Parry Field Lawyers

# Key Concepts and Principles of Data Compliance

# Relevant Legislation

- Privacy Act 2020
- Fair Trading Act 1986
- Human Rights Act 1993
- Unsolicited Electronic Messages Act 2007

# Operational Data Governance Framework - Stats NZ

*"Data governance approaches and associated frameworks have not evolved to reflect the increasing volume and growing influence of data and information on business practice and strategic planning."*

*"There is a persistent low level of data and information management maturity"*

# Privacy Act 2020

The purpose of this Act is to promote and protect individual privacy including by providing a framework for protecting an individual's right to privacy of personal information.

**Personal Information** means information about an identifiable individual.

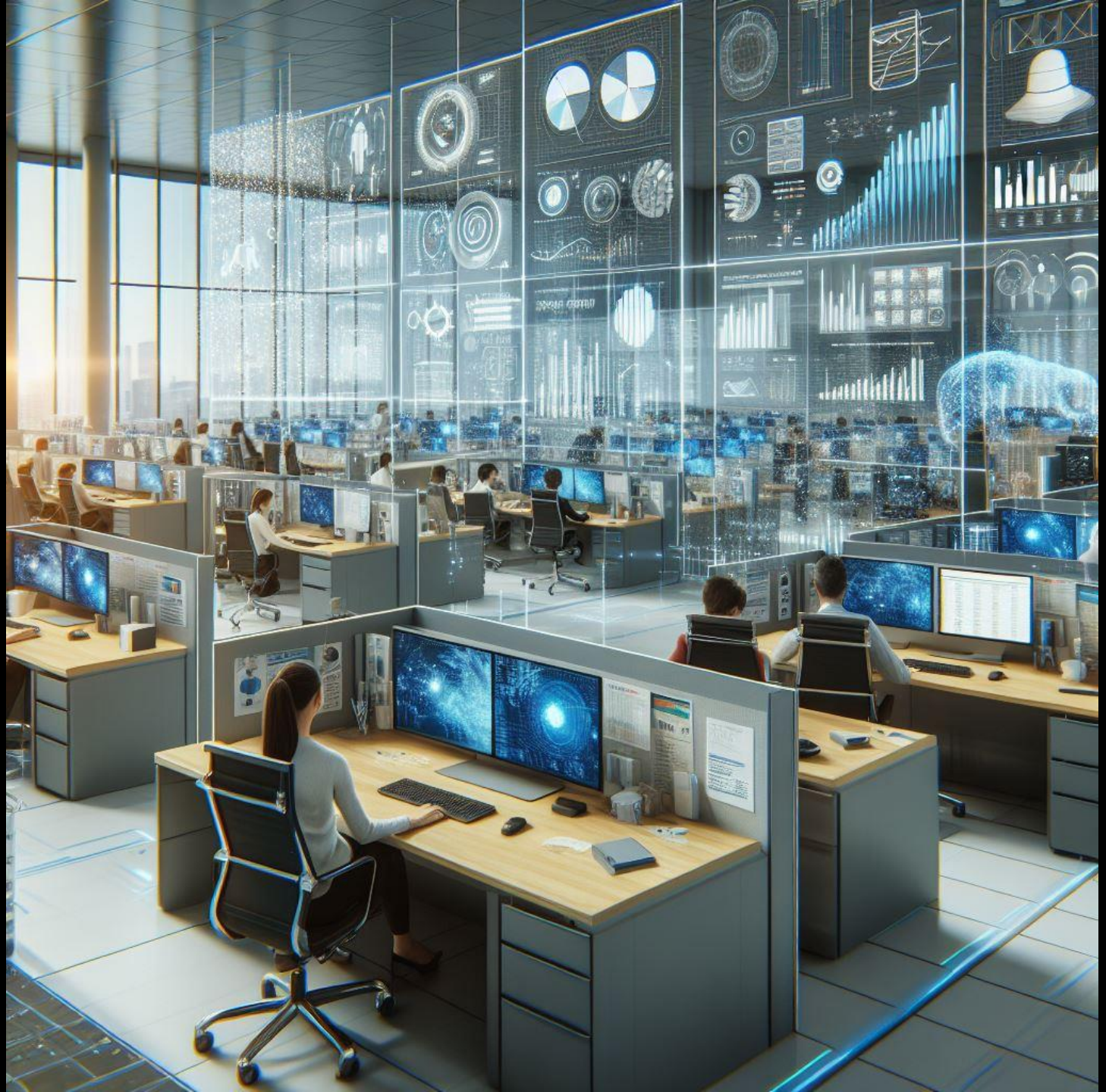
# Data Awareness

Who do you collect personal information about?

- Staff, clients, donors, suppliers …

What personal information do you collect?

- Names, contact details, activities, financial position, donation history, payment methods/details, memberships, health, biometric, employment history, criminal record.



# Information Privacy Principles

Privacy Commissioner Summary:

1. **Purpose** –
   - You can only collect personal information if it is for a lawful purpose and the information is necessary for that purpose.
   - You should not require identifying information if it is not necessary for your purpose.

# Questions to ask

- Who do we collect personal information from?
- What personal information do we collect?
- Why do we need it?

Note, as we will see, holding data can be a headache, so perhaps it is better not to hold some data.

# Information Privacy Principles

2. **Collection** –
   - Generally, collect personal information directly from the person it is about.
   - But you can collect it from other people in certain situations.

# Information Privacy Principles

2. **Collection** –

   For instance, if:

   - the person concerned gives you permission;
   - collecting it in another way would not prejudice the person's interests;
   - you are getting it from a publicly available source.

# Questions to ask

- What personal information do we collect?
- How do we collect personal information?
- Do we have consent for our methods of collection?

# Information Privacy Principles

3. **Fair Notice** –

   Take reasonable steps to make sure that the person knows:

   - why it's being collected;
   - who will receive it;
   - whether giving it is compulsory or voluntary;
   - what will happen if information is not given.

# Information Privacy Principles

4. **Manner** –
   - Only collect personal information in ways that are lawful, fair and not unreasonably intrusive.
   - Take particular care when collecting personal information from children and young people.
     - ❖ Unsolicited Electronic Messages Act 2007
     - ❖ PFRA Code of Conduct

# Information Privacy Principles

5. **Storage and Security** –
   - Make sure that there are reasonable security safeguards in place to prevent loss, misuse or disclosure of personal information.
   - This includes limits on employee browsing of other people's information.

# Questions to ask

- How do we store personal information?
- Where do we store personal information?
- What third party vendors do we rely on to store and process personal information?
- What third party vendors do our third party vendors rely on?
- How do we know the personal information is safe and secure?


WARNIEN
CYBER SECURITY
BIEACHI
DETECTED

# Optus Data Breach

Optus suffered a data breach in September 2022, which took advantage of an unprotected and publicly exposed API.

The design of the API was that such that anyone who found the API could connect to it without any requirement to submit a username or password.

# Optus Data Breach

The open Optus API was an open door that gave access to sensitive personal information about Optus customers including:

- Driver' License numbers
- Phone numbers
- Dates of birth
- Home addresses


WARNIEN
CYBER SECURITY
BIEACHI
DETECTED

# Pareto Phone Data Breach

When Pareto Phone suffered a LockBit ransomware attack, a large amount of data was posted on the darknet. Data released included detailed documentation from and concerning charities that had engaged Pareto's services, and including details about their donors. The records that were released stretched back as far as 2007

# Information Privacy Principles

6. **Access**
   - People have a right to ask you for access to their personal information.
   - In most cases you have to promptly give them their information.

# Information Privacy Principles

7. **Correction**
   - A person has a right to ask an organisation or business to correct their information if they think it is wrong.
   - Even if you don't agree that it needs correcting, you must take reasonable steps to attach a statement of correction to the information to show the person's view.

# Information Privacy Principles

8. **Accuracy**

   Before using or disclosing personal information, you must take reasonable steps to check it is accurate, complete, relevant, up to date and not misleading.

# Information Privacy Principles

9. **Duration**

   You must not keep personal information for longer than is necessary

# Questions to ask

- What personal information do we hold?
- How long do we hold personal information before we delete it?
- Do we have regular processes for review and removal of obsolete information?

# Optus Data Breach

After the Optus breach was discovered, Optus were criticized because the leaked data included obsolete data from former clients who had not been clients of Optus for some years.

# Pareto Phone Data Breach

Similarly, Pareto Phone were criticized because leaked data included data dating back to 2007.

# Information Privacy Principles

## 10.Using Personal Information

- You can generally only use personal information for the purpose you collected it.
- You may use it in ways that are directly related to the original purpose, or you may use it another way if the person gives you permission, or in other limited circumstances.

# Questions to ask

- How do we use the personal information we hold?
- Do we have permission to use the personal information in that way?
- How can we demonstrate we have permission to use the personal information in that way?

# Information Privacy Principles

## 11.Disclosure

You may only disclose personal information in limited circumstances. For example, if:

- disclosure is one of the purposes for which you got the information;
- the person concerned authorised the disclosure;
- the information will be used in an anonymous way.

# Questions to ask

- To whom do we disclose personal information we hold?
- Do we have permission to disclose the personal information in that way?
- How can we demonstrate we have permission to disclose the personal information in that way?

# Information Privacy Principles

## 12.Sending Overseas

You can only send personal information to someone overseas if the information will be adequately protected.

# Questions to ask

- Is any personal information that we hold stored with vendors located overseas or otherwise disclosed to overseas persons?
- Do we have permission to hold/disclose the personal information in that way?
- How can we demonstrate we have permission to hold/disclose the personal information in that way?
- Where information is held overseas, does the party holding that information have adequate protection measures in place? How do we know?

# Information Privacy Principles

## 13.Unique Identifiers

- You can only assign your own unique identifier to individuals where it is necessary for operational functions.
- Generally, you may not assign the same identifier as used by another organisation.
- If you assign a unique identifier you must make sure that the risk of misuse (such as identity theft) is minimised.

# Optus Data Breach

The Optus data base used incrementing identifiers for its customers. All customer identifiers differed by an increment of 1. This meant that hackers who accessed the open API were able to write a script that requested every customer record in the database by simply incrementing each unique identifier by one.

# Questions to ask

- Do we or our vendors use database tools that assign unique identifiers to our customers?
- Are these structured in a way that makes it easier for hackers to access large amounts of information.

# QUESTIONS

Parry Field Lawyers

To the heart of what matters.