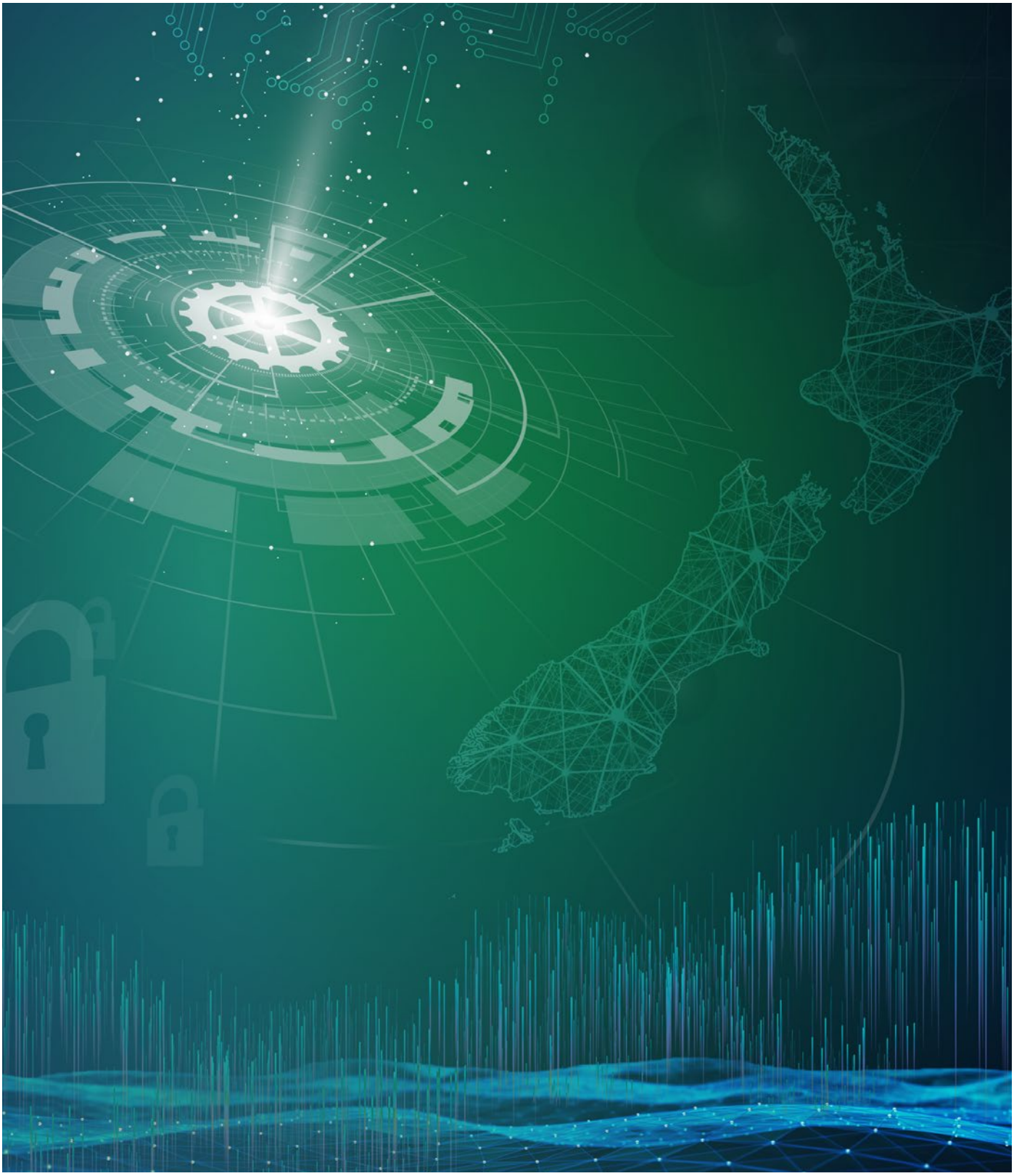
PRIVACY GUIDE

Mandatory Data Breach Notification

A guide to preparing for the new notifiable privacy breach requirements and other changes under the Privacy Act 2020



June 2020

WWW.BELLGULLY.COM

BELL GULLY

Contents

Introduction

On 1 December 2020, the Privacy Act 2020 (**Privacy Act**) will come into force and replace the Privacy Act 1993. This follows a very long period of review dating back to the appointment of the Law Commission to review the Privacy Act in 2006. Over that time, there has been exponential growth in data-driven innovation, significant developments in international data protection regulation and a plethora of high profile data breaches. Against that background, the need to modernise New Zealand's Privacy Act has had strong bipartisan and industry support.

> **A key purpose of the Privacy Act is to promote individuals' confidence that their personal information is secure and will be treated properly in an increasingly digital and data-rich society. One of the key changes to achieve this purpose is the introduction of a mandatory reporting regime for 'notifiable privacy breaches'.**

It is essential that you take action to ensure that your privacy practices are up-to-date and reflect the applicable changes under the new Privacy Act.

The updates that you adopt should also build in flexibility for future developments, as we expect further changes will follow. These are likely to arise from ongoing review of New Zealand's privacy laws, developments in international legislation with reach to New Zealand businesses, as well as a developing industry-led response in New Zealand to Open Banking and other data driven challenges and opportunities. Your Bell Gully team is monitoring these developments and is available to assist.

To assist you with preparing for the notifiable privacy breach regime and other changes under the Privacy Act, we have prepared this practical guide which provides:

- an overview of the new notifiable privacy breach regime
- a summary of other changes
- a checklist of key steps to ensure you are prepared.

If you require further guidance on any aspect of this guide or other legal issues arising from the new Privacy Act, please contact your usual Bell Gully advisor, or our specialist privacy team outlined in Section 8 of this guide.

Laura Littlewood
PARTNER

DDI +64 9 916 8928 MOB +64 21 828 429
laura.littlewood@bellgully.com

Tania Goatley
PARTNER

DDI +64 9 916 8766 MOB +64 21 326 731
tania.goatley@bellgully.com

Richard Massey
SENIOR ASSOCIATE

DDI +64 9 916 8824 MOB +64 21 208 2355
richard.massey@bellgully.com

At a glance: the new notifiable privacy breach regime

From 1 December 2020, an entity must notify the Privacy Commissioner and affected individuals if it is aware a notifiable privacy breach has occurred.

1. WHAT is a notifiable privacy breach?

A privacy breach is notifiable if it is reasonable to believe it has caused serious harm to an affected individual (or individuals) or is likely to do so.

Refer to page 5.

2. WHICH entities must comply?

All entities that are subject to the Privacy Act must comply with the new regime. This now includes almost every New Zealand entity, as well as overseas entities in the course of carrying on business in New Zealand. Limited exceptions apply.

Refer to page 7.

3. WHO must be notified?

The Privacy Commissioner and affected individuals. Limited exceptions apply.

Refer to page 8.

4. WHEN should they be notified?

An entity should notify the Privacy Commissioner and affected individuals as soon as reasonably practicable after becoming aware that a notifiable privacy breach has occurred. Limited exceptions apply.

Refer to page 9.

5. HOW should they be notified?

Individuals should be notified directly, or through a public notice if it is not reasonably practicable to notify an affected individual or each member of a group.

The notification must cover a prescribed list of information.

Refer to page 10.

When does it come into force?

1 December 2020.

What are the consequences of getting it wrong?

Under the Privacy Act, failure to notify the Privacy Commissioner of a notifiable privacy breach (without reasonable excuse) is an offence with a fine of up to $10,000.

A failure to notify may also amount to a breach of other laws (such as directors' duties, fair trading and employment legislation), as well as contractual obligations.

How can you prepare?

Mitigating the risks of a breach occurring is not enough. It is essential that you are adequately prepared to respond if a breach occurs.

This includes ensuring you have a Privacy Breach Response Plan in place.

You should also consider whether it is timely to undertake a full privacy "Health Check" to review your privacy management framework as a whole, including contracts with suppliers who have access to personal information.

Please refer to the checklist on page 12.

* Privacy Act 2020, Part 6, Sections 112 - 122

1. WHAT is a notifiable privacy breach?

The Privacy Act has introduced a new regime for mandatory reporting of a notifiable privacy breach.

A notifiable privacy breach means:

A privacy breach

A privacy breach can be either a:

- **Confidentiality or integrity breach** — unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, personal information; or
- **Availability breach** — an action that prevents an entity from accessing personal information on either a temporary or permanent basis (e.g., a denial-of-service attack).

that it is reasonable to believe

Guidance **published by the OAIC**[1] (on similar wording under the Australian regime) indicates that this means the assessment of whether a privacy breach is notifiable is:

- an **objective assessment**
- determined from the viewpoint of a **reasonable person in the entity's position** (rather than the viewpoint of an individual whose personal information was breached)
- who is **properly informed** (based on information immediately available or following reasonable inquiries or an assessment of the data breach).

has caused serious harm

See further discussion on page 6.

to an affected individual or individuals

This means the individual or individuals to whom the information relates, regardless of whether they are located inside or outside of New Zealand.

or is likely to do so

In Australia, similar wording imports a test of being "**more probable than not**", but New Zealand Courts so far have preferred formulations such as "**appreciable possibility**" in other contexts.

[1] A range of Privacy Act 2020 resources are available on the Office of the Privacy Commissioner's website. As New Zealand's regime is closely aligned with the equivalent framework in Australia, we have also referred to useful guidance published by the Office of the Australian Information Commissioner.

HARM — threshold test

Harm is an established concept under New Zealand privacy laws as it is relevant to an assessment of whether an interference with privacy has occurred. Harm may include:

Specific damage

Financial loss, loss of employment, physical injury or other forms of specific harm.

Loss of benefits

Any adverse effect on the rights, benefits, privileges, obligations or interests of the individual.

Emotional harm

Significant humiliation, significant loss of dignity or significant injury to feelings.

For example, in the context of a privacy breach, harm may include identity theft or fraud (as a result of unauthorised access to identify documents), financial loss (as a result of compromised passwords or costs associated with the steps required to mitigate the potential harm from the breach) and psychological distress (as a result of unauthorised disclosure of sensitive personal information).

SERIOUS HARM — relevant factors

Whether harm is "serious harm" depends on the unique circumstances of a privacy breach and requires an assessment on a breach-by-breach basis. The Privacy Act states that the assessment must include consideration of the following factors:

Nature of information

Whether the personal information is sensitive in nature. The more sensitive the information, the higher the risk of harm to people affected. For example, credit card details, health information and identity documents (passport, driver licence).

Mitigation

Any action taken by the entity to reduce the risk of harm following the breach. For example, cancelling or changing computer access codes, disabling the breached system and trying to get lost information back.

Security measure

Whether the personal information is protected by a security measure. If the information is protected (e.g. by encryption or other security measures) then the risk of serious harm may be reduced.

Recipient

The person or body that has obtained or may obtain personal information as a result of the breach. The risk of serious harm is likely to be greater if personal information is in the hands of people with unknown or malicious intentions. For example, a ransomware attack.

Nature of harm

The nature of the harm that may be caused to affected individuals.

Refer to the discussion at the top of this page.

Other

Other relevant factors will depend on the particular circumstances of the breach. For example, how many individuals are affected, how wide spread is the breach and how long has it been occurring.

Q: We use a marketing platform to facilitate our EDM marketing. The platform provider has notified us that, as result of a security breach, our customer distribution list has been downloaded by an external IP address. The list included name, gender and email address. As part of our investigation, we have discovered that some customers have received an email that fraudulently claimed to be sent from us asking for credit card details. Are we required to notify?

A: A privacy breach has occurred. Whether it is reasonable to believe the breach is likely cause serious harm (and is therefore notifiable) requires an assessment of the relevant factors set out above. **In this scenario, notification is required**. The attacker has used the distribution list for the purposes of fraud and identity theft, which is likely to cause serious financial harm to the relevant individuals.

Q: An error in our user authorisation controls has resulted in a vulnerability that potentially enabled customers to access the accounts of other customers. Our security team quickly identified and rectified the issue and confirmed that the vulnerability was not exploited. Are we required to notify?

A: A privacy breach has occurred. Whether it is reasonable to believe the breach is likely cause serious harm to relevant individuals (and is therefore notifiable) requires an assessment of the relevant factors set out above. **In this scenario, notification is not required**. The successful mitigation steps taken by your security team, to avoid any risk of harm, is a relevant consideration in assessing whether notification is required. You should retain a record of the breach and your assessment that notification was not required. You should also carry out a review to assess whether preventative action is required to ensure a similar breach does not occur in future.

2. WHICH entities must comply?

The Privacy Act covers all personal information collected or held by a New Zealand entity, or an overseas entity in the course of carrying on business in New Zealand, regardless of where:

- **the information was collected or held**
- **the relevant person is located.**

The notifiable privacy breach regime applies to all entities that are subject to the Privacy Act. This now includes almost every New Zealand entity, as well as overseas entities in the course of carrying on business in New Zealand.

There is no minimum threshold. For example, the Privacy Act applies irrespective of an entity's annual revenue or number of employees.

New Zealand entities

The Privacy Act applies to almost all New Zealand entities, including a:

- private sector entity established under New Zealand law
- private sector entity having its central management and control in New Zealand
- public sector entity or department
- individual who is ordinarily resident in New Zealand
- a court or tribunal (except in relation to its judicial functions).

Overseas entities

The Privacy Act also applies to personal information collected or held by an overseas entity in the course of carrying on business in New Zealand.

"Carrying on business in New Zealand" is not defined but an entity is treated as carrying on business in New Zealand whether or not it:

- has a place of business in New Zealand
- charges any monetary payment for the supply of goods or services
- intends to makes a profit from its business in New Zealand.

It does not include the government of an overseas country.

Exceptions

Limited exceptions apply. For example, the Privacy Act, including the notifiable breach regime, does not apply to the House of Representatives, a court in relation to its judicial functions or any news entity in relation to its news activities.

Q: I don't have a physical place of business in New Zealand. Do I still need to comply with the Privacy Act and notifiable breach regime?

A: You must comply if you carry on business in New Zealand, whether or not you have a place of business here. Whether you are carrying on business in New Zealand is a question of degree and relatively minimal activity in New Zealand can be sufficient. It is likely that you will be carrying on business in New Zealand if you offer goods and services to New Zealand consumers.

Service providers

Under the Privacy Act, a principal entity remains responsible for information held by a service provider, including a cloud storage provider, on its behalf.

Q: My customer records are held by a cloud storage provider in Singapore. Its systems have been accessed through a phishing attack and it has notified us that our customer records may have been compromised. Who is responsible for complying with the notifiable privacy breach regime?

A: As the principal entity, you remain responsible for complying with the notifiable privacy breach regime. Your contract with the cloud service provider will also be relevant – for example, ideally, the cloud service provider should have contractual obligations to assist you with complying with your obligations and mitigating any harm, as well as contractual restrictions on making any public notifications that refer to you or your customers.

3. WHO must be notified?

You must notify the Privacy Commissioner and affected individuals (or, in some circumstances, an individual's representative).

There are no exceptions to the requirement to notify the Privacy Commissioner. However, there are some limited exceptions when it comes to notifying an affected individual.

General exceptions

You are not required to notify an affected individual, or give public notice of a notifiable privacy breach, if you believe that the notification or notice would be likely to:

- endanger the safety of any person
- reveal a trade secret
- prejudice the health of the individual
- prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand
- prejudice the maintenance of the law by any public sector entity, including the prevention, investigation, and detection of offences.

Exceptions relating to particular individuals

You are not required to notify an affected individual or give public notice (relating to a particular individual) if:

- the individual is **under the age of 16** and you believe the notification would be contrary to that individual's interests
- you consult with the individual's health practitioner (where practicable) and believe that the notification would be likely to prejudice the **health** of the individual.

If you are relying on this exception, you must:

- consider whether it would be appropriate to notify a **representative** (taking into account certain matters, including whether a representative can be readily identified, as well as the circumstances of both the individual and the privacy breach)
- notify at a **later time**, if circumstances change so that the exception no longer applies and there is still a risk of serious harm to the individual.

Other considerations

You may be required to notify other entities (outside the requirements of the Privacy Act). For example, depending on the nature of the breach, your insurer, the Police, CERT NZ or NZX, as well as customers or other parties to whom you have contractual obligations.

4. WHEN should they be notified?

You must notify the Privacy Commissioner and affected individuals as soon as practicable after becoming aware that a notifiable privacy breach has occurred.

Can entities delay notification?

You can delay notifying affected individuals if you believe that notification or public notice may have risks for the **security of personal information** and those risks outweigh the benefits of informing affected individuals. If you rely on this exception, you must notify once the grounds for delay no longer exist, or no longer outweigh the benefits of informing affected individuals.

Q: An attack on our security systems has resulted in a privacy breach and revealed a vulnerability in our wider systems. Can we delay notification?

A: When assessing when to notify affected individuals, you should consider whether notification should be delayed until the vulnerability has been fixed. This delay is permitted if notification would give rise to a risk of further exploitation of the vulnerability and that risk outweighs the benefits of informing affected individuals. You should still notify the Privacy Commissioner as soon as reasonably practicable after you become aware of the notifiable privacy breach.

5. HOW should they be notified?

Individuals should be notified directly, or through a public notice* if it is not reasonably practicable to notify an affected individual or each member of a group.

The notification must cover a prescribed list of information.

What are the requirements for notification?

Notice to Privacy Commissioner

- **Describe the breach**, including (if known):
  - the number of affected individuals
  - the identity of any person or body that you suspect may be in possession of personal information as the result of the breach.
- **Explain the steps taken (or intended to be taken) in response to the breach,** including whether any affected individual has been or will be contacted.
- If you are **notifying affected individuals** by way of **public notice**, explain the reasons for doing so.
- If you intend to **delay notification** to affected individuals, explain why a delay is needed and the expected period of delay.
- If you are relying on an **exception to notifying** affected individuals, state the exception relied on and set out the reasons for relying on it.
- State the names or give a general description of any **other entities** contacted about the privacy breach and the reasons for having done so.
- Give details of a **contact person** within your entity for inquiries.

Notice to Affected Individuals

- **Describe the breach**. This should include similar information to the notice to the Privacy Commissioner. However, in general, you should not identify the person or body that you suspect may be in possession of personal information as the result of the breach (except where a serious threat exists to the life or health of the affected individual or any other person).
- **Explain the steps taken (or intended to be taken) by the entity in response to the breach.**
- Where practicable, set out the steps (if any) the affected individual may wish to take to **mitigate or avoid** potential loss or harm.
- Confirm that the **Privacy Commissioner** has been notified.
- State that the individual has the right to make a **complaint** to the Privacy Commissioner.
- Give details of a **contact person** within your entity for inquiries.

* A public notice must comply with the procedure set out in the Privacy Regulations 2020.

6. Summary of other changes under the Privacy Act

The Privacy Act retains the current principles-based framework through the Information Privacy Principles (the IPPs). However, additional changes have been introduced to reflect the needs of the digital age. The table below summarises the key changes under the new Privacy Act (in addition to the Notifiable Privacy Breach regime discussed in this Guide).

Cross border protections *IPP 12*	The Privacy Act includes stronger protections relating to the transfer of personal information to an entity outside New Zealand. An entity can disclose personal information to a foreign entity if: (i) **comparable safeguards** will apply (e.g., if the foreign entity is in a prescribed country (which will be set out in regulations) or subject to contractual obligations that are comparable to the Privacy Act); or (ii) the individual concerned **authorises** the disclosure (after being informed that the destination does not have comparable protections).
Extra-territorial reach *Section 4*	The Privacy Act clarifies its application to overseas agencies and overseas activities. In particular (i) for a New Zealand entity, the Privacy Act applies to any action taken and all personal information collected or held by it, both inside and outside New Zealand; and (ii) for an overseas entity, the Privacy Act applies to any action and all personal information collected or held by it in the course of "carrying on business in New Zealand".
Service providers *Section 11*	The Privacy Act clarifies that, in certain circumstances, information is treated as being held by a principal entity, notwithstanding that it is held by a third party on the principal entity's behalf (e.g., where it is held by a cloud services provider for safe custody or processing).
Amendments to the IPPs *Section 22*	IPP 1 (ID Documents): An entity may not require individuals' identifying information unless it is necessary for the lawful purpose for which the information is collected. IPP4 (Children): IPP4 now emphasises that the manner of collection must be fair and not intrude to an unreasonable extent upon the personal affairs of the individual concerned "particularly in circumstances where personal information is being collected from children or young persons". IPP 13 (Unique identifiers): An entity must take reasonable steps to minimise the risk of misuse when displaying unique identifiers on computer screens or receipts, such as the use of truncated account numbers.
Access requests *IPPs 6 and 7* *Sections 41, 43, 48, 56, 57, 66 and 67*	The Privacy Act clarifies: (i) certain factors relevant to access requests (e.g., where a request is made under a threat of physical or mental harm); (ii) that documents may be provided to a requestor in hard copy or an electronic copy; and (iii) when a public or private sector entity may impose a charge for access or correction. Other changes include extending the time to comply with a request if it involves large amounts of information and further clarification on managing urgent access requests and transferring access requests.
News media exemption *Section 7*	The Privacy Act clarifies and amends the scope of the news media exemption. For example (among other changes) it covers all forms of media, including 'new' media such as bloggers.
Public register principles	The Public Register Privacy Principles have been removed from the Privacy Act.
New criminal offences and penalties - $10,000 *Section 212*	The Privacy Act creates new criminal offences for: (i) misleading an entity to obtain access to someone else's personal information; and (ii) destroying a document containing personal information with knowledge of a request related to it. A person is liable on conviction to a fine of up to $10,000.
Powers of the Commissioner *Sections 82-84, 92 and 123*	Under the Privacy Act, the Privacy Commissioner: (i) can make binding decisions on **access requests**; (ii) can issues **compliance notices**; and (iii) has increased **investigatory powers**.

Notably, the new Privacy Act does not include any changes that specially relate to data portability or data anonymization. In addition, it has not introduced a specific concept of sensitive data or other data categorisation.

7. Checklist: Are You Prepared?

Adopting a Privacy Breach Response Plan is an essential step to prepare for the new mandatory privacy breach notification regime. A holistic privacy management framework within your business is also important to reduce the risks associated with a privacy breach and the potential harm if a breach occurs. The relevant steps will depend on your business, but some common examples are set out below.

- **Privacy Breach Response Plan** — prepare, implement and test a response plan. This should cover notification obligations under the Privacy Act as well as any other notification steps that may be relevant to your business (e.g. GCSB, contractual obligations, government requirements, insurers). Ensure a copy can be accessed even when systems are "locked down" following a breach.
- **Privacy Review** — carry out a privacy review (or privacy 'health check') to make sure you understand the full 'life cycle' of information within your business, and your privacy practices are up to date. Bell Gully routinely undertakes privacy reviews and can assist you with this process.
- **Supplier contracts** — review your supplier contracts to ensure appropriate provisions are incorporated to reflect the new breach notification obligations as well as other changes under the Privacy Act. Consider the impact on other provisions, including force majeure, liability, data sovereignty, confidentiality, announcements and disaster recovery.
- **Customer contracts** — review your customer contracts to ensure appropriate provisions are incorporated to reflect the risk of a data breach as well as other changes under the Privacy Act. Consider the impact on other provisions, including force majeure, liability, data sovereignty, confidentiality and disaster recovery.
- **Governance** — consider whether your data strategy delivers on your purpose and is consistent with your values. Does it identify your strengths, weaknesses and maturity level regarding data? Consider whether privacy should be on the agenda for your risk committee.
- **Privacy Statement** — ensure your privacy statements are up-to-date and accurately and transparently reflect your collection, use and disclosure of personal information.
- **Policies and Procedures** — update your internal policies and procedures (e.g. privacy policies, Privacy Impact Assessments, IT/security policies) to support your data strategy and privacy management framework.
- **Training** — provide regular training to make sure your staff are aware of the policies and procedures in place and their obligations.
- **Security** — it is important your privacy framework is integrated across teams to ensure appropriate security measures (including access controls) are in place to prevent and minimise the risks of a privacy breach.
- **Retention** — make sure you have clear record-keeping and document destruction processes in place to ensure the information you hold is up-to-date and securely destroyed when no longer required.
- **Preserving privilege** — there is a risk that a privacy breach could lead to legal and regulatory claims. You should ensure your processes for responding to, investigating and reviewing a breach take into account legal privilege.
- **Insurance** — review insurance policies to ensure these are appropriate to your business and the risks associated with a privacy breach (including cyber attacks).

8. Any questions?

Please contact your usual Bell Gully advisor, or our specialist privacy team:

Laura Littlewood
PARTNER

DDI +64 9 916 8928 MOB +64 21 828 429
laura.littlewood@bellgully.com

Tania Goatley
PARTNER

DDI +64 9 916 8766 MOB +64 21 326 731
tania.goatley@bellgully.com

Richard Massey
SENIOR ASSOCIATE

DDI +64 9 916 8824 MOB +64 21 208 2355
richard.massey@bellgully.com

Susannah Shaw
SPECIAL COUNSEL

DDI +64 4 915 6525 MOB +64 27 644 4813
susannah.shaw@bellgully.com

Kristin Wilson
SENIOR ASSOCIATE

DDI +64 9 916 8913 MOB +64 21 658 320
kristin.wilson@bellgully.com

Tim Clarke
PARTNER

DDI +64 9 916 8347
tim.clarke@bellgully.com

Rachael Brown
PARTNER

DDI +64 4 915 6882 MOB +64 21 390 383
rachael.brown@bellgully.com

AUCKLAND
VERO CENTRE
48 SHORTLAND STREET
NEW ZEALAND

WELLINGTON
ANZ CENTRE
171 FEATHERSTON STREET
NEW ZEALAND