22 DEGREES LIMITED PRIVACY POLICY MANUAL

CONTENTS

This manual was prepared for 22 Degrees Limited by EC Credit Control (NZ) Ltd

www.eccreditcontrol.co.nz | info@eccreditcontrol.co.nz

Phone 0800 324 768

1. INTRODUCTION

With the passing of the privacy legislation (including subsequent updates), the government introduced legislation to protect personal information about individuals. The Privacy Act 2020 ("the Act") incorporates the New Zealand's Privacy Principles (NZPP's) covered in Part 2 of the Act. These principles apply to private sector organisations who deal with information relating to individuals. This legislation is designed to protect personal information about individuals and sets in place a framework and guidelines about how to deal with this information.

As at 25 May 2018, the EU General Data Protection Regulation ("GDPR") was introduced providing increased transparency for data protection for all businesses transferring data to the Europe Union "EU". While the GDPR and the NZPP share some similarities, 22 Degrees is providing robust privacy policies and procedures for its staff and clients. This includes ensuring that it conforms to all required NZPP's including the provision of a clearly expressed and readily available Privacy Policy. This is completed by the provision of this Privacy Policy Manual.

An NZPP privacy policy is a key tool for meeting NZPP 1's requirements.

To assist with this compliance, 22 Degrees ensures that all of its staff members adhere to these policies and procedures. Any breaches of these policies and procedures must be reported to the relevant staff member's manager or supervisor immediately so that any appropriate measures can be taken to mitigate any issues surrounding an identified breach.

Every staff member of 22 Degrees who handles personal information is required to have an understanding of the New Zealand Privacy Principles (NZPP's), the Act and the GDPR, where necessary. Where a more detailed knowledge of 22 Degrees' rights and responsibilities is required, the Privacy Officer will be able to provide assistance.

All staff is encouraged to discuss privacy issues with the nominated Privacy Officer.

Review

Formal review of this privacy policy shall be undertaken on a 6 monthly basis with the details of this review recorded by the Privacy Officer.

2. NEW ZEALAND PRIVACY PRINCIPLES (NZPP'S)

The Privacy Act 2020 and the Credit Reporting Privacy Code 2020 places obligations and responsibilities on employers and employees to ensure that information collected from individuals is collected, retained and used in line with the NZPP's. 22 Degrees shall abide by the following NZPP's at all times:

1/ Purpose of collection of personal information
2/ Source of personal information
3/ Collection of personal information from subject
4/ Manner of collection of personal information
5/ Storage and security of personal information
6/ Access to personal information
7/ Correction of personal information
8/ Accuracy of personal information to be checked before use or disclosure
9/ Agency not to keep personal information for longer than necessary
10/ Limits on use of personal information
11/ Limits on disclosure of personal information
12/ Disclosure of personal information outside of New Zealand
13/ Use of unique identifiers

NZPP No.

NZPP 1 to 4	governs the reason for collection of personal information, where personal information may be collected from, and how it is collected.
NZPP 5	governs how personal information should be stored.
NZPP 6	governs that individuals have access to the personal information held about them.
NZPP 7	governs that if an individual requests changes to their personal information held about them then it should be done unless there are grounds not to do so.
NZPP 8 – 11	govern how personal information is used or disclosed.
NZPP 12	governs how personal information is used or disclosed outside of New Zealand
NZPP 13	governs that an individual's bank number, IRD number, drivers licence number, passport number etc cannot be used to identify an individual between agencies, unless authorisation is granted to 22 Degrees to enable them to complete their performance of any Services to be provided.

Further information regarding the NZPP's can be obtained from the office of the Privacy Commissioner at http://www.privacy.org.nz. A full copy of the Privacy Principles is attached as Appendix B.

In the event of any potential data breach that is likely to result in serious harm to any individuals whose personal information is involved in the breach, 22 Degrees' Privacy Policy Manual provides a data breach preparation and response to any potential breaches to ensure compliance under the Act.

3. GENERAL DATA PROTECTION REGULATION ("GDPR")

Upon the implementation of the GDPR on 25 May 2018, 22 Degrees has updated the way they use and collect personal data from residents in the EU. This involves, identifying 22 Degrees' data protection officer ("Privacy Officer"), how clients can contact the Privacy Officer and identifying the process of transferring client's personal information. Further, the implementation of cookies notices on 22 Degrees' website has been activated to ensure 22 Degrees' clients have adequate protection in providing consent to 22 Degrees in withholding their personal data.

4. TYPES OF PERSONAL INFORMATION THAT IS COLLECTED, USED, PROCESSED & HELD

22 Degrees collects personal information for a variety of reasons. This personal information will be collected in the normal course of business and will relate to Goods and/or Services that are provided by 22 Degrees to clients. This information collected will be done so in the course of business where the client is a customer of 22 Degrees or when the client acts as a guarantor for another person or company that is a client of 22 Degrees. 22 Degrees will not collect information that is not relevant or sensitive in nature unless it is required in the normal course of business.

The personal information that is collected may include, but will not be limited to the following;

1/ Full name
2/ Address
3/ Date of birth
4/ Credit references if applicable
5/ Publicly available information which relate to the clients activities in New Zealand
6/ Any information recorded in the New Zealand Insolvency Trustee Service Register
7/ Driver's license details

8/ Medical insurance details (if applicable)
9/ Electronic contact details including email, Facebook and Twitter details
10/ Next of kin and other contact information where applicable

The client acknowledges that provided the correct Privacy Act disclosures have been made that 22 Degrees may conduct a credit report on the client for the purposes of evaluating the credit worthiness of the client.

22 Degrees ensures that all personal information is held in a secure manner. Where applicable and to the best of 22 Degrees' knowledge all computers or servers have the required security protections in place to safeguard and protect any personal information that is held by 22 Degrees.

22 Degrees use cookies on their website. Cookies are small files which are stored on the individual users computer. They are designed to hold a modest amount of data (including personal information) specific to a particular client and website, and can be accessed either by the web server or the client's computer. In so far as those cookies are not strictly necessary for the provision of 22 Degrees' Services, they will ask for consent to the use of cookies upon a persons first visit their website.

In the event that someone utilises the 22 Degrees website for the purpose of purchases/orders, 22 Degrees agrees to display reference to cookies and /or similar tracking technologies, such as pixels and web beacons (if applicable), and requests consent for 22 Degrees collecting personal information which may include:

a) IP address, browser, email client type and other similar details;
b) Tracking website usage and traffic; and
c) Reports are available to 22 Degrees when 22 Degrees sends an email to the client, so 22 Degrees may collect and review that information

If an individual consents to 22 Degrees' use of cookies on their website and later wishes to withdraw their consent, they may manage and control 22 Degrees' privacy controls through their own browser, including removing cookies by deleting them from their browser history when they leave the site.

22 Degrees also regularly conducts internal risk management reviews to ensure that its infrastructure (to the best of its knowledge) is secure and any identifiable risks have been mitigated as much as they can be in the normal course of business.

5. PROCEDURES AND RESPONDING TO POTENTIAL BREACHES OF PRIVACY

In accordance with the Act. 22 Degrees is aware of its responsibilities to notify its clients in the event of a potential data breach that may cause serious harm to clients. Further, in the event the client is located in the EU, 22 Degrees acknowledges that any potential data breaches will be safeguarded by the provisions of the GDPR.

22 Degrees will collect and process personal information in the normal course of business. This personal information may be collected and processed (but is not limited to) by any of the following methods;

1/ 1/ Credit applications forms
2/ 2/ Work authorisation forms, quote forms or any other business documentation
3/ 3/ Publicly available databases that hold information
4/ 4/ Websites that detail information such as Sensis, Facebook, Google etc
5/ 5/ By verbally asking you for information as part of normal business practices

Where relevant to data processing as per the GDPR, and in particular where 22 Degrees uses new technologies, and takes into account the nature, scope, context and purposes of processing and considers that the data processing is likely to result in a high risk to the rights and freedoms of natural persons, the Privacy Officer shall, prior to the

processing of personal information, carry out an assessment of impact of the envisaged processing operations by way of a protection impact assessment. The data protection assessment will be required in instances whereby:

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) of the GDPR, or of personal data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or
c) a systematic monitoring of a publicly accessible area on a large scale.

The assessment shall be carried out in accordance with Article 35 (7) of the GDPR and carry out reviews of such data protection impact assessments when there is any change of the risk associated with the processing of personal information.

As a client of 22 Degrees and agreeing to 22 Degrees' Terms and Conditions of Trade, which includes of 22 Degrees' privacy policy you hereby agree and consent to the provisions of this Privacy Policy Manual, including but not limited to the collection, processing, use and disclosure of your personal information. In the event that you withdraw your agreement and consent to any of the above use, processing collection and disclosure, then 22 Degrees warrants that any request by you to withdraw your consent or agreement shall be deemed as confirmation by you to cease any and/or all collection use, processing and disclosure of your personal information. You may make a Request to withdraw your consent at anytime by telephone and/or by e-mail to the following contact details;

The Privacy Officer
22 Degrees
25 Crummer Road
Grey Lynn
AUCKLAND 1021
mel@22degrees.co.nz
(09) 373 2299

22 Degrees will ensure that any Information that is to be obtained from you is done so verbally or by using 22 Degrees' prescribed forms which;

Authorise 22 Degrees:

1/ To collect personal information; and
2/ Inform the individual what personal information is being collected; and
3/ Inform the individual why (the purpose) the personal information is being collected; and
4/ Inform the individual why & when personal information will be disclosed to 3rd parties.

It is the responsibility of 22 Degrees to ensure that any personal information obtained is as accurate and up to date as possible and information is only collected by lawful means in accordance with the Act and relevantly, in accordance with the GDPR.

6. PURPOSES FOR WHICH INFORMATION IS COLLECTED, HELD, USED AND DISCLOSED

Disclosure To Third Parties

22 Degrees will not pass on your personal information to third parties without first obtaining your consent.

In accordance with the Act, including the GDPR (where relevant), personal information can only be used by 22 Degrees for the following purposes:

1/ Access a credit reporter's database for the following purposes:
   a) To assess your application for a credit account; or
   b) To assess your ongoing credit facility; or
   c) To notify a credit reporter of a default by you; or
   d) To update your details listed on a credit reporter's database; or
2/ Check trade references noted on the prescribed form for the following purposes:
   a) To assess your application for a credit account; or
   b) To assess your ongoing credit facility; or
   c) To notify a default.
3/ Marketing products and Services provided by 22 Degrees; and
4/ Any other day to day business purposes such as complying with IRD requirements, managing accounting returns or legal matters.

Relationship With Credit Reporter - In the event that notification of a default has been reported to a Credit Reporter and your credit file has been updated (including any changes to the balance outstanding or contact details), then the Credit Reporter shall be notified as soon as practical of any such changes.

22 Degrees will only gather information for its particular purpose (primary purpose). In accordance with the Act, including the GDPR (where relevant) 22 Degrees will not disclose this information for any other purpose unless this has been agreed to by both parties.

7. HOW AN INDIVIDUAL MAY ACCESS PERSONAL INFORMATION HELD, AND HOW THEY MAY SEEK CORRECTION OF SUCH INFORMATION

You shall have the right to request from 22 Degrees a copy of all the information about you that is retained by 22 Degrees. You also have the right to request (by telephone and/or by e-mail) that 22 Degrees correct any information that is incorrect, outdated or inaccurate.

Any requests to receive your personal information or to correct personal information should be directed to the following contact details;

The Privacy Officer
22 Degrees
25 Crummer Road
Grey Lynn
AUCKLAND 1021
mel@22degrees.co.nz
(09) 373 2299

22 Degrees will destroy personal information upon your request (by telephone and/or by e-mail) or when the personal information is no longer required. The exception to this is if the personal information is required in order for 22 Degrees to fulfil their performance of Services or is required to be maintained and/or stored in accordance with the law.

8. HOW AN INDIVIDUAL MAY COMPLAIN ABOUT A BREACH OF THE NZPP, AND HOW THE COMPLAINT WILL BE DEALT WITH

You can make a complaint to 22 Degrees' internal dispute resolution team ('IDR') regarding an interference with and/or misuse of your personal information by contacting 22 Degrees via telephone or e-mail.

Any complaints should be directed to the following contact details in the first instance;

The Privacy Officer
22 Degrees
25 Crummer Road
Grey Lynn
AUCKLAND 1021
mel@22degrees.co.nz
(09) 373 2299

In your communication you should detail to 22 Degrees the nature of your complaint and how you would like 22 Degrees to rectify your complaint.

We will respond to that complaint within 7 days of receipt and will take all reasonable steps to make a decision as to the complaint within 30 days of receipt of the complaint.

We will disclose information in relation to the complaint to any relevant credit provider and or Credit Reporting Body that holds the personal information the subject of the complaint.

In the event that you are not satisfied with the resolution provided, then you can make a complaint to the Privacy Commissioner at http://www.privacy.org.nz.

9. WILL PERSONAL INFORMATION BE DISCLOSED TO OVERSEAS RECIPIENTS

22 Degrees does not disclose information about the client to third party overseas recipients unless the client has provided its consent. 22 Degrees will notify you if circumstances change regarding overseas disclosure and will comply with the Act and the GDPR in all respects.

Unless otherwise agreed, 22 Degrees agrees not to disclose any personal information about the client for the purpose of direct marketing. You have the right to request (by telephone and/or by e-mail) that 22 Degrees does not disclose any personal information about you for the purpose of direct marketing.

10. AVAILABILITY OF THIS PRIVACY POLICY MANUAL

This Privacy Policy manual is available to all clients of 22 Degrees. It will be made available (where applicable) on 22 Degrees' website.

This manual will also be available upon request at 22 Degrees' business premises and is available to be sent to you if required.

If you require a copy of this Privacy Policy please make a request utilising the following contact information in the first instance:

The Privacy Officer
22 Degrees
25 Crummer Road
Grey Lynn
AUCKLAND 1021
mel@22degrees.co.nz
(09) 373 2299

11. PRIVACY OFFICER (RESPONSIBILITIES)

22 Degrees has appointed an internal Privacy Officer to manage its privacy matters. The name of this officer is available by making contact with 22 Degrees. The privacy officers duties include (but are not limited to) the following:

The Privacy Officer needs to be familiar with the NZPP's. Educational material is available from the office of the Privacy Commissioner which explains what 22 Degrees needs to know in order to comply with the Privacy Act.

If a person complains to the Privacy Commissioner that 22 Degrees has breached their privacy, the Privacy Commissioner may contact the Privacy Officer to discuss the complaint, and to see whether there is any means of settling the matter. The Privacy Officer shall provide whatever assistance is necessary. The Privacy Officer may be asked to provide background information or identify the staff members who can do so.

Complaints

In the event that a complaint about privacy issues is received the Privacy Officer will:

1/ Take ownership of the complaint and ensure that it is dealt with in a timely manner.
2/ Acknowledge receipt of the complaint within 24 hours and advise the complainant of their rights.
3/ Fully investigate the complaint.
4/ Respond, with findings, to the complainant within 20 days of receipt.
5/ Keep a record of all complaints received for ongoing review of policies and procedures.

In the event that a complaint about privacy issues is received via a credit reporter the Privacy Officer will:

1/ Take ownership of the complaint and ensure that it is dealt with in a timely manner.
2/ Acknowledge receipt of the complaint to the credit reporter within 24 hours (see attached Appendix A).
3/ Fully investigate the complaint.
4/ Respond, with findings, to the credit reporter within 7 days of receipt.
5/ Keep a record of all complaints received for ongoing review of policies and procedures.

Other

The Privacy Officer shall ensure that 22 Degrees' documentation complies with the Privacy Act and Credit Reporting Privacy Code at all times.

APPENDIX A - SUMMARY OF RIGHTS

(Rules 6 and 7 and clause 8)

A Summary Of Your Rights Under The Credit Reporting Privacy Code 2004

The Credit Reporting Privacy Code 2004 is issued under the Privacy Act 2020. It promotes fairness, accuracy, and privacy in the practice of credit reporting. Credit reporters gather and sell information about you such as a failure to pay your bills or if you have been made bankrupt.

You can find the complete text of the **Code** at:

https://www.privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/credit-reporting-privacy-code/#:~:text=Credit%20Reporting%20Privacy%20Code%202004.%20This%20code%20applies,takes%20the%20place%20of%20the%20information%20privacy%20principles.

Privacy Act at:

http://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html

The Code, together with the Act, gives you specific rights, many of which are summarised below.

Limited information can be reported about you.

A credit reporter can only collect certain classes of information, set out in the Code, for its credit reporting database. A credit reporter will generally report information for no longer than 5 – 7 years: the actual retention periods are required to be displayed on each credit reporter's website.

Only certain people can access your file for certain purposes.

The Code limits the people who can gain access to your credit information. These will usually be credit providers who are considering your application for credit, but in some strictly defined situations the information may be available to prospective landlords, employers or insurers, to debt collectors, to those involved in court proceedings and to certain public sector agencies.

Your consent is required in most situations.

Most credit checks can only take place with your authorisation. This applies to access by credit providers, prospective landlords and prospective employers. Your authorisation may not be required for access by certain public sector agencies, those involved in court proceedings and debt collectors. The credit reporter is required to log each access that is made to your information and will normally disclose this information to you on request.

You can find out what is held about you.

You are entitled to request a copy of the credit information held about you by a credit reporter. You can ask for just the information contained in your credit report or for all the information held about you (which may include additional information, such as a more complete list of those who have accessed your report). If you want the information quickly (within 5 working days) you may be required to pay a reasonable charge, but otherwise no charge may be made. A credit reporter must take precautions to check the identity of anyone making a personal access request. This may involve asking you for certain identification details, although these cannot be added to the credit reporter's database without your authorisation.

You can dispute inaccurate information with the credit reporter.

Credit reporters must take reasonable steps to ensure the accuracy of the information they hold and must act promptly to correct any errors they become aware of. If you tell a credit reporter that your report contains an inaccuracy, the credit reporter must take steps to correct it. This will usually involve checking the information you provide with the source, such as a creditor who submitted a default. While the checking process is under way, the credit reporter must flag your credit report to show that the item has been disputed. The credit reporter must, as

soon as reasonably practicable, decide whether to make the correction you have requested or to confirm the accuracy of the information. If the credit reporter needs longer than 20 working

days to make a decision it must notify you of the extension and the reasons for it. If the requested correction is not made you must be told the reason and you may ask to have a statement of the correction sought but not made, attached to the relevant information. This statement will be included with future reports. If a correction is made or a correction statement is added, the credit reporter must inform anyone who has recently received your credit report of the change. They must tell you what they have done and provide you with a copy of the amended report. A credit report describes your credit history, not simply your current debts. Information about a bankruptcy that has been discharged or a default that has subsequently been paid in full can continue to be reported, provided it is updated to reflect the later developments, as it remains an accurate statement of those historical events.

You have the right to make a complaint.

Each credit reporter must maintain an internal complaints procedure and have a designated person to facilitate the fair, simple, speedy and efficient resolution of complaints. If you believe a credit reporter has breached the Code you should first approach them directly. If your complaint is not resolved you may complain to the Privacy Commissioner who has statutory powers to investigate the matter. Some cases that cannot be settled can be taken to the Human Rights Review Tribunal for final determination. Other civil law remedies may also be available including defamation and negligence.

Contact addresses.

22 Degrees
25 Crummer Road
Grey Lynn
AUCKLAND 1021
Phone (09) 373 2299

Office of the Privacy Commissioner
PO Box 10094, The Terrace
WELLINGTON 6143
Fax (04) 474 7595

Warning: This is only a generalised summary. In the event of a discrepancy between this summary and a provision of the code or Act, the code or Act prevails.

APPENDIX B - INFORMATION PRIVACY PRINCIPLES

NOTE

In some cases agencies are authorised or required by other legislation to collect, use, retain, or make available, personal information, and in most cases where an agency collects, uses, retains or makes available personal information in accordance with such legislation this will not amount to a breach of the Privacy Act. (IPP's10 & 11 of the Privacy Act 2020).

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 individuals' identifying information, the agency may not require the individual's identifying information.

PRINCIPLE 2

Source of personal information

1/ If an agency collects personal information, the information must be collected from the individual concerned.

2/ 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
   f. that compliance is not reasonably practicable in the circumstances of the particular case; or
   g. 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.

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.

PRINCIPLE 4

Manner of collection of personal information

a. An agency may collect personal information only—
(a) by a lawful means; and
b. (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.

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.

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.

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.

PRINCIPLE 8

Accuracy, etc., of personal information to be checked before use

An agency that holds 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.

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.

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.

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.

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,—

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

5/ 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.