

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Information Privacy Individual Action Plan**

New Zealand (2008, updated in 2011 and 2021)

|  | **APEC Principle/ Commentary** | **Privacy Protection Scheme (legislation, rules, codes, frameworks, and other) [[1]](#footnote-1)** | **Provision[[2]](#footnote-2)** | **Sanction[[3]](#footnote-3)** | **Results/ Status[[4]](#footnote-4)** |
| --- | --- | --- | --- | --- | --- |
| A | Is privacy a constitutionally protected right in your economy? | No | N/A | N/A | N/A |
| B | If not, what other available legislation deals with privacy or confidentiality of personal information. | New Zealand has a comprehensive privacy law framework provided by the [Privacy Act 2020](https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html?src=qs) (“the Act”). The Act replaces the old Privacy Act 1993 and provides increased protection for personal privacy. | Privacy Act 2020.  **Information Privacy Principles**  The Act sets out strict safeguards for the handling of personal information by both public and private sector entities (generally “agencies”). The Act governs how agencies should collect, secure, use and disclose, and provide for access to and correction of personal information. The Act sets out obligations with broadly applicable Information Privacy Principles (“[IPPs](https://www.legislation.govt.nz/act/public/1993/0028/latest/DLM297038.html)”).  **Extraterritoriality**  The new Act now clearly states that it has extraterritorial effect. This means that an overseas business or organisation that is ‘carrying on business’ in New Zealand will be subject to the Act’s privacy obligations, even if it does not have a physical presence here. This will affect businesses located offshore, such as Google and Facebook.  **Codes of practice**  The Commissioner has the power to issue legally enforceable codes of practice under the Act. The codes govern the treatment of personal information as it pertains to areas such as health, civil defence emergencies, credit reporting sectors and telecommunications.  **Prohibiting onward transfer**  Part 8 of the Privacy Act relates to the transfer of personal information outside New Zealand. In particular, it authorises the Commissioner to issue a notice prohibiting the transfer of personal information to another economy where the Commissioner is satisfied that the information has been received from another economy and is likely to be transferred from New Zealand to a third economy where it will not be subject to comparable privacy safeguards.  **Information sharing and information matching**  The Commissioner also has oversight functions relating to government data matching programmes and sharing agreements.  The Act also regulates access to law enforcement information by various public sector agencies.  The Actgives effect to New Zealand’s agreement to implement Guidelines adopted in 1980 by the OECD for the [Protection of Privacy and Transborder Flows of Personal Data](http://www.privacy.gov.au/publications/oecdgls.pdf) | An independent Privacy Commissioner (“the Commissioner”) oversees the Act’s application. The Office of the Privacy Commissioner assists businesses and agencies to comply with the Act; assists individuals in regard to their rights under the Act; and promotes best practice in privacy standards.  If an individual believes an agency has not properly dealt with their personal information, the individual has a right to make a complaint.  The Commissioner deals with complaints at first instance through investigation, then promoting settlements, issuing binding decisions on access requests, and issuing non-binding opinions.  If a complaint has not been settled, the Commissioner may refer it to the Director of Human Rights Proceedings, who may decide to institute proceedings in the Human Rights Review Tribunal. Alternatively, the aggrieved individual may bring such proceedings. Remedies include declaratory relief; orders in the nature of an injunction; compensatory (including general) damages; an order that the defendant take action to remedy the breach; and such other relief as the Tribunal thinks fit. The Tribunal can award costs.  There is a right of appeal from the Tribunal to the High Court, Court of Appeal, and Supreme Court.  **Access Direction**  The Commissioner can direct a business or organisation to provide an individual access to the individual’s personal information in any manner that the Commissioner considers appropriate. Access directions will be enforceable in the Human Rights Review Tribunal.  **Own Motion Inquiry**  The Commissioner also has the power to investigate, on the Commissioner’s own initiative, an action that may be an interference with the privacy of an individual, even if no complaint has been made.  **Notifiable privacy breaches**  If a business or organisation has a privacy breach that it believes has caused (or is likely to cause) serious harm, it will need to notify the Office of the Privacy Commissioner and affected individuals as soon as practicable. Under the Act, it is an offence to fail to inform the Commissioner when there has been a notifiable privacy breach. Failure to do so may result in a fine of up to $10,000.  Agencies can notify a privacy breach to the Commissioner through the OPC’s [NotifyUs tool](https://privacy.org.nz/responsibilities/privacy-breaches/notify-us/).  **Compliance notices**  The Commissioner can issue compliance notices to agencies requiring them to do something, or stop doing something, to comply with the Privacy Act. Compliance notices describe the steps that the Commissioner considers are required to remedy non-compliance with the Act and will specify a date by which the organisation or business must make the necessary changes.  **Criminal offences**  The Act now has criminal offences. It is now an offence to mislead an agency to access someone else’s personal information – for instance, impersonating someone in order to access information that you are not entitled to see. The penalty for this offence is a fine of up to $10,000. It is also an offence for an organisation or business to destroy personal information, knowing that a request has been made to access it. The penalty for this offence is a fine of up to $10,000. | The Act was enacted in December 2020. |
| 1 | ***I Preventing Harm***  **(Ref. Para. 20)**  Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information. | [Privacy Act 2020](https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html?search=ts_act%40bill%40regulation%40deemedreg_Privacy+Act+2020_resel_25_a&p=1) | Section 22 of the Actcontains 13 IPPs governing the collection, security, quality, use, and disclosure of personal information. They also provide individuals with rights to access and correct personal information.  Obligations under the IPPs take account of relevant risks and are proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information:   * IPP1 – states that an agency must collect information only for a lawful purpose connected to a function or activity of the agency. If the lawful purpose does not require the collection of personal information then the agency may not require to collect personal information. * IPP5 states that organisations must ensure there are safeguards in place that are reasonable in the circumstances to prevent loss, misuse or disclosure of personal information. * IPP7 states that a person has a right to ask an organisation or business to correct information about them if they think it is wrong. If an organisation does not agree that the information needs correcting, an individual can ask that an agency attach a statement of correction to its records, and, if reasonable, the agency should do so. * IPP8 states that an organisation must check before using or disclosing personal information that it is accurate, up to date, complete, relevant and not misleading.   IPPs 7 and 8 mitigate the harm which could flow from usage and transfer of inaccurate or incorrect personal information.  Section 66 provides that an action constitutes an interference with an individual’s privacy only if it breaches an IPP or code of practice made under the Privacy Act, and it has caused or may cause some harm or loss, or it has resulted in or may result in, significant humiliation, loss of dignity or injury to feelings for the individual.  As per section 212, it is a criminal offence punishable by a fine of up to $10,000 to impersonate another individual to obtain their personal information or to have that individual’s personal information used, altered or destroyed. It is an offence for an organisation or business to destroy personal information, knowing that a request has been made to access it. | The Privacy Act provides for mechanisms for dealing with complaints by individuals about misuse of their personal information and other interferences with their privacy. | Enacted. |
| 2 | ***II Notice***  **(Ref. Para. 21-23)**  Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should  include:  a) the fact that personal information is being collected;  b) the purposes for which personal information is collected;  c) the types of persons or organizations to whom personal information might be disclosed;  d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information;  e) the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information.  All reasonably practicable steps shall be taken to ensure that such notice is provided either before or at the time of collection of personal information. Otherwise, such notice should be provided as soon after as is practicable.  It may not be appropriate for personal information controllers to provide notice regarding the collection and use of publicly available information. | [Privacy Act 2020](https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html?search=ts_act%40bill%40regulation%40deemedreg_Privacy+Act+2020_resel_25_a&p=1) | IPP2(1) provides that when an agency collects personal information, it should collect it directly from the individual concerned unless one of the specified exceptions applies.  IPP3(1) provides that when an agency collects personal information directly from an individual, the agency should take reasonable steps to ensure that the individual is aware of:   * the fact the information is being collected; * the purpose for which the information is being collected; * the intended recipients of the information; * the name and address of the agency collecting the information, and the agency that will hold it; * if the collection is authorised or required by law, the particular law concerned, and whether or not the supply of the information by the individual is voluntary or mandatory; * the consequences, if any, for the individual if the information is not provided; and * the rights of access to and correction of personal information under the Privacy Act.   IPP3(2) provides that the above information should be communicated before the information is collected, or, if that is not practicable, as soon as practicable after the information is collected.  IPP 3(3) provides that the requirements of IPP 3(1) and (2) are not necessary if the agency has taken those steps in relation to the collection, from the same individual, of the same information or same kind of information, on a recent previous occasion.  IPP3(4) provides for specific exceptions to IPP3(1).  IPP6(1) provides that an individual is entitled to receive from an agency upon request –   * confirmation of whether the agency holds any personal information about them; and * access to their personal information.   IPP6(2) provides that when individuals are given access to their personal information, they must be advised that there is a right to request correction of that information under IPP7.  Under IPP2(2) an agency does not have to collect personal information directly from an individual if it believes on reasonable grounds that the information is publicly available. If agencies are legitimately collecting from a source that is not the individual concerned, they are not required to provide the comprehensive notice required by IPP3. | Idem. | Idem.  Agencies commonly provide notice and information about  their privacy policies on their websites, other publications, and wherever they collect personal information.  OPC consults with agencies to review their privacy statements, ensuring they are fit for purpose and comply with the Act. |
| 3 | ***III Collection Limitation***  **(Ref. Para. 24)**  The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned. | [Privacy Act 2020](https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html?search=ts_act%40bill%40regulation%40deemedreg_Privacy+Act+2020_resel_25_a&p=1) | IPP1(1) provides that an agency must not collect personal information unless the information is collected for a lawful purpose connected with a function or activity of the agency, and the collection is necessary for that purpose. Under IPP1(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.  IPP2(1) provides that if an agency collects personal information, the information must be collected from the individual concerned. IPP2(2) sets out exceptions to IPP2(1) (for example, where the information is publicly available).  As per 2 above, under IPP3, agencies must take reasonable steps to ensure the individual is aware that their personal information is being collected; the purpose(s) of the collection; the intended recipients; the name and address of the agency that is collecting it and that will hold it; whether the collection of information is authorised or required under law; whether the supply of the information is voluntary or mandatory; and the consequences for the individual of not providing the information.  IPP4 provides that an agency may collect information only by lawful means and by means that, in the circumstances of the case (particularly in circumstances where personal information is being collected from children or young persons), is fair and does not unreasonably intrude upon the personal affairs of the individual.  Under IPP9, 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. | Idem. | Idem. |
| 4 | ***IV Use of Personal Information***  **(Ref. Para. 25)**  Personal information collected should be used only to fulfill the purposes of  collection and other compatible or related purposes except:  a) with the consent of the individual whose personal information is collected;  b) when necessary to provide a service or product requested by the individual; or,  c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect. | [Privacy Act 2020](https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html?search=ts_act%40bill%40regulation%40deemedreg_Privacy+Act+2020_resel_25_a&p=1) | IPP10 provides that an agency that holds personal information that was obtained in connection with one purpose must not use it for any other purpose unless the agency reasonably believes 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; * the information is to be used in a form in which the individual concerned is not identified or is to be used for statistical or research purposes; * the information is publicly available; * the individual authorised the use for the other purpose; * non-compliance is necessary for law enforcement; or * use of the information is necessary to prevent or lessen a serious threat to public health or safety, or an individual’s life or health.   Furthermore, an intelligence and security agency holding personal information obtained in connection with one purpose may use the information for any other purpose if the agency reasonably believes that the use of the information for the secondary purpose is necessary to enable the agency to perform any of its functions.  IPP11 provides that an agency that holds personal information may not disclose it unless the agency reasonably believes that:   * the disclosure is to the individual concerned; or * the disclosure is necessary to facilitate the sale or other disposition of a business as a going concern.   IPP11 otherwise essentially duplicates the exceptions that apply to IPP10.  IPP11 is subject to the new IPP12 which governs the disclosure of personal information outside New Zealand. Under IPP12, an agency may only disclose personal information to another organisation outside New Zealand if the receiving organisation:   * is subject to the Privacy Act because they do business in New Zealand; * is subject to privacy laws that provide comparable safeguards to the Privacy Act; * agrees to adequately protect the information, e.g. by using model contract clauses; or * is covered by a binding scheme or is subject to the privacy laws of a jurisdiction prescribed by the New Zealand Government.   If none of the above criteria apply, a business or organisation may only make a cross-border disclosure with the permission of the person concerned. The person must be expressly informed that their information may not be given the same protection as provided by the New Zealand Privacy Act. | Idem. | Idem. |
| 5 | ***V Choice***  **(Ref. Para. 26)**  Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be  appropriate for personal information controllers to provide these mechanisms when collecting publicly available information. | [Privacy Act 2020](https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html?search=ts_act%40bill%40regulation%40deemedreg_Privacy+Act+2020_resel_25_a&p=1) | Choice is exercised at the time of the collection of personal information. As per 2 and 3 above, personal information should be collected directly from individuals unless a specified exception applies (IPP2), and individuals should be given notice about a number of matters (IPP3), including the fact that personal information is being collected; for what purpose; by and for whom; and under what conditions.  When individuals exercise the right under IPP6 to access their own personal information, they must be advised that they have the right to request correction of the information under IPP7. Where an agency denies access to personal information section 46 provides that an agency may only refuse an access request if it can rely on the exceptions in sections 49-53. When agencies notify a requestor of a refusal, they must provide their reason for refusal and state the requestor’s right to make a complaint to the Commissioner.  When individuals exercise their right under IPP6 to access their own personal information, section 56(1) provides for a number of ways in which that information may be made available, and s 56(2) provides that the agency must make the information available in the way preferred by the individual unless to do so would impair efficient administration; be contrary to a legal duty of the agency; or prejudice an interest protected under the Privacy Act.  Publicly available information is exempt from the IPPs relating to collection, use, and disclosure. Such information is defined as personal information contained in a publicly available publication, which means a magazine, book, newspaper, or other publication that is or will be generally available to members of the public, and it includes a public register. | Idem. | Idem.  In practice, many agencies provide individuals with choice as to how they wish to provide personal information. |
| 6 | ***VI Integrity of Personal Information***  **(Ref. Para. 27)**  Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use. | [Privacy Act 2020](https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html?search=ts_act%40bill%40regulation%40deemedreg_Privacy+Act+2020_resel_25_a&p=1) | Under IPP5, an agency holding personal information must ensure that the information is protected by such security safeguards as are reasonable in the circumstances against loss; unauthorised access, use, modification, or disclosure; and other misuse. If it is necessary for the information to be given to another person in connection with the provision of a service to the agency, the agency must do everything it reasonably can to prevent unauthorised use or disclosure of the information.  IPP6(2) provides that where an individual is given access to personal information, he or she must be advised that there is a right to request correction of that information under IPP7.  IPP7(1) provides that an individual whose personal information is held by an agency is entitled to request the agency to correct the information.  IPP7(2) provides that 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 the information is accurate, up to date, complete, and not misleading.  IPP7(3) provides that when requesting the correction of personal information, or at any later time, and individual is entitled to –   * provide the agency with a statement of the correction sought to the information (a “statement of correction”); and * request the agency attach the statement of correction to the information if the agency does not make the correction sought.   Under IPP7(4) if any agency that holds personal information is not willing to correct the information as requested and has been given a statement of correction, the agency must take reasonable steps in the circumstances to ensure that the statement of correction is attached to the information in a manner that ensures it will always be read with the information.  Under IPP7(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.  IPP8 prohibits agencies that hold personal information from using it without taking reasonable steps in the circumstances to ensure that, having regard to the purpose for which the information is to be used, the information is accurate, up to date, complete, relevant, and not misleading. | Idem. | Idem. |
| 7 | ***VII Security Safeguards***  **(Ref. Para. 28)**  Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment. | [Privacy Act 2020](https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html?search=ts_act%40bill%40regulation%40deemedreg_Privacy+Act+2020_resel_25_a&p=1) | Under IPP5, agencies holding personal information must ensure that the information is protected by such security safeguards as are reasonable in the circumstances against loss; unauthorised access, use, modification, or disclosure; and other misuse. Furthermore, if it is necessary for the information to be given to a person providing a service to the agency, the agency must ensure that everything is reasonably done to prevent unauthorised use or disclosure of the information.  IPP9 provides that 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. | Idem. | Idem. |
| 8 | ***VIII Access and Correction***  **(Ref. Para. 29-31)**  Individuals should be able to:  a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them;  b) have communicated to them, after having provided sufficient proof of their identity, personal information about them;  i. within a reasonable time;  ii. at a charge, if any, that is not excessive;  iii. in a reasonable manner;  iv. in a form that is generally understandable; and,  c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.  Such access and opportunity for correction should be provided except where:  (i) the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual’s privacy in the case in question;  (ii) the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or  (iii) the information privacy of persons other than the individual would be violated.  If a request under (a) or (b) or a challenge under (c) is denied, the individual should be provided with reasons why and be able to challenge such denial. | [Privacy Act 2020](https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html?search=ts_act%40bill%40regulation%40deemedreg_Privacy+Act+2020_resel_25_a&p=1) | **Access**  IPP6 provides that where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned is entitled to obtain from the agency confirmation of whether or not it holds such information, and to have access to it.  Part 4 subpart 1 of the Act contains the procedural provisions relating to access to personal information.   * Agencies must give reasonable assistance to individuals wishing to make or are making requests for access or correction (section 42). * Where a request for access is made to an agency, and the relevant information is not held by it but by another agency, the agency to which the request was made must promptly, and in any case not later than 10 working days, transfer the request to the other agency and inform the individual accordingly (section 43). * Under section 44, an agency must respond to an access request as soon as practicable and in any case not later than 20 working days after the request is received. The response must notify the requestor that either the information is not readily retrievable, the agency does not hold any information about the person; or it does hold information and that the request is either granted or refused. * Under section 45, if an agency grants access to personal information, the notice under section 44 must state the way the information is going to be given, the charge payable (if any), and the requestor’s right to complain about the charge. * Section 46 provides that an agency can only refuse access by relying on the withholding grounds in sections 49-53. If an agency refuses access, they must state the reason and that the requestor can complain to the Commissioner about the refusal. * Section 47 provides that an agency can refuse to confirm or deny that it holds information on the requestor for several reasons. For instance, disclosure would likely pose a serious threat to the life, health or safety of any individual, or to public health or safety. * Section 48 provides that an agency may extend the time limits in section 43 and 44 under limited circumstances. For instance, if 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.   The grounds for withholding access are under sections 49-53.  Section 49 sets out situations in which an agency may refuse access to personal information. For instance, if disclosing it would likely pose a serious threat to the life, health, or safety of any individual, or to public health or safety; or would create a significant likelihood of serious harassment of an individual.  Section 50 provides that an agency can withhold personal information from a requester if the information is evaluative material.  "Evaluative material" is evaluative or opinion material compiled solely for one of the below purposes:   * Determining a person's suitability, eligibility, or qualifications to be: * employed or appointed to a position; * promoted or continued in their position; * removed from employment or from their position; or * given a contract, award, scholarship, honour, or other benefit. * Determining whether any contract, award, scholarship, honour or benefit should be continued, modified, or cancelled * Deciding whether to insure a person, or property, or to continue or renew the insurance of the person or property.   Section 51 provides that an agency can withhold personal information if disclosing the information to a requestor could   * prejudice New Zealand's security, defence or international relations; or * prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by another Government or international organisation   Section 52 provides that an agency may refuse access if making the information available would disclose a trade secret or would likely prejudice the commercial position of the person who supplied the information or who is the subject of the information.  Section 53 covers a variety of other withholding grounds. For instance, access may be withheld if:   * disclosure would prejudice the maintenance of the law; or * the request if frivolous or vexatious or the information requested is trivial.   If any agency has good reason under any of the sections 49 -53 to refuse access, the agency may instead grant conditional access.  **Correction**  IPP 7 provides that where an agency holds personal information, individuals are entitled to request correction of the information and, if the agency refuses to correct it, to request that there be attached to the information a statement of the correction sought but not made.  Part 4 subpart 2 of the Act contains the procedural provisions relating correction of personal information.  Under section 60 a requestor may ask that a correction by treated as urgent and state the reasons why. An agency must consider the request for urgency when determining priority to be given to it.  Under section 61 an agency must give reasonable assistance to a person wishing to make a correction request or is making a correction request.  Under section 62, if an agency:   * does not hold the information to which the request relates but believes that information is held by another agency; or * believes that the information to which the request relates is more closely connected with the functions or activities of another agency;   the agency must promptly and in any case not later than 10 working days after the correction request is received transfer the request to the other agency and inform the requestor accordingly.  Section 63(1) provides that as soon as is reasonably practicable and in any case not later than 20 working days after receiving a correction request, an agency must decide whether to grant the request; and notify the requestor that the agency has corrected or will correct the personal information or the agency will not correct the personal information. This notice the must inform them of the action the agency has or taken or will take to correct the information (if any). If the agency refuses a request, the notice must inform the requestor of:   * the reason for the agency’s refusal to correct the information; * the requestor’s entitlement to provide a statement of the correction sought and to request that it be attached to the information; and * the requestor’s right to make a complaint to the Commissioner in respect of the agency’s refusal to correct the information.   Section 64 provides that as soon as reasonably practicable after receiving a request to attach a statement of correction, an agency must decide whether to grant the request and notify the requestor that the agency has either attached the statement of correction to the information or has not. Likewise, this notification must inform the requestor of the action the agency has taken or the requestor’s right to complain to the Commissioner in respect of a refusal.  Under section 65, an agency may extend the time limits in respect of correction requests or decisions on requests to correct personal information if, for instance -   * The request requires a search through a large quantity of information and meeting the original time limit would be unreasonable; or * the processing of the request raises issues of such complexity that a response cannot reasonably be given within the original time limit.   The notice effecting the extension must specify the period; the reasons; state the requestor has the right to make a complaint to the Commissioner about the extension; and contain any other information that may be necessary.  Other matters:   * Personal information held by the public sector is prima facie free of charge (s 66(1)). There is provision for the Commissioner to authorise a public sector agency to impose a charge for access or a correction request if satisfied that it would be commercially disadvantaged (s 67). Private sector agencies may impose a reasonable charge for making information available, correcting information or providing assistance in relation to the same (s 66). * Where personal information is comprised in a document, it may be made available in several different ways (s 56). Agencies must make the information available in the way preferred by the individual requesting it unless to do so would impair efficient administration; be contrary to a legal duty of the agency; or prejudice an interest protected under the Privacy Act. | Idem. | Idem. |
| 9 | ***IX Accountability***  **(Ref. Para. 32)**  A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles. | [Privacy Act 2020](https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html?search=ts_act%40bill%40regulation%40deemedreg_Privacy+Act+2020_resel_25_a&p=1) | As described at B above (Sanctions), agencies are accountable for breaches of the IPPs. The Commissioner investigates at first instance, and if a complaint cannot be settled, remedies are available for proved breaches in the Human Rights Review Tribunal. Furthermore, the Commissioner can issue enforceable compliance notices and access directions. There are also the aforementioned offences.  Moreover, section 96 of the Act provides that if, during or after any investigation, the Commissioner is of the opinion there is evidence of any significant breach of duty or misconduct on the part of any agency or any officer or employee or member of an agency, the Commissioner must refer the matter to the appropriate authority.  IPP11 (as per 4 above) places limits on the disclosure of personal information about an individual to others.  Under section 10, personal information held by a person in the person’s capacity as an officer, employee, or member of an agency is to be treated as being held by the agency. This does not apply to personal information if –   * the information is held only because of the person’s connection with a private sector agency; and * that connection is not in the person’s capacity as an officer, an employee, or a member of the agency.   Section 11 of the Act provides that where an agency holds information as an agent for another agency (e.g. for safe custody or processing), and does not use or disclose the information for its own purposes, the information is deemed to be held by the agency on whose behalf that information is so held or processed. It does not matter whether this agent is outside New Zealand or holds the information outside New Zealand. If the agent uses or discloses the information for its own purposes, both the agent and principal agency are deemed to hold the information.  Section 23 governs the application of the IPPs in relation to information held overseas. It provides that an action taken by an agency in relation to information held overseas does not breach any of the IPPs if the action is required by or under the law of any jurisdiction other than New Zealand.  IPP 12 sets rules around sending personal information to organisations or people outside New Zealand (cross-border disclosure). A business or organisation may only disclose personal information to another organisation outside New Zealand if the receiving organisation:   * is subject to the Privacy Act because they do business in New Zealand * is subject to privacy laws that provide comparable safeguards to the Privacy Act * agrees to adequately protect the information, e.g. by using model contract clauses. * is covered by a binding scheme or is subject to the privacy laws of a jurisdiction prescribed by the New Zealand Government.   If none of the above criteria apply, a business or organisation may only make a cross-border disclosure with the permission of the person concerned. The person must be expressly informed that their information may not be given the same protection as provided by the New Zealand Privacy Act.  The Privacy Act includes provisions relevant to accountability for cross-border transfers of personal information. The provisions empower the Commissioner to issue a transfer prohibition notice to stop a transfer where information has been received in New Zealand from another economy and is proposed to be transferred to an economy having no law providing protections comparable to the Privacy Act and there is likely to be a contravention of basic principles of privacy protection. | Idem.  2011 update: Transfer prohibition notices are legally binding on the agency named in the notice once they take effect (which may be delayed if an appeal is lodged). Breach of a notice is a criminal offence carrying a maximum NZ$10,000 fine. | Idem. |
| C | Network point of contact arrangements |  | **John Edwards**  Privacy Commissioner  **Liz MacPherson**  Assistant Commissioner – Policy and Operations  **Jo Hughes**  Assistant Commissioner – Strategy and Insights  **Joanna Hayward**  General Counsel  **Office of the Privacy Commissioner (Wellington Office)**  PO Box 10094, The Terrace, Wellington 6143  11/215 Lambton Quay, Wellington Central, Wellington 6011  New Zealand  +64 4 494 7086  [International@privacy.org.nz](mailto:International@privacy.org.nz)  **Office of the Privacy Commissioner (Auckland Office)**  Auckland Office  PO Box 466  Auckland 1140  Level 13, 51 Shortland Street  Auckland 1010  New Zealand  +64 9 302 8658  [International@privacy.org.nz](mailto:International@privacy.org.nz) |  |  |

-- // --

*Please provide contact details such as name and/or title, address, telephone and email contacts. This information will not be published but will be made available to economies.*

1. *Note here the legislation, rule, code, framework or other privacy protection scheme. Where possible please provide the URL for the website where the legislation or arrangement is available.* [↑](#footnote-ref-1)
2. *Insert the full text or summary of the provisions of your privacy protection scheme(s) that correspond to the APEC Privacy Principles identified in the column titled “APEC Principle/ Commentary”.* [↑](#footnote-ref-2)
3. *Sanctions should include the nature of the remedies available, the means by which they are obtained, and by whom (for example, government, local law enforcement, private right of action, etc.).*  [↑](#footnote-ref-3)
4. *Identify areas where the practice and the intent of the principle need further consideration; and identify the status of the economies’ practice, for example enacted, introduced, draft.  If your legislation, rule, code, framework or other privacy protection scheme is at the drafting or proposal stage and has not yet been enacted or implemented, please indicate here and provide any other useful comments."* [↑](#footnote-ref-4)