Privacy Commissioner
Te Mana Mātāpono Matatapu

PRIVACY BREACH GUIDELINES

How to Prevent and Respond to Privacy Breaches

CONTENTS

INTRODUCTION

Privacy is precious. Every day, organisations and businesses are entrusted with personal information and have obligations under the Privacy Act to protect it and respect it.

Sometimes, organisations entrusted with personal information experience privacy breaches and personal information is used or shared in ways that cause the owner of the information harm. Privacy breaches can be caused through accidents, carelessness, system hacks or.

Privacy breaches can impact businesses or organisations of all sizes. They may affect the personal information of a single person or, in extraordinary cases, hundreds of thousands of people.

What is personal information?

Personal information is any piece of data about an identifiable individual. The information does not necessarily need to name someone if they are identifiable in other ways, such as through their home address.

Personal information may include:

- People's names
- Contact details
- Financial records
- Health records
- Purchase history
- Date of birth
- Log in details.

What is a privacy breach?

A privacy breach occurs when an organisation or individual who holds personal information either intentionally or accidentally:

- Provides unauthorised or accidental access to personal information.
- Discloses, alters, loses, or destroys personal information.
- Prevents someone from accessing their personal information, for example, where it is encrypted by ransomware.

What is a “notifiable privacy breach"?

Under the Privacy Act 2020, a notifiable privacy breach is one in which an organisation has reasonably judged that a breach it has experienced either has caused or is likely to cause someone serious harm.

If the breach is notifiable, organisations must inform the Office of the Privacy Commissioner and, unless an exception applies, the affected people. Our expectation is that we will be notified within 72 hours.

Not all privacy breaches need to be reported. Each breach should be considered on its own merits. Our online tool NotifyUs helps you assess whether your breach is notifiable and guides you through the reporting process.

> *Even if your breach doesn't reach the notifiable threshold, you can still learn from it to avoid it happening again.*

How do privacy breaches happen?

Common privacy breaches include:

- Personal information being sent to the wrong postal address, email address or mobile phone number.
- Employees accessing or sharing personal information without authorisation (known as employee browsing).
- Computers, removable storage devices, or documents containing personal information being lost or stolen.
- Hardware being thrown away, recycled, or returned to leasing companies without personal information being deleted first.
- Personal information being illegally accessed or hacked.
- Organisations losing the ability to access personal information on its systems.

What is serious harm?

The unwanted sharing, exposure, or loss of access to people's personal information may cause individuals or groups serious harm. Some types of information are inherently more sensitive than others and therefore more likely to cause people serious harm [see What is Sensitive Information? below].

Examples of serious harm include:

- Physical harm or intimidation
- Financial fraud, including unauthorised credit card transactions or credit fraud
- Family violence
- Psychological or emotional harm

Serious harm is defined in Section 113 of the Privacy Act 2020.
If you suspect a privacy breach may result in extreme harm, call 111 immediately and report the breach to us through NotifyUs.

Examples of extreme harm include:

- Imminent threats to national security.
- Physical violence or kidnapping.
- Financial hardship.
- A risk that an individual's life could be in danger.

How to report privacy breaches

Report privacy breaches to the Office of the Privacy Commissioner through NotifyUs. It will guide you through the steps to report your privacy breach and instruct you on the information you need to provide.

When to report privacy breaches

Suppose an organisation experiences a privacy breach and makes a reasonable assessment that it may result in serious harm to someone. In that case, it is a legal requirement for it to notify the Privacy Commissioner and affected individuals as soon as practically possible.

There may be reasons why you hold off notifying those affected by your organisation's privacy breach, such as if you are concerned that informing someone may adversely affect their mental health. Exceptions are detailed in Section 116 of the Privacy Act 2020.

> *Organisations failing to report notifiable privacy breaches to OPC may receive fines of up to $10,000.*

Who is responsible for reporting privacy breaches?

An organisation's privacy officer is responsible for reporting privacy breaches.

Under the Privacy Act 2020, any organisation or self-employed person that collects personal information must appoint a privacy officer.

In smaller organisations, the manager is normally responsible for all legal compliance, including privacy. If an organisation consists of just one person, they are, by default, the privacy officer.

Large organisations, or organisations that handle a lot of personal information, may need one or more employees focusing exclusively on privacy matters.

What about near misses or non-notifiable breaches?

Often organisations or individuals will narrowly avoid a serious privacy breach through sheer luck.

For example, you might be about to send an email containing personal information to the wrong person. Or you may have drafted an email containing sensitive information to a list of people and CC'd each email address, rather than BCC'd.

In each of these instances, a breach could be avoided if, just before clicking 'send', you double check and rectify your mistake.

Near misses provide the perfect opportunity for you to examine how you handle customer or client information and improve your privacy game.

I’ve reported my privacy breach. Now what?

After you have notified us of a privacy breach, any action we take will depend on the nature of your breach, the number of people impacted and the actual or potential harm.

If you used the NotifyUs tool to report the incident, you will receive an automated email (to the address you entered in the form) confirming the tool has processed your report.

You can expect to receive an acknowledgement email from our Office if you report a breach.

Other actions we may take include:

- Asking for further information from the notifying organisation.
- Providing advice.
- In cases where an organisation is failing to take appropriate steps promptly, we may take other actions to encourage or require the organisation to protect the privacy interests of the individuals affected. Such steps may include publicly naming the organisation or issuing a Compliance Notice (to do something or stop doing something).
- We prefer to work with organisations to gain the best outcomes for affected individuals and to avoid recurrences.

RESPONDING TO PRIVACY BREACHES

There are four key steps in dealing with a privacy breach:

1. Contain
2. Assess
3. Notify
4. Prevent

STEP 1: Contain

Once you discover a privacy breach has occurred, you should act immediately to contain it.

Steps to help contain a breach could include:

- Diagnosing what went wrong and disabling any systems that may be compromised until they have been secured.

- If your organisation can remotely wipe information from devices that was mistakenly sent to someone by you, you should do so.

- Trying to retrieve lost information, e.g. if you have sent a letter to the wrong person, see if you can get the recipient to send it back unopened.

- Cancelling or changing computer access codes and fixing any weaknesses in the organisation's physical or electronic security.

- Appointing someone within the organisation to lead and conduct an initial investigation into what has happened. A more detailed review can be carried out later if necessary.

- Assembling a response team. Such a team may include people from within the organisation as well as external parties which have the expertise to deal with the situation (for example, IT analysts or risk advisers).

- Considering who outside the organisation needs to be told about the breach, such as CERT or NetSafe - also, assessing whether your insurer, internal auditors, risk managers and legal advisers need to be informed.

Extra Tips

- If the breach involves theft or other criminal activity, inform the Police.

- Do not destroy information. It may be needed by your organisation or Police to find the cause of the issue.

STEP 2: Assess

Assessing a privacy breach as quickly as possible can help an organisation understand the steps needed to appropriately respond.

Knowing what information is involved will help you determine whether serious harm has occurred or is likely to occur and whether it is appropriate to tell the individuals affected.

For example, a leaked list of subscribers to an adult magazine is likely to be more sensitive and, therefore, more likely to cause serious harm to the individuals affected than a leaked list of subscribers to a newspaper.

The criteria for assessing the likelihood of serious harm stemming from a privacy breach is laid out in section 113 of Privacy Act 2020.

Those criteria are:

- **Any action taken by the organisation to reduce the risk of harm following the breach**

  Have you taken steps to contain the breach? See STEP 1: *Contain* above.

  Do you have a breach response plan? Such a plan outlines the procedures that your organisation will take following a breach.

  Try to identify the size and scope of the breach, including the number and nature of the likely recipients as well as the number of affected people. Identify the risk of the information being circulated further and respond accordingly.

- **Whether the personal information is sensitive in nature**

  The more sensitive the information involved in a breach, the higher the risk of harm to the people affected. Sensitive information is typically personal information relating to someone's health, genetic or ethnic background, finances, identity documents, political or religious beliefs, sex life or sexual orientation.

  Sensitive information may also relate to whether someone is affiliated with a trade union or if they have committed any crimes. The disclosure of a person's sensitive information may cause them serious harm.

  Context matters. Personal information which might not normally be considered sensitive, such as email addresses, may, in specific circumstances, be considered sensitive.

- **The person or body that has obtained or may obtain personal information because of the breach (if known)**

  Was the receiver a trusted, known person or organisation that can be expected to return the information?

Or, was the information taken by, or given to, an unknown receiver, someone who might pose a particular risk, or to a wide range of people who may include those who might misuse the information?

Knowing who has received the information will shape how you respond.

- **Whether the personal information is protected by a security measure**

  If breached personal information is password secured or encrypted, there is a lesser chance of it being accessed and misused than if it is unprotected.

  You should consider whether the security measures that protect information involved in a breach are likely to be effective at preventing access to it in the circumstances?

- **Any other relevant matters**

STEP 3: Notify

Being open and transparent with people about how personal information is being handled is a fundamental rule of privacy, especially when there has been a breach. Notification can also be a key step in helping people affected by a breach.

If a privacy breach creates a risk of serious harm to people, those affected should generally be notified. Prompt notification can enable people to take steps to protect themselves and regain control of their information.

When should you notify people?

You must inform the Privacy Commissioner of serious privacy breaches as soon as you practically can after becoming aware of them. Our expectation is that you will do this within 72 hours. You can do this using *NotifyUs*. If a breach looks serious when you discover it, you should report it rather than taking a 'wait and see' approach.

In most cases, you will also need to notify the people affected by the breaches unless an exception applies, such as if notifying them would adversely affect that person's mental health.

> *Only notify people if you are sure their information has been compromised by the breach.*

Incorrectly notifying the wrong people that their information has been breached may cause them unnecessary stress and harm.

If there is no risk of serious harm, it is not necessary to notify people of a privacy breach. Sometimes, notification can do more harm than good. Each incident needs to be considered on a case-by-case basis.

Things to consider:

- What is the risk of harm to people whose information has been breached?
- Is there a risk of identity theft or fraud?
- Is there a risk of physical harm?
- Is there a risk of humiliation or loss of dignity, damage to someone's reputation or relationships? For example, when the lost information includes mental health, medical or disciplinary records?
- What is the person's ability to avoid or minimise possible harm?
- What are the legal and contractual obligations?
- Consider the impact notification of a breach may have on at-risk people. You may then decide not to inform them or do so with particular care.

NotifyUs helps you assess how serious your breach is and whether you will need to notify the Privacy Commissioner.

If law enforcement authorities are involved, check with those authorities on when to notify so that their investigation is not compromised.

You don't always need to notify the people involved, or give public notice, of a notifiable privacy breach.

When you don't need to notify

You don't need to notify the people involved, or give public notice, of the notifiable privacy breach if you believe that the notification or public notice will:

- prejudice the security, defence, or international relations of New Zealand
- prejudice the maintenance of the law by a public sector agency
- endanger someone's safety, or
- reveal a trade secret.

Notifying someone else – at-risk people

You don't need to notify a person about, or give public notice of, a notifiable privacy breach involving their personal information if:

- the person is under the age of 16 and you believe that the notification or public notice won't be in their interests, or
- after you first consult that person's health practitioner (where practical), you believe that the notification or public notice will likely prejudice that person's health.

In those circumstances, however, you must:

- first think about whether it would be more appropriate to contact the person's parent, guardian or other representative, and

- before deciding whether to contact the person's parent or guardian, consider the person's individual circumstances and the circumstances of the privacy breach itself.

Then, you must notify the person's parent, guardian or other representative (rather than notify the person involved or give public notice).

Delaying notification or public notice

You can also delay notifying the people involved, or giving public notice, of the notifiable privacy breach if you believe that:

- the notification or public notice may have risks for the security of personal information that you hold for example, if you have to patch a security exploit to avoid a further privacy breach); and
- those risks outweigh the benefits of informing the affected people.

However, you can delay the notification or public notice only while those risks continue to outweigh those benefits.

In any case, you should not delay or refuse to tell us about a notifiable privacy breach. Contact us to find out how we can help.

How to notify affected people

It is always best to notify affected people directly - by phone, letter, email or in person. Direct notification is more sincere and personal.

Public Notices

Where it is not reasonably practical to notify individuals directly, you may notify them publicly.

Examples where it is not practical for an organisation to notify people individually of a breach could be when the organisation does not know exactly which people were affected by a breach or if it is prohibitively expensive. Details around issuing a public notice are specified in Section 115 of the Privacy Act 2020.

Public notices can be issued by posting an advertisement on a news website or making an announcement on radio or television. They should be in a form in which no affected individual is identified. Using multiple methods of notification may be appropriate.

It is also important to consider whether notification might reveal the value of the missing information to the likes of hackers or criminals. If you are notifying at-risk people, consider notifying them through or with a support person.

Who should notify customers/stakeholders?

Organisations that have direct relationships with its customers, clients or employees should be the party to notify the affected people. For example, if a credit card information breach comes from a retailer, the credit card issuer would be the best agency to inform the customer.

What to say?

Breach notifications to individuals should generally include:

- Information about the incident, including when it happened.
- A description of the personal information that was disclosed and what has not been disclosed.
- What the organisation is doing to control or reduce the harm.
- What the organisation is doing to help people and what steps those affected can take to protect themselves.
- Contact information for enquiries and complaints.
- Offers of assistance when necessary, for example, advice on changing passwords.
- Whether the organisation has notified the Office of the Privacy Commissioner.
- Contact information for the Privacy Commissioner.

Notifying third parties

Organisations should consider whether the following groups or organisations should also be informed. Bear in mind any obligations of confidentiality.

- Police
- insurers
- professional or other regulatory bodies
- credit card companies, financial institutions or credit reporting agencies
- third party contractors or other parties who may be affected
- internal business units not previously advised of the privacy breach, for example, government relations, communications and media relations
- other members of senior management
- the board
- the government minister
- union or other employee representatives.

STEP 4: Prevent

There are several steps an organisation can take to minimise or prevent future privacy breaches.

The most effective strategy is having a well-thought-out security plan for all personal information you hold.

A strong security standard to use is the International Standards Organisation Information Security Management Standard.

Organisations should review policies to minimise the collection and retention of personal information, investigate the cause of any breaches they have experienced and update their prevention plans.

The significance of a breach, and whether it happened due to a systemic problem or an isolated event, will help inform the steps needed to prevent future breaches.

These steps could include:

- an audit of both physical and technical security
- a review of policies and procedures
- a review of employee training practices
- a review of any service delivery partners caught up in the breach.

The prevention plan may include an audit requirement to ensure the plan is put into action.

PRIVACY BREACH PREVENTION MEASURES

You can follow some simple tips to avoid some of the most common breaches.

Sending emails safely

- Establish email procedures that involve double-checking the address to ensure it is correct before pressing 'send'.
- For mass emails, double-check that all emails are in the bcc, not the cc field.
- Have a policy on the types of documents that staff may send by email.
- When including attachments, ensure you have the right ones.
- Spreadsheets can contain a lot of information. Protect them using passwords. Check if other personal information is hidden behind spreadsheet document tabs and in pivot tables.
- If sending spreadsheets, get employees to check if the entire document needs to be sent or if there is a way of extracting only the relevant information intended for the recipient.

Preventing employee browsing

- Foster and maintain a culture of respect for personal information.
- Ensure there are systems in place that monitor employee access to files.
- Have systems to prevent employees from accessing files for non-work purposes.
- Include a policy about employee browsing in the code of conduct with clear consequences for violations of the code.
- Have different levels of security for types of files, for example, general access and restricted.
- Ensure that staff members are aware of organisational practices around monitoring and auditing of file access.
- If you are developing a new IT system, employ Privacy by Design techniques to reduce future risk.

Preventing the theft or loss of devices and documents

- Pay attention to the physical security of mobile and portable devices, including smartphones, laptops, USB sticks and portable hard drives.
- Review your organisation's policy about the types of information that can be stored on a portable device.
- Use extra security measures for portable devices such as encryption, password locks, remote wiping and physical security.
- Protect sensitive documents and information using physical security measures such as locks or filing cabinets.
- Lock workstations and laptops.
- Don't leave papers, computers or other electronic devices visible in homes or in parked cars.
- Don't leave sensitive information lying around, including on printers, photocopiers, or in storage.
- Delete personal information and other data when it is no longer needed.

- Report thefts to Police and let them know if the stolen equipment contains sensitive information.
- Have a comprehensive workplace security policy for BYOD (bring your own device).

Preventing employees from disclosing information

- Control which staff members have access to sensitive information.
- If an employee deliberately discloses information without permission, disable their access to electronic systems and ensure they return keys and access cards.
- Make sure employees understand the importance of protecting personal information when working from home.
- Store sensitive paper records in locked filing cabinets. Lock mobile phones, laptops and other portable storage devices.
- Keep files separate on content management systems and put in place access controls and carry out routine audits.
- Ensure no personal information is stored on obsolete databases.

Storing personal information securely

- Know who has access to sensitive information.
- Be sure that sensitive information cannot be accessed publicly through your website or the internet. If you can access it online without a password, so can others.
- Send data safely, especially in remote access and client/server transmissions.
- Don't use unsecured Wi-Fi when working with or sending data.
- Don't email or instant message unencrypted sensitive information.
- Check for sensitive information in email attachments, especially when forwarding them to others.

Disposing of information safely

- Destroy or securely delete sensitive information prior to re-use or disposal of equipment or media.
- Shred physical records of personal information you no longer need.
- Do not re-use paper records.

Dealing with personal information wrongly published to websites

- Contact the website or business and ask it to take the information down immediately.
- If a business or website does not comply with a takedown request, you can contact the Office of the Privacy Commissioner to see if we can assist.
- Make sure you have a copy of the information before it is deleted from the website, so you know who the affected people are.
- Identify how the information came to be published on the website.

Keeping software up-to-date and using strong passwords

- Computer operating systems and mobile device apps need to be kept up to date to avoid system vulnerabilities. Patches are regularly issued by Microsoft, Google, Apple and others. Updating your device software protects you from hackers and makes your device more secure.

- Carry out regular security checks and audits.
- Be cautious when using personal accounts for work purposes.
- Use strong passwords, change them regularly and don't share or reveal them.
- If a computer is used by different staff - it should have a strong password if it connects to your work network.
- Don't click on unknown or unexpected links or attachments - these can infect your computer.
- Avoid opening files sent via IM (instant messaging) or P2P (peer-to-peer) software on a machine that contains restricted data. These files can bypass anti-virus screening.
- Don't install unknown programs on your computer. These can be computer viruses or open a "back door", giving others access to your computer without your knowledge. Consider restricting the ability to install software.

EXAMPLE SCENARIOS

Please note: These are a mixture of real and hypothetical privacy breaches.

SCENARIO 1: Rugby club mistakenly sends email to entire mailing list

A small-town rugby club planned to email five of its players, informing them that their club fees were overdue and if they did not pay, they would no longer be able to play.

The club’s chairman drafted an email containing this warning, but instead of emailing the five players in question, he accidentally emailed the club’s entire email list of 50 people.

A parent of one of the players complained to the club that her son had experienced significant embarrassment due to the email being seen by others in his team and community. The mother informed the club that the delay in payment of his fees had been due to her experiencing financial difficulties.

The mother did not hear from the club for several days after contacting them and decided to complain to the Privacy Commissioner.

Following OPC’s contact with the club’s chairman, he sincerely apologised to the mother for the mistake, stating it was unacceptable. He assured the Privacy Commissioner and the players that the club had implemented processes to ensure it would not occur again.

The player’s mother accepted this apology, and the complaint file was closed.

> *When sending emails containing sensitive information to groups of people, double-check the email addresses. If sending the same email to many people, BCC, rather than CC each email address.*

Note: This breach is unlikely to be notifiable as the risk of serious harm to the individual affected is minimal. Whether a breach is notifiable or not, you can always notify us.

SCENARIO 2: Employee browses accounts of friends and family

A New Zealand bank conducted a routine audit of its staff members' access to customer records.

The audit revealed an unusual pattern of client account enquiries in one branch over a 12-month period.

Following an internal investigation, the bank discovered that a staff member had been browsing the accounts of his friends and family without any legitimate reason. There was no evidence he had shared that information with third parties.

The bank recognised that the information the staff member had accessed was sensitive, and there was a real risk of serious harm to the customers due to the staff member's personal relationship with them. The bank notified the Office of the Privacy Commissioner and affected customers.

Following the bank's internal investigation, the staff member was dismissed from his position.

The bank informed OPC that it had taken measures to prevent unauthorised access to customers' accounts by staff members. The bank committed to ensuring all staff members received additional training and were made aware of their obligations to act appropriately and not access customer's personal information without legitimate work-related reasons.

> *Maintain a culture of respect for personal information in your workplace. Only access customers' personal information for legitimate work reasons.*

SCENARIO 3: Staff members sends spreadsheet to wrong person

A woman contacted a government agency seeking a registration form to sign up for a programme. In the email replying to her, an employee accidentally sent a spreadsheet attachment instead of the form she had requested. The spreadsheet contained the details of 1,500 other applicants including their names, birth dates, contact details and addresses.

The woman called the agency to tell them what had happened. The agency asked the woman to delete the information, which she did.

An internal inquiry revealed the employee did not follow internal protocol when sending the request form and simply went to the 'recent document' tab in the database and selected the incorrect attachment.

The agency assessed the breach using the self-assessment tool available on OPC's website under NotifyUs. Because the recipient of the spreadsheet had deleted it, they determined that there was little risk of serious harm occurring and decided not to report the breach to the individuals concerned or OPC.

After this incident, the agency updated its staff privacy training procedures and committed to undertaking more frequent audits of its practices.

> *Always check attachments before sending them. Make sure you are not mistakenly sharing other people's personal information.*

SCENARIO 4: Database of customer information is hacked

An online gaming company held a database of its customers' information, including their names, dates of birth, email addresses, postal addresses, and credit card numbers.

During a routine security check, the gaming company discovered its servers had been compromised, and more than 10,000 of its customers' accounts had been hacked.

The company took immediate steps to contain the breach (including temporarily shutting down its servers) and notified OPC. Based on its belief that criminal activity had been involved, it also contacted Police, CERT and employed a security firm to enhance the security of its systems.

When Police were satisfied it would not compromise their investigation, the company notified their affected customers. It explained to customers exactly what happened and when; that Police were investigating and OPC had been notified. It also suggested that affected customers monitor their credit card accounts and contact their financial institution if they had any concerns.

> *Carry out regular security audits of your systems. If you have a privacy breach, act swiftly to contain it.*

SCENARIO 5: Insurance company resells iPad containing personal information

A man sent a broken iPad through to an insurance company as part of a claim. The insurance company wrote the iPad off and compensated him.

The insurance company's contractor later repaired and sold the iPad on Trademe. The purchaser of the iPad contacted the original owner advising him that he had access to his data. The buyer requested the former owner's password so that he could delete the man's iCloud account from the iPad.

The former owner's iCloud account contained family photos, credit card details and passwords. The former owner was concerned about who might have access to his personal information and contacted the insurance company to complain. The insurance company then reported the breach to OPC.

The insurance company recognised that its procedures were not fit for purpose and updated its policies. The new policy included instructions for contractors requiring them to ensure personal data was deleted from devices. The company compensated the man for the emotional harm he had suffered.

> *Ensure no personal or customer information remains on digital devices when your organisation no longer needs them.*

SCENARIO 6: School holiday programme publishes photos of children without consent

A mother enrolled her daughter in a school holiday programme. When filling out the enrolment form, the mother ticked 'No' to the question requesting permission for her daughter's name, photo and/or video to be published in programme newsletters or used for publicity.

A local news website published a photograph of the daughter and three other children. The picture named the children identified them as participants in the holiday programme and stated where the programme was held. The mother complained to OPC that her daughter's privacy had been breached.

The mother advised OPC that in the past, she and her daughter had been harassed by the mother's former partner. She had contacted the Police, who advised her that no information should be shared with the former partner that would enable him to have access to the family. Because of the publication, the mother feared for their safety.

OPC accepted that in this situation, there was potential for serious harm. It was clear that the publication of the daughter's name, photograph and location could adversely affect her.

The holiday programme apologised for the incident and expressed genuine regret. It put new procedures in place to prevent any recurrence.

> *Ensure you have people’s permission before sharing their photos or other personal information in publications.*

More case notes are available on our website.

ADDITIONAL SUPPORT

What support is available for victims of privacy breaches?

People impacted by privacy breaches may become victims of identity theft, which can ruin lives. IDCARE is Australia and New Zealand's national identity and cyber support service. It offers free phone consultations and advice and has helped thousands of individuals and organisations reduce the harm they experienced from the misuse of their identity information.

> *If you have been negatively affected by a privacy breach, you can contact IDCARE for help and support at www.idcare.org or on 0800 121 068*

Privacy breach insurance

If your organisation handles significant quantities of personal information, you may wish to consider cyber or privacy breach insurance*.

Cyber and privacy breach insurance are available from multiple insurers and cover privacy breaches and security liability as well as third party costs that you, as the insured, become liable for in the event of a privacy breach.

*OPC does not endorse or recommend insurance policies. If you deem a privacy breach insurance policy necessary, you should research and find a policy suitable for your needs.

Contact us:

- www.privacy.org.nz
- NotifyUs: www.privacy.org.nz/notifyus
- Enquiries line (for general enquiries):
  0800 803 909 (Monday to Friday, 10:00 am to 3:00pm).
- enquiries@privacy.org.nz
- PO Box 10-094
  Wellington 6143