Foundation Life (NZ) Limited

Privacy Policy

Issue Date:	December 2015
Review date	November 2024
Next Review:	December 2025
Version:	V11 - Reviewed November 2024
Applies to:	All Staff
Policy Owner:	Chief Executive Officer

Table of Contents

Table of Contents 1

Introduction 2

1. Application of this Policy 2

2. What is personal information? 2

3. Privacy Officer 3

4. Protection of personal information 3

5. Health Information Privacy Code 7

6. Privacy breach 7

7. Data retention and destruction 8

8. Further information 9

9. Review of policy 9

Schedule 1 10

Privacy Act 13 Information Privacy Principles 10

Schedule 2 17

New Zealand and Australian Privacy Commissioner and European Union Supervisory Authorities contact information. 17

Introduction

Foundation Life (NZ) Limited ("FLNZ") is committed to protecting the privacy of its customers, advisors, employees, directors and shareholders in accordance with the New Zealand Privacy Act 2020[1] (NZ PA), the General Data Protection Regulation (EU-GDPR), and the Australian Privacy Act 1988 (AU PA).

FLNZ has adopted this Policy to govern the collection, use, storage, disclosure and retention and disposal of personal information. It is the responsibility of all FLNZ personnel to protect personal information. Compliance with this Policy is mandatory.

1. Application of this Policy

1.1 This Policy takes effect immediately. It will be reviewed from time to time and may be amended or supplemented.

1.2 This Policy applies to all personal information collected, held, stored, transferred or otherwise used by FLNZ and to the management of that personal information.

2. What is personal information?

2.1 Personal information means information about an identifiable individual that is not publicly available information and includes information in any form, whether oral, electronic or written. Personal information may include (but is not limited to):

2.1.1 Name, gender, home address and telephone number, date of birth, marital status, emergency contacts.

2.1.2 Residency and work permit status, military status, nationality and passport information.

2.1.3 Inland Revenue Department number or Tax Identification Number relevant to the country of residence.

2.1.4 Automatic Exchange of Financial Account Information in Tax Matters (AEOI) information. For policies held by overseas residents.

2.1.5 Financial and investment records, banking details.

2.1.6 Health records, certifications and test results.

2.1.7 Height, weight, photograph, physical limitations and special needs.

2.1.8 Where permitted by law, the results of credit and criminal background checks, the results of drug and alcohol testing, screening, driving license number, vehicle registration and driving history.

2.1.9 Information captured on security systems, including CCTV.

2.1.10 Voicemails, emails, correspondence and other communications created, stored or transmitted using FLNZ's computer or communications equipment including tapes of recorded telephone calls, website and mobile applications.

[1] https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html

2.2 Personal information classified as 'Special Category' data by the EU-GDPR is collected for the purposes of carrying out the business of FLNZ. Data processing is necessary for performance of the life insurance contract held with FLNZ.

2.3 FLNZ also collects information from clients residing in Australia and has obligations to these clients under the Australian Privacy Act of 1988 and the Notifiable Data Breaches scheme (NDB). Personal data collected from these clients is necessary for the performance of the life insurance contract held with FLNZ.

3. Privacy Officer

3.1 FLNZ's privacy officer, Tracey Thorpe, can be contacted at tracey.thorpe@foundationlife.co.nz

3.2 FLNZ's privacy officer is responsible for all privacy related issues and will:

3.2.1 Handle privacy queries and complaints.

3.2.2 Be aware of privacy risks and address them.

3.2.3 Arrange training to all FLNZ personnel regarding their privacy obligations.

3.2.4 Provide guidance in respect of requests for access to, or correction of, personal information.

3.2.5 Be FLNZ's person of contact with the Privacy Commissioner and other third parties.

3.3 Any questions relating to privacy obligations should be referred to the privacy officer.

4. Protection of personal information

4.1 General

4.1.1 Personal information for NZ residents must be collected, used, stored, disclosed and retained in accordance with the NZ PA.

4.1.2 Personal information for European Union residents must be collected, used, stored, disclosed and retained in accordance with the EU-GDPR.

4.1.3 Personal information for Australian residents must be collected, used, stored, disclosed and retained in accordance with the AU PA.

4.1.4 FLNZ's website privacy policy can be found at: http://www.foundationlife.co.nz/privacy.html

4.1.5 The NZ PA has 13 information privacy principles. The complete text is set out in Schedule 1.

4.1.6 The EU-GDPR has 99 articles related to the protection of data subjects' information and further information can be accessed at https://www.gdpr.org.

4.1.7 The AU PA has 13 information privacy principles and information about these can be accessed at https://www.legislation.gov.au/details/c2014c00076

Collection of personal information (NZ PA principles 1-4), (EU-GDPR articles 5, 6, 9, 32), (AU PA part 2, principle 3).

4.1.8 Personal information may only be collected for a lawful purpose connected with a function or activity of FLNZ and the collection of the information must be necessary for that purpose.

4.1.9 The personal information must be collected directly from the individual concerned unless FLNZ believes on reasonable grounds that a specified exception applies (for example, that the non-compliance would not prejudice the interests of the individual concerned, compliance would prejudice the purposes of the collection, the information is publicly available, the individual concerned authorizes the collection of the information from someone else or that compliance is not reasonably practicable in the circumstances of the particular case).

4.1.10 Before collecting the information (or, if that is not practicable, as soon as practicable after the information is collected), reasonable steps must be taken to ensure that the individual is aware (unless FLNZ believes, on reasonable grounds, that one of the exceptions apply):

a) that the information is being collected;

b) why the information is being collected;

c) who at FLNZ will receive and use the information;

d) the name and address of the FLNZ entity collecting and holding the information;

e) if the collection of the information is authorised or required by law, the relevant law and whether or not the supply of the information is voluntary or mandatory;

f) the consequences (if any) if the requested information is not provided; and

g) the rights of access to, and correction of, the personal information.

4.1.11 Personal information must be collected by lawful means and in a manner (particularly in circumstances where personal information is being collected from children or young persons) that is fair and does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

4.2 Storage and security of personal information (NZ PA principle 5), (EU-GDPR articles 5, 9, 30, 32), (AU PA principle 11)

4.2.1 Personal information must be protected by reasonable security safeguards to prevent:

a) loss;

b) unauthorized access, use, modification or disclosure; and

c) other misuse.

4.2.2 If it is necessary for personal information to be given to a person outside of FLNZ in connection with the carrying on of FLNZ's business, everything reasonable must be done to prevent unauthorised use or unauthorised disclosure of the information.

4.2.3 Every area at FLNZ must establish adequate safeguards and protocols to store and use information in a secure way, including:

a) **physical security** of premises, rooms, cabinets holding records or computer systems and electronic files, identifying who has access and any appropriate levels of access;

b) **operational security** prohibiting printing any password or PIN online, giving a password or PIN to others unless required for technical services or maintenance, writing down a password or PIN in a place where others may find it, or allowing a password or PIN to be used by others;

c) **remote access** through secure Virtual Private Network (VPN) connections;

d) **technical security** relating to managing computer systems and networks to guard against unauthorised access, viruses, corruption of data etc. including implementing a business continuity plan or disaster recovery plan;

e) **security of transmission** including guidelines for use of mail, email, and other mobile devices and applications that may be used to transmit information or data;

f) **transfer of information** or records only to the individual concerned or a designated agent; and

g) **destruction** of physical records and electronic records and files in a secure way when they are no longer needed; in accordance with Governance New Zealand guidelines, this will be 10 years after either lapse of policy or policy being paid out.

4.2.4 FLNZ uses a cloud-based service provider (Microsoft Azure Cloud) to store information. When information is passed on to our cloud-based service provider, we take steps to ensure it is treated in the same way that we would treat it, and that, through our contract with the provider, an adequate level of protection is in place in accordance with relevant privacy and data protection laws.

4.3 Access to and correction of personal information (NZ PA principles 6 and 7, and parts 4 and 5), (EU-GDPR articles 12, 13-22), (AU PA principle12 and 13)

4.3.1 An individual is entitled to:

a) obtain from FLNZ confirmation of whether or not FLNZ holds personal information about them; and
b) access that information.

4.3.2 Where an individual submits a request for personal information, FLNZ 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 decide whether to grant the request, and in what manner, and inform the individual of its decision.

4.3.3 Where an individual is given access to personal information FLNZ will advise that individual of the right to request the correction of that information.

4.3.4 FLNZ may (in accordance with parts 4 and 5 of the NZPA decide to withhold personal information on specific permitted grounds or transfer the request to another appropriate organisation. FLNZ may charge a reasonable fee for dealing with a request.

4.3.5 FLNZ personnel must refer all requests for access to personal information to the privacy officer. The privacy officer will keep a register of all requests for personal information, detailing the substance of the request, the outcome and the basis of the decision.

4.3.6 An individual is entitled to request FLNZ to correct personal information held by FLNZ about the individual. When requesting the correction of personal information, or at any later time, an individual is entitled to provide FLNZ with a statement of the correction sought and request FLNZ to attach the statement of correction to the information if FLNZ does not make the correction sought.

4.3.7 If FLNZ is not willing to correct the information and has been provided with a statement of correction, FLNZ must take reasonable steps to ensure that the statement of correction is attached to the information in a manner that ensure that it will always be read with the information.

4.3.8 If FLNZ corrects personal information or attaches a statement of correction to personal information, FLNZ must, so far as is reasonably practicable, inform every other person to whom FLNZ has disclosed the information.

4.4 Use and disclosure of personal information (NZ PA principles 8 to 11), (AU PA principles 6 and 8)

4.4.1 Personal information must not be used without taking reasonable steps to ensure that the information is accurate, up to date, complete, relevant and not misleading.

4.4.2 FLNZ must not keep information for longer than is required for the purposes for which the information may lawfully be used. Where personal information is no longer required to be kept, it must be disposed of in a manner that preserves the privacy of the individual concerned.

4.4.3 Personal information must not be used or disclosed for any purpose other than one of the purposes in connection with the purpose for which it was collected. There are certain exceptions to this requirement including where the information is publicly available, the individual's authority has been obtained, the proposed use or disclosure is required by law or is directly connected to the purpose for which it was collected. FLNZ personnel must discuss the matter with the privacy officer before relying on any exceptions.

4.4.4 When speaking to an individual, at the outset, FLNZ personnel must ensure that the individual is properly identified using a minimum of two identifier checks (e.g. date of birth, telephone number).

4.4.5 Personal information must not be disclosed to any third party without the authorisation of the privacy officer, unless disclosure is required in the normal course of business.

4.5 Disclosure of personal information outside of New Zealand (NZ PA principle 12)

4.5.1 FLNZ may disclose personal information to a foreign person or entity only if:

a) The individual concerned authorizes the disclosure after being expressly informed by FLNZ that the foreign entity may not be required to protect the information in a way that, overall, provides comparable safeguards to those in the NZ PA;

b) FLNZ believes on reasonable grounds that the foreign entity is subject to privacy laws that, overall, provide comparable safeguards to those in the NZ PA; or

c) FLNZ otherwise believes on reasonable grounds that the foreign entity is required to protect the information in a way that, overall, provides comparable safeguards to those in the NZ PA (for example pursuant to an agreement entered into between FLNZ and the foreign entity).

4.6 Unique identifiers (NZ PA principle 13)

4.6.1 FLNZ assigns each of its policyholders with a unique policy number to identify a person in relation to the relevant policy, in order for FLNZ to carry out its functions efficiently. Policy numbers are only assigned to an individual whose identity has been clearly established.

5. Health Information Privacy Code

5.1.1 In the course of its business as a life insurer, FLNZ collects, uses and stores health information about individuals. The Health Information Privacy Code 2020 (as amended)[1] sets specific rules applicable to the health sector to better ensure the protection of individual privacy. The code applies to the health information collected, used, held and disclosed by FLNZ in respect of health information and takes the place of the information privacy principles. FLNZ personnel processing health information must read and comply with the code.

6. Privacy breach

6.1 A privacy breach is any unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, the personal information or any action that prevents the agency from accessing the information on either a temporary or permanent basis. It does not matter whether or not the breach was caused by a person inside the agency, is attributable in whole or in part to any action by the agency, or is ongoing. (Part 6 of the NZ PA), (EU-GDPR articles 32-34, NDB scheme)

6.2 If FLNZ personnel know or suspect that a privacy breach has occurred, the privacy officer must be notified immediately.

6.3 The privacy officer will take steps to:

6.3.1 Contain the breach.

6.3.2 Identify what personal information is involved.

6.3.3 Establish the cause and extent of the breach.

6.3.4 Consider who is affected by the breach.

6.3.5 Identify whether harm could foreseeably result from the breach.

6.3.6 Consider whether affected individuals should be notified.

6.3.7 Consider whether the Privacy Commissioner should be notified.

6.3.8 Consider how to prevent further breaches.

6.3.9 Notify the CEO immediately.

[1] https://www.privacy.org.nz/assets/New-order/Privacy-Act-2020/Codes-of-practice/Health-information-privacy-code-2020/HIPC-Amendment-No-1/Consolidated-Code-incorporating-Amendment-No-1.pdf

6.4 The privacy officer will document any privacy breach in a privacy breach report.

6.5 If a breach involves a New Zealand client, whether a privacy breach is notifiable to the Privacy Commissioner depends on whether the privacy breach is a "notifiable privacy breach". Please refer to Schedule 2 for contact details.

6.6 A "notifiable privacy breach" is a privacy breach that it is reasonable to believe has caused "serious harm" to an affected individual, or is likely to do so.

6.7 "Serious harm" is not defined in the Privacy Act, but would generally include harms such as identity theft.

6.8 It is worthwhile noting that the "serious harm" must be caused to the affected individual in order for there to be a notifiable privacy breach.

6.9 FLNZ must consider the factors in section 113 of the NZ PA when assessing whether a privacy breach is likely to cause serious harm, which include:

6.9.1 action taken by the agency to reduce the risk of harm following the breach;

6.9.2 whether the personal information is sensitive in nature;

6.9.3 the nature of the harm that may be caused to affected individuals;

6.9.4 who has obtained or may obtain personal information as a result of the breach (if known);

6.9.5 whether the personal information is protected by a security measure; and

6.9.6 any other relevant matters.

6.10 If a breach involves an EU client and the breach is likely to result in a high risk to the rights and freedoms of the client, then both they and the Supervisory Authority of the country of residence will be notified within 72 hours (articles 32-34, 55)[2]. Please refer to Schedule 2 for details of Supervisory Authorities in the EU.

6.11 If a breach involves an Australian client when it is likely to result in serious harm and FLNZ is unable to prevent the likely risk of serious harm with any remedial action, then the Office of the Australian Information Commissioner and the client involved will be notified. Please refer to Schedule 2 for contact details.

6.12 As part of FLNZ's compliance with the legislation covering our clients, regular testing of client data security will be carried out (article 32) (NDB).

7. Data retention and destruction

7.1 All personal information provided to FLNZ will be held by FLNZ for the purpose of providing services and to respond to requests in relation to life insurance contracts held with FLNZ.

7.2 All personal information provided to FLNZ will be held on the physical file for the life of the policy.

7.3 All personal information held on the physical file will be destroyed 10 years after the policy lapses or is fully paid out.

7.4 All personal information provided to FLNZ via telephone calls will be held for a period of 12 months.

[2] https://www.gdpr.org/regulation/article-32.html

8. Further information

8.1 For further information relating to FLNZ's privacy obligations, the Privacy Act, the information privacy principles or the code, contact the privacy officer.

8.2 Additional guidance can also be found at the Privacy Commissioner's website.

9. Review of policy

This policy will be reviewed annually.

CEO	Director
Name: Grant Piercy	Name: Board Approved
Date: 8 November 2024	Date:

Schedule 1

Privacy Act 13 Information Privacy Principles

Information privacy principle 1

Purpose of collection of personal information

(1) Personal information must not be collected by an agency unless—

(a) the information is collected for a lawful purpose connected with a function or an 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.

Information privacy principle 2

Source of personal information

(1) 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 compliance would prejudice the purposes of the collection; or

(c) that the individual concerned authorises collection of the information from someone else; or

(d) that the information is publicly available information; or

(e) 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

(v) to prevent or lessen a serious threat to the life or health of the individual concerned or any other individual; or

(vi) 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.

Information privacy principle 3

Collection of information from subject

(1) If an agency collects personal information from the individual concerned, the agency must take any steps that 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 authorised or required; and

(ii) whether the supply of the information by that individual is voluntary or mandatory; and

(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, information provided by the IPPs.

(2) The steps referred to in subclause (1) must be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected.

(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.

Information privacy principle 4

Manner of collection of personal information

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.

Information privacy principle 5

Storage and security of personal information

An agency that holds personal information must ensure —

(a) that the information is protected, by such security safeguards as are reasonable in the circumstances to take, against—

(i) loss; and

(ii) access, use, modification, or disclosure that is not authorised by the agency; and

(iii) other misuse; and

(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.

Information privacy principle 6

Access to personal information

(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.

(2) If an individual concerned is given access to personal information, the individual must be advised that, under IPP 7, the individual may request the correction of that information.

(3) This IPP is subject to the provisions of **Part 4**.

Information privacy principle 7

Correction of personal information

(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 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 (4) are subject to the provisions of Part 4.

Information privacy principle 8

Accuracy, etc, of personal information to be checked before use or disclosure

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.

Information privacy principle 9

Agency not to keep personal information for longer than necessary

An agency that holds personal information must not keep that information for longer than is required for the purposes for which the information may lawfully be used.

Information privacy principle 10

Limits on use of personal information

(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,—

(a) that the purpose for which the information is to be used is directly related to the purpose in connection with which the information was obtained; or

(b) 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

(c) that the use of the information for that other purpose 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 use the information; or

(e) that the use of the information for that other purpose 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

(f) that the use of the information for that other purpose 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.

(2) In addition to the uses authorised by subclause (1), an intelligence and security agency that holds personal information that was obtained in connection with one purpose may use the information for any other purpose (a secondary purpose) if the agency believes on reasonable grounds that the use of the information for the secondary purpose is necessary to enable the agency to perform any of its functions.

Information privacy principle 11

Limits on disclosure of personal information

(1) An agency that holds personal information must not disclose the information to any other agency or to any person 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, 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

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

(2) This IPP is subject to IPP 12.

Information privacy principle 12

Disclosure of personal information outside New Zealand

(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; or

(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; or

(c) A believes on reasonable grounds that B is subject to privacy laws that, overall, provide comparable safeguards to those in this Act; or

(d) A believes on reasonable grounds that B is a participant in a prescribed binding scheme; or

(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 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 IPP,—

prescribed binding scheme means a binding scheme specified in regulations made under section 213

prescribed country means a country specified in regulations made under section 214.

Information privacy principle 13

Unique identifiers

(1) An agency (A) may assign a unique identifier to an individual for use in its operations only if that identifier is necessary to enable A to carry out 1 or more of its functions efficiently.

(2) A may not assign to an individual a unique identifier that, to A's knowledge, is the same unique identifier as has been assigned to that individual by another agency (B), unless —

(a) A and B are associated persons within the meaning of **subpart YB** of the Income Tax Act 2007; or

(b) the unique identifier is to be used by A for statistical or research purposes and no other purpose.

(3) To avoid doubt, A does not assign a unique identifier to an individual under subclause (1) by simply recording a unique identifier assigned to the individual by B for the sole purpose of communicating with B about the individual.

(4) A must take any steps that are, in the circumstances, reasonable to ensure that —

(a) a unique identifier is assigned only to an individual whose identity is clearly established; and

(b) the risk of misuse of a unique identifier by any person is minimised (for example, by showing truncated account numbers on receipts or in correspondence).

(5) An agency may not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or is for a purpose that is directly related to one of those purposes.

Schedule 2

New Zealand and Australian Privacy Commissioner and European Union Supervisory Authorities contact information.

Office of the Privacy Commissioner New Zealand

Email	enquiries@privacy.org.nz
Phone	0800 803 909
Street Address	Office of the Privacy Commissioner New Zealand PO Box 10 094 Wellington 6140

Visits to their office are by appointment only.

Office of the Australian Information Commissioner

Email	enquiries@oaic.gov.au
Phone	+00 61 1300 363 992
Post	GPO Box 5218 Sydney, NSW 2001 Australia
Street Address	Office of the Australian Information Commissioner Level 3, 175 Pitt Street Sydney, NSW 2000 Australia

European Union Supervisory Authorities

The DPA (Data Protection Authority) is the agency within each European Union country that is responsible for GDPR (General Data Protection Regulation) assistance and enforcement.

What's the difference between a Data Protection Authority and a Supervisory Authority?

A Data Protection Authority handles reports of data breaches, mediates issues like data subject access requests and works to educate their country about best practices in keeping digital data secure. The Supervisory Authority is which particular Data Protection Authority has jurisdiction over a particular matter.

Because online services are so intertwined it's quite common to have situations where it's a German citizens data that is being held by a French company.

Who should have jurisdiction over the matter? Should it be France's Commission Nationale de l'Informatique et des Libertés (CNIL) or the German Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit?

The answer: it's complicated (and in truth would rely upon some factors not presented in this extremely simplified example). However, whichever agency ends up with jurisdiction would be the DPA that was acting as the Supervisory Authority for the matter.

Why you need every DPA's Contact Information

As either a data controller or data processor, you will be responding to requests for data from users of your system. Per Article 12 of the GDPR you may need to inform them of which supervisory authority they can escalate to if you exceed the initial 30 day grace period for a request.

Additionally, at the time of consent (when the user says: 'I do' to you collecting their personal information) you need to inform them their right to lodge a complaint with a supervisory authority. This and other consent requirements are spelled out in Article 13.

EUROPEAN ECONOMIC UNION	
Austria	Österreichische Datenschutzbehörde Barichgrasse 40-42 1030 Wein Tel. +43 1 52 152-0 dsb@dsb.gv.at http://www.dsb.gv.at/
Belgium	Commission de la protection de la vie privée Commissie voor de bescherming van de persoonlijke levenssfeer Rue de la Presse 35 / Drukpersstraat 35 1000 Bruxelles / 1000 Brussel Tel. +32 2 274 48 00 Fax +32 2 274 48 35 commission@privacycommission.be http://www.privacycommission.be/
Bulgaria	Commission for Personal Data Protection 2, Prof. Tsvetan Lazarov blvd. Sofia 1592 Tel. +359 2 915 3580 Fax +359 2 915 3525 kzld@cpdp.bg http://www.cpdp.bg/
Croatia	Croatian Personal Data Protection Agency Selska cesta 136 10000 Zagreb Tel. +385 1 4609 000 Fax +385 1 4609 099 azop@azop.hr or info@azop.hr http://www.azop.hr/

Cyprus	Commissioner for Personal Data Protection 1 Iasonos Street, 1082 Nicosia P.O. Box 23378, CY-1682 Nicosia Tel. +357 22 818 456 Fax +357 22 304 565 commissioner@dataprotection.gov.cy http://www.dataprotection.gov.cy/

Czech Republic	The Office for Personal Data Protection Urad pro ochranu osobnich udaju Pplk. Sochora 27 170 00 Prague 7 Tel. +420 234 665 111 Fax +420 234 665 444 posta@uoou.cz http://www.uoou.cz/
Denmark	Datatilsynet Carl Jaobsens Vej 35 2500 Valby Tel. +45 33 1932 00 dt@datatilsynet.dk http://www.datatilsynet.dk/
Estonia	Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon) Tatari 39 10134 Tallinn Tel. +372 6828 712 info@aki.ee http://www.aki.ee/en
Finland	Office of the Data Protection Ombudsman P.O. Box 800 FL-00531 Helsinki Tel. +358 10 3666 700 Fax +358 10 3666 735 tietosuoja@om.fi http://www.tietosuoja.fi/en/
France	Commission Nationale de l'Informatique et des Libertés – CNIL 3 Place de Fontenoy TSA 80715-75334 Paris, Cedex 07 Tel. +33 1 53 73 22 22 Fax +33 1 53 73 22 00 http://www.cnil.fr/
Germany	Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Graurheindorferstraße 153 53117 Bonn Tel. +49 228 997799 0; +49 228 81995 0 Fax +49 228 997799 550; +49 228 81995 550 zast@bfdi.bund.de http://www.bfdi.bund.de/

Germany splits complaints among a number of different agencies, to sort out which one applies, use: The Federal Commissioner for Data Protection and Freedom of Information

Germany does not have one central Data Protection Authority but a number of different Authorities for each of the 16 German states (Länder) that are responsible for making sure that data protection laws and regulations are complied with. In addition the German Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragte für Datenschutz und Informationsfreiheit – 'BfDI') is the Data Protection Authority for telecommunication service providers and represents Germany in the European Data Protection Board. To ensure that all the Authorities have the same approach a committee consisting of members of all Authorities has been established – the 'Data Protection Conference' (Datenschutzkonferenz 'DSK'). The coordination mechanism between the German Authorities mirrors the consistency mechanism under the GDPR.

Greece	Hellenic Data Protection Authority Kifisias Av. 1-3 11523 Ampelokipi Athens Tel. +30 210 6475 600 Fax +30 210 6475 628 contact@dpa.gr http://www.dpa.gr/
Hungary	National Authority for Data Protection and Freedom of Information Falk MiKSA UTCA 9-11 H-1055 Budapest Tel. +36 1 3911 400 PRIVACY@naih.hu http://www.naih.hu/
Ireland	Data Protection Commissioner 21 Fitzwilliam Square D02 RD28 Dublin 2 Tel. +353 76 110 4800 info@dataprotection.ie http://www.dataprotection.ie/
Italy	Garante per la protezione dei dati personali Piazza di Monte Citorio, 121 00186 Roma Tel. +39 06 69677 1 Fax +39 06 69677 785 segreteria.stanzione@gpdp.it http://www.garanteprivacy.it/
Latvia	Data State Inspectorate Director: Ms Jekaterina Macuka Elijas Street 17 LV-1050 Riga Tel. +371 6722 3131 Fax +371 6722 3556 info@dvi.gov.lv http://www.dvi.gov.lv/

Lithuania	State Data Protection L. Sapiegos str.17 LT-10312 Vilnius Tel. + 370 5 279 14 45 Fax +370 5 261 94 94 ada@ada.lt http://www.ada.lt/
Luxembourg	Commission Nationale pour la Protection des Données 1, avenue du Rock'n'Roll L-4361 Esch-sur-Alzette Tel. +352 2610 60 1 Fax +352 2610 60 29 info@cnpd.lu http://www.cnpd.lu/
Malta	Office of the Data Protection Commissioner Data Protection Commissioner: Mr Ian Deguara 2, Airways House High Street, Sliema SLM 1549 Tel. +356 2328 7100 Fax +356 2328 7198 commissioner.dataprotection@gov.mt http://www.dataprotection.gov.mt/
Netherlands	Autoriteit Persoonsgegevens Bezuidenhoutseweg 30 P.O. Box 93374 2509 AJ Den Haag/The Hague Tel. +31 70 888 8500 Fax +31 70 888 8501 info@autoriteitpersoonsgegevens.nl https://autoriteitpersoonsgegevens.nl/nl
Poland	The Bureau of the Inspector General for the Protection of Personal Data – GIODO ul. Stawki 2 00-193 Warsaw Tel. +48 22 53 10 440 Fax +48 22 53 10 441 kancelaria@giodo.gov.pl; desiwm@giodo.gov.pl http://www.giodo.gov.pl/
Portugal	Comissão Nacional de Protecção de Dados – CNPD Av. D. Carlos 1, 134,1o 1200-651 Lisboa Tel. +351 21 392 84 00 Fax +351 21 397 68 32 geral@cnpd.pt http://www.cnpd.pt/

Romania	The National Supervisory Authority for Personal Data Processing President: Mrs Ancuţa Gianina Opre B-dul Magheru 28-30 Sector 1, BUCUREŞTI Tel. +40 21 252 5599 Fax +40 21 252 5757 anspdcp@dataprotection.ro http://www.dataprotection.ro/
Slovakia	Office for Personal Data Protection of the Slovak Republic Hraničná 12 820 07 Bratislava 27 Tel.: + 421 2 32 31 32 14 Fax: + 421 2 32 31 32 34 statny.dozor@pdp.gov.sk http://www.dataprotection.gov.sk/

Slovenia	Information Commissioner Ms Mojca Prelesnik Dunajaska cesta 22 1000 Ljubljana Tel. +386 1 230 9730 Fax +386 1 230 9778 gp.ip@ip-rs.si https://www.ip-rs.si/
Spain	Agencia de Protección de Datos C/Jorge Juan, 6 28001 Madrid Tel. +34 91 266 3517 Fax +34 91 455 5699 internacional@agpd.es https://www.agpd.es/
Sweden	Datainspektionen Drottninggatan 29 5th Floor Box 8114 104 20 Stockholm Tel. +46 8 657 6100 Fax +46 8 652 8652 datainspektionen@datainspektionen.se http://www.datainspektionen.se/
United Kingdom	The Information Commissioner's Office Wycliffe House , Water Lane, Wilmslow, Cheshire SK9 5AF Tel. +44 303 123 1113 international.team@ico.org.uk https://ico.org.uk

EUROPEAN FREE TRADE AREA (EFTA)	
Iceland	Icelandic Data Protection Agency Rauðarárstíg 10 105 Reykjavík Tel. +354 510 9600 postur@dpa.is
Liechtenstein	Data Protection Office Stadtle 38 9490 Vaduz Principality of Liechtenstein Tel. +423 236 6090 info.dss@llv.li
Norway	Datatilsynet The Data Inspectorate Tollbugta 3 0152 Oslo Tel. +47 22 39 69 00; postkasse@datatilsynet.no
Switzerland	Data Protection and Information Commissioner of Switzerland Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter Mr Adrian Lobsiger Feldeggweg 1 3003 Bern Tel. +41 58 462 43 95; Fax +41 58 462 99 96 contact20@edoeb.admin.ch

Document Control

Document history

This table shows a record of changes to the document.

Version	Date	Changes	Reason for changes	Author	Date approved by Owner & ACC
V1	December 2016	No material changes	Annual review	Grant Piercy	8 December 2016
V2	December 2017	No material changes – Privacy offer updated.	Annual review	Grant Piercy	7 December 2017
V3	December 2018	No material changes	Annual review	Grant Piercy	11 December 2018
V4	December 2019	Additions throughout document to include GDPR and DNB requirements	Annual review	Grant Piercy	17 January 2020
V5	September 2020	Additions throughout document to include change to cloud-based server and to reflect changes in Privacy Act 2020	To incorporate Privacy Act 2020 updates	Grant Piercy	04 September 2020
V6	December 2020	No material changes	Annual review	Grant Piercy	17 December 2020
V7	December 2021	No material changes	Annual review	Grant Piercy	9 December 2021
V8	December 2022	No material changes	Annual review	Grant Piercy	5 December 2022
V9	July 2023	EEU and Australian contact details and privacy officer name updated.	Update contact EEU and Australian details and privacy officer.	Grant Piercy	20 July 2023
V10	December 2023	No material changes	Annual review	Grant Piercy	14 December 2023
V11	November 2024	No material changes	Annual Review	Grant Piercy	

Copyright

© 2024Foundation Life (NZ) Limited. All rights reserved.