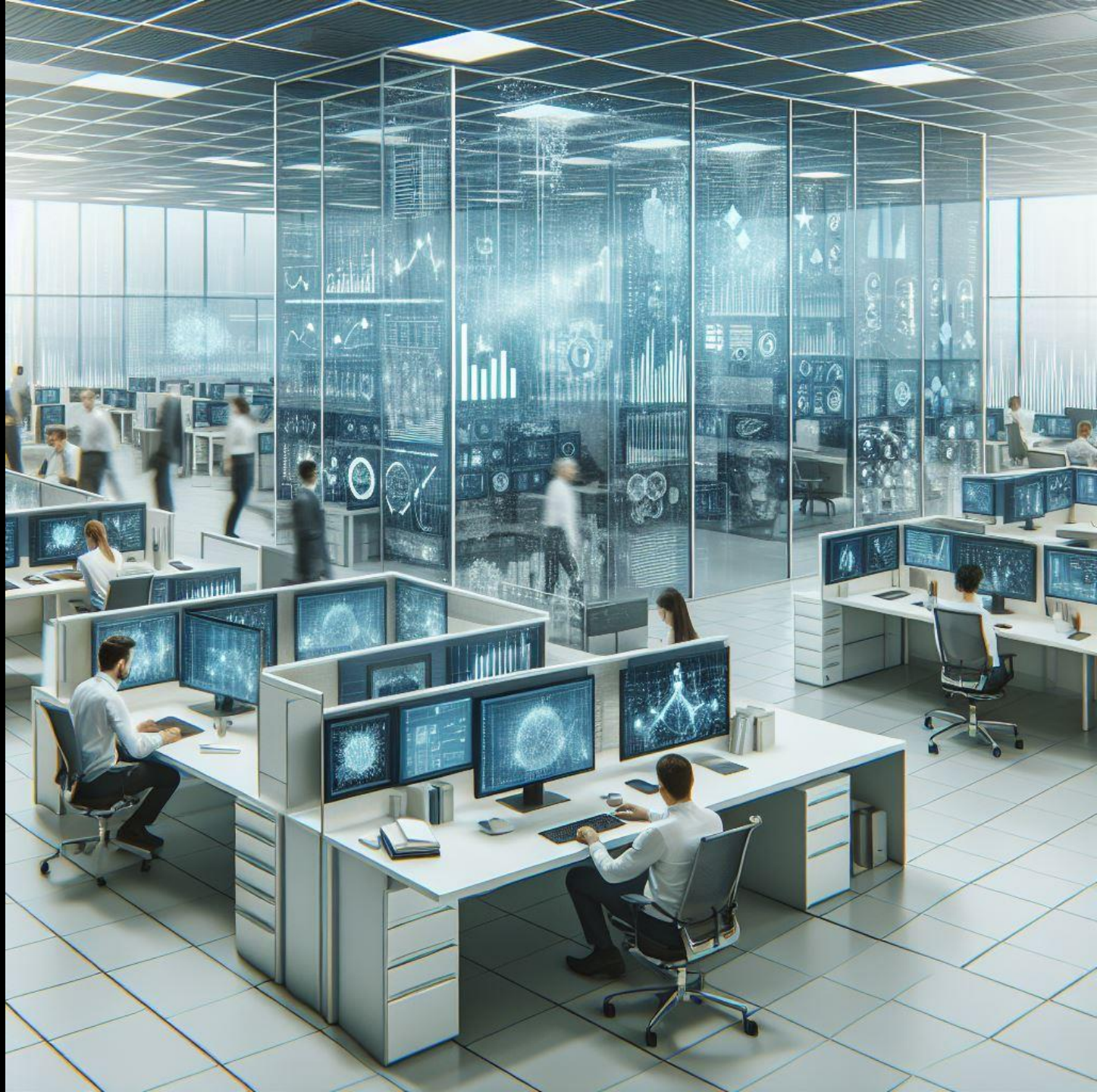




Ethical Data: Navigating Data Rights and Donor Privacy Responsibility





Recent Serious Data Breaches

- Latitude Financial
 - 7.9 million affected customers
 - OAIC and OPC joint investigation - focused on whether Latitude took reasonable steps to protect the personal information they held from misuse, interference, loss, unauthorised access, modification or disclosure.
 - The investigation will also consider whether Latitude took appropriate steps to destroy or de-identify personal information that was no longer required.
- Optus
- Pareto Phone

Relevant Legislation

- Privacy Act 2020
- Human Rights Act 1993

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”

Big Data

- The volume of data that passes through organisations has increased massively.
- Technology advancements make utilising that data more feasible.
- Accuracy
- Awareness – do you know what you hold?
- Security

AI

- Makes it possible to interrogate and utilise your data faster.
- Makes it possible to identify specific individuals from aggregated data even when those individuals are not named.
- Accuracy / Hallucinations
- Bias / Discrimination – Human Rights Act

Data Awareness – What?

You probably collect and hold more personal information than you realise.

Who do we collect personal information about?

- Staff, clients, donors, suppliers ...

Data Awareness – What?

What personal information do we collect?

- Names, contact details, activities, financial position, donation history, payment methods/details, memberships, health, biometrics, date of birth, criminal record checks, employment history

Data Awareness – Why?

- Why do we need it?
- How long do we need it for?

Data Minimisation

- The less data you have, the less data you have to lose.
- Data minimisation is about collecting only what you need, storing it only as long as necessary, and then securely disposing of it. It can drastically reduce your risk footprint.
- Latitude Financial held data dating back as far as 2005. Pareto Phone held data dating back to 2007.

Data Awareness – How?

- Who do we collect personal information from?
- Do we have consent for our methods of collection?

Data Awareness – How?

- How does personal information pass through our organisation?
- How do we look after it?
- What third party vendors do we rely on to collect and hold personal information?
- What third party vendors do our third party vendors rely on?
- What data protection controls do they have in place?



⚠️ WARNIEN ⚠️
CYBER SECURITY
BIEACH
DETECTED

Questions to ask

- How do we use the personal information we do 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?

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?

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”

Operational Data Governance Framework - Stats NZ

- Knowledge:
 - Developing, building and extending your understanding of the data you hold.
 - Mapping how data flows into, through and out of your organisation.
 - Identifying who touches (and what business processes touch) data within your organisation.

Operational Data Governance Framework - Stats NZ

- Care:
 - Develop staff capabilities in best practice data management:
 - Data Point of Contact
 - Subject Matter Expertise
 - Access Control
 - Risk Management
 - Internal Relationship Management
 - External Relationship Management
 - Quality Assurance
 - Data Management
 - Data Champion
 - Data Innovation



1 950 01

27

07

Privacy by Design (Pbd)

“A design methodology that includes privacy as an essential priority of any product, service, system or process.”

Privacy by Design (Pbd)

Seven Principles:

1. Proactive, not reactive, preventative not remedial.
2. Privacy as the default.
3. Privacy embedded into design.
4. Full functionality – positive-sum, not zero-sum.

Privacy by Design (Pbd)

Seven Principles:

5. End-to-end security – lifecycle protection
6. Visibility and transparency
7. Respect for user privacy – keep it user centric.

QUESTIONS

ParryField
Lawyers



To the heart of what matters.

