be - (i) continued without amendment; or (ii) continued with amendment; or (iii) revoked; or (iv) replaced.
 (2) The responsible Minister may, for the following purposes, request the Commissioner to provide advice on whether the privacy laws of a country, overall, provide comparable

Tasks of Authority (cont'd)

or duties of the Commissioner (other than the Crown Entities Act 2004).

(2) The Commissioner may from time to time, in the public interest or in the interests of any person or body of persons, publish reports relating generally to the exercise of the Commissioner's functions under this Act or to any case or cases investigated by the Commissioner, whether or not the matters to be dealt with in any such report have been the subject of a report to the responsible Minister or the Prime Minister.

safeguards to those in this Act: (a) to assist the Minister in deciding whether to recommend the making of regulations under Section 214 prescribing the country;

(b) to assist the Minister in deciding whether any regulations made under Section 214 prescribing the country should be - (i) continued without amendment; or (ii) continued with amendment; or (iii) revoked;

(c) to assist the Minister in deciding whether, for the purposes in paragraph (a) or (b)(i) or (ii), the country should be subject to any limitation or qualification of the kind specified in Section 214(3).

Section 20: The Commissioner must act independently in performing statutory functions and duties, and exercising statutory powers, under (a) this Act; and (b) any other act that expressly provides for the functions, powers, or duties of the Commissioner (other than the Crown Entities Act 2004).

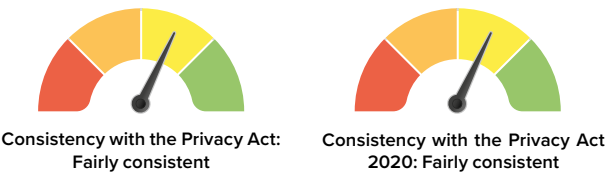
Annual Report

Article 59: Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

Section 24(1): Without limiting the right of the Commissioner to report at any other time, but subject to Section 120, the annual report of the Commissioner under Section 150 of the Crown Entities Act 2004 must include a report with respect to the operation of this Act during the year to which the report relates.

The Privacy Act 2020 does not stipulate that the OPC must provide an annual report, however there are alternative reporting requirements (see Section 17 above).

6.3. Other remedies



Like the GDPR, both the Privacy Act and the Privacy Act 2020 provide for civil remedies for damages that may be material or non-material in nature, but do not detail a process for calculating the amount for such damages. Neither the Privacy Act nor the Privacy Act 2020 specifically refer to processor liabilities, however they do outline general liabilities.

GDPR	Privacy Act	Privacy Act 2020
Provides for Claims/Cause of Action		
Article 79: Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.	Section 85: If, in any proceedings under Section 82 or Section 83, the Tribunal is satisfied on the balance of probabilities that any action of the defendant is an interference with the privacy of an individual, it may grant 1 or more of the following remedies: [...] (c) damages in accordance with Section 88; (d) an order that the defendant perform any acts specified in the order with a view to remedying the interference, or redressing any loss or damage suffered by the aggrieved individual as a result of the interference, or both; (e) such other relief as the Tribunal thinks fit.	Section 102: (2) If, in the proceedings, the Tribunal is satisfied on the balance of probabilities that any action of the defendant is an interference with the privacy of an 1 or more individuals, the Tribunal may grant 1 or more of the following remedies; [...] (c) damages in accordance with Section 108; (d) an order that the defendant perform any acts specified in the order with a view to remedying the interference, or redressing any loss or damage suffered by the aggrieved individual as a result of the interference, or both; (e) any other relief that the Tribunal considers appropriate.

Material and Non-Material Damage		
Article 82(1): Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.	Section 88(1): In any proceedings under Section 82 or Section 83, the Tribunal may award damages against the defendant for an interference with the privacy of an individual in respect of any 1 or more of the following (a) pecuniary loss suffered as a result of, and expenses reasonably incurred by the aggrieved individual for the purpose of, the transaction or activity out of which the interference arose; (b) loss of any benefit, whether or not of a monetary kind, which the aggrieved individual might reasonably have been expected to obtain but for the interference; and/or (c) humiliation, loss of dignity, and injury to the feelings of the aggrieved individual.	Section 103: (1) In any proceedings, the Tribunal may award damages against the defendant for an interference with the privacy of an individual in respect of 1 or more of the following: (a) pecuniary loss suffered as a result of the transaction or activity out of which the interference arose; (b) expenses reasonably incurred by the aggrieved individual for the purpose of the transaction or activity out of which the interference arose; (c) loss of any benefit, whether or not of a monetary kind, that the aggrieved individual might reasonably have been expected to obtain but for the interference; and/or

Material and Non-Material Damage

(d) humiliation, loss of dignity, and injury to the feelings of the aggrieved individual.

(2) If the proceedings are brought on behalf of more than one aggrieved individual, the Tribunal may award damages under Subsection (1) to each aggrieved individual.

Mandate for Representation

Article 80(1): The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

The Privacy Act does not explicitly address this matter.

The Privacy Act 2020 provides that aggrieved individuals may be represented and that representatives may commence proceedings in a Tribunal (see Section 98).

Specifies Amount for Damages

Not applicable.

The Privacy Act does not specify amounts for damages.

The Privacy Act 2020 does not specify amounts for damages.

Processor Liability

Article 82(2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations

Section 126: Subject to subsection (4), anything done or omitted by a person as the employee of another person shall, for the purposes of this Act, be treated as done or omitted by that other person as well as by the first-mentioned person, whether or not it was done with that

Section 211: For the purpose of this Act, (a) anything done or omitted to be done by a person (A) as an employee of another person (B) is to be treated as being done or omitted by both A and B, whether or not it was done or omitted with B's knowledge or approval;

Processor Liability (cont'd)

of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

other person's knowledge or approval.

(2) Anything done or omitted by a person as the agent of another person shall, for the purposes of this Act, be treated as done or omitted by that other person as well as by the first-mentioned person, unless it is done or omitted without that other person's express or implied authority, precedent or subsequent.

(3) Anything done or omitted by a person as a member of any agency shall, for the purposes of this Act, be treated as done or omitted by that agency as well as by the first-mentioned person, unless it is done or omitted without that agency's express or implied authority, precedent or subsequent.

(4) In proceedings under this Act against any person in respect of an act alleged to have been done by an employee of that person, it shall be a defence for that person to prove that he or she or it took such steps as were reasonably practicable to prevent the employee from doing that act, or from doing as an employee of that person acts of that description.

(b) anything done or omitted to be done by a person (A) as an agent of another person (B) is to be treated as being done or omitted by both A and B, unless it was done or omitted without B's express or implied authority;

(c) anything done or omitted to be done by a person as a member of an agency is to be treated as being done or omitted by both the person and the agency, unless it is done or omitted without the agency's express or implied authority.

(2) In proceedings under this Act against any person (C) in respect of an act alleged to have been done by an employee of that person (D), it is a defence to prove that C took such steps as were reasonably practicable to prevent D from doing that or any similar act.

(3) Subsection (2) overrides subsection (1)(a).

(4) This Section is subject to Sections 122AA and 122AB.

Exceptions

Article 82(3): A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

Section 87: Where, by any provision of the IPPs or of this Act or of a code of practice issued under Section 46 or Section 63, conduct is excepted from conduct that is an interference with the privacy of an individual, the onus of proving the exception in any proceedings under this Part lies upon the defendant.

Section 105: If an apology is given by an agency in connection with an action alleged to be an interference with the privacy of an individual, it is not admissible as evidence in any civil proceedings against the agency under this Part except as provided in subsection (2).

(2) An agency may bring evidence of the apology for the purpose of the Tribunal's assessment of remedies to be awarded against the agency.

Section 106: If any provision of this Act, or any code of practice, excepts

Processor Liability (cont'd)

or exempts any action from being an interference with the privacy of an individual, the defendant has the onus of proving that exception or exemption in any proceedings under this Part.



