CYBR 373 Presentation

By Tom, Raashna, Patrick, Mathias

Introduction

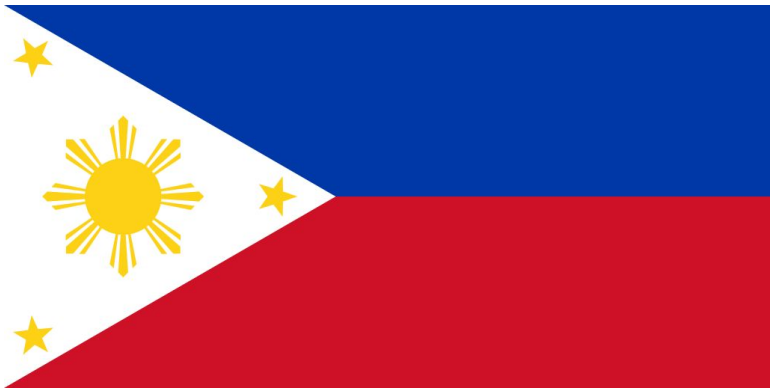
- Our organisation proposes transferring personal information from New Zealand to an overseas cloud provider in the Philippines.
- This presentation will go over the practical, legal and ethical implications of this proposal.

The implications include:

- Relevant New Zealand legislation, specifically the Privacy Act 2020.
  - How it applies here in New Zealand.
  - How it applies if data is transferred overseas.
- Respect and adherence to the Treaty of Waitangi, including Māori data sovereignty.
- Privacy legislation in the Philippines, including the Data Privacy Act of 2012.
- Privacy guidelines/frameworks/laws, including OECD, APEC, DPUP, ISO, GDPR.
- Ethics.
  - Consent to transfer data overseas.
  - Data ownership overseas.

Choice of Philippines

- The Philippines was chosen over Namibia and Argentina.
- We believed that the Philippines had similar laws and conditions to New Zealand, informing our decision.



https://commons.wikimedia.org/wiki/File:Flag_of_the_Philippines.svg

New Zealand Context

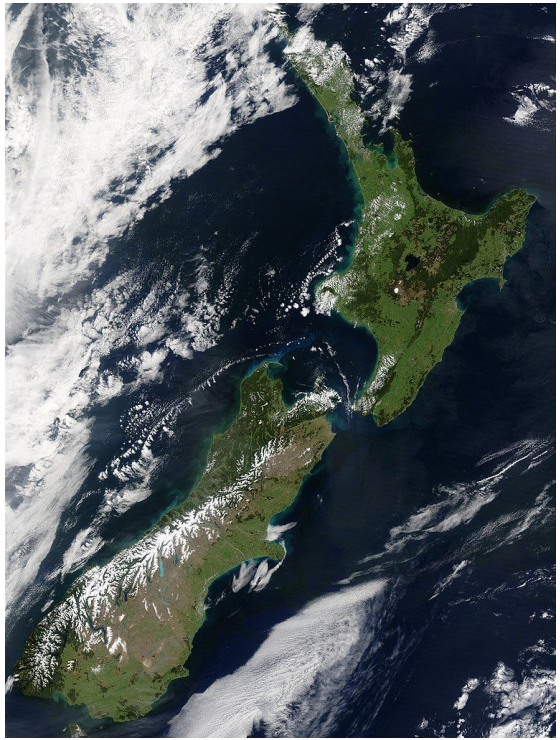


Image Source: https://commons.wikimedia.org/wiki/File:New_Zealand_23_October_2002.jpg

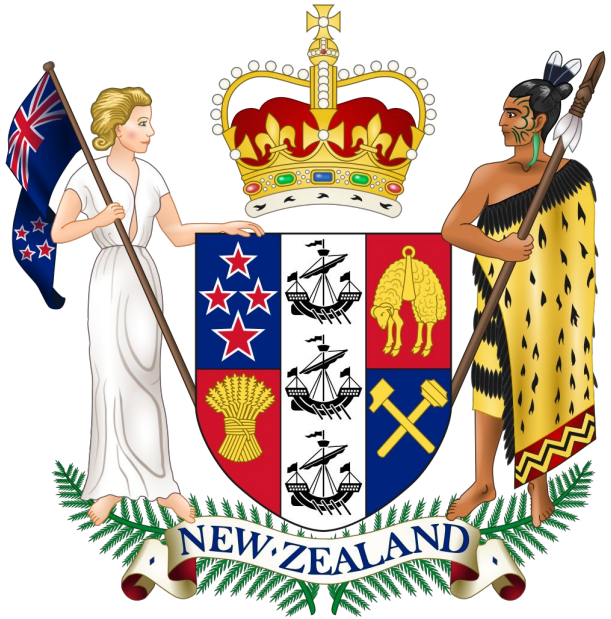
Introduction to first section

This section will outline:

- New Zealand legislation that must be complied with for New Zealand cloud providers
- How New Zealand legislation applies if data is sent to an overseas cloud provider.
- Respect to and commitment to comply with Te Tiriti o Waitangi.

Privacy Act 2020 (New Zealand)

- The primary piece of legislation New Zealand cloud providers must adhere to [1].
- Sections of it will apply if data is to be transferred to a foreign country [2].



Privacy Act 2020 (New Zealand) Overview

- The act has 13 principles [1].
- Some of the requirements in the principles include:
  - Only necessary personal information should be collected for lawful purposes [3].
  - Only collect information from the person it is about [4].
  - Must inform the person why information is collected [5].
  - Safeguards must be put in place to protect the information [6].
  - People can ask to view [7] or correct [8] their information.
  - Before an organisation uses data, reasonable steps must be taken to ensure information is accurate and not misleading [9].
  - Specific requirements for disclosing data overseas [2].

Privacy Act 2020 when transferring data overseas

- Information Privacy Principle 12 is concerned with sending data overseas [2].
- We determined that transferring data to a foreign cloud service was not covered under principle 12, based on a decision tree tool, unless the cloud service was to use the data for their own purposes [10].

Te Tiriti o Waitangi and Maori Data Sovereignty

- Respect and adherence to Te Tiriti o Waitangi (The Treaty of Waitangi) is important.
- Data is a taonga (treasure) [11].
- Māori must have input and leadership in data decisions [12].
- If Māori do not have control over their data, it is hard for that data to bring benefits [12].
- Māori data sovereignty is also concerned with how government legislation affects the storage and use of Māori data [12].

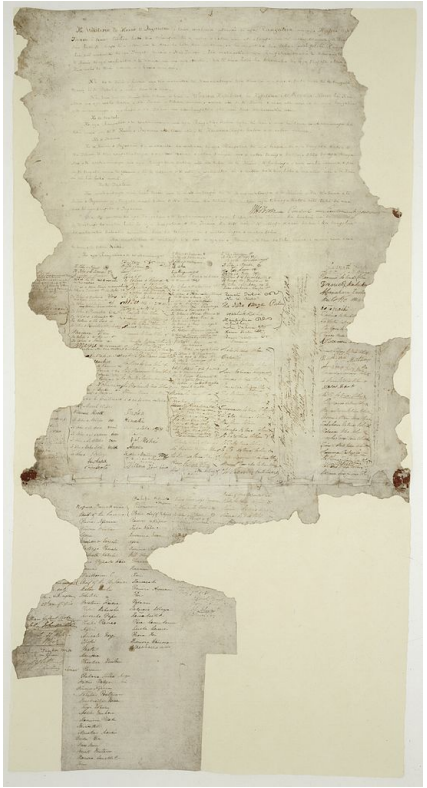


Image Source: https://en.wikipedia.org/wiki/File:Treatyofwaitangi.jpg

Laws and regulations to consider for New Zealand, Philippines, and internationally

New Zealand Privacy Act 2020

- As stated before [13]
- Precautions in place so that foreign company adheres to this Act adequately
- Must notify Privacy Commissioner of data breaches, and those whose information has been breached
- $10,000 for failure to disclose and failure to comply with order

Is PH law similar?

Data Privacy Act of 2012 (PH)

[14] Personal Information: immediate identification, or identification in conjunction with other information

Sensitive personal information:

- Race, ethnic origin, marital status, age, colour, and religious, philosophical or political affiliations
- Health, education, sexual information, criminal offences committed or alleged, and details of law proceedings
- Government-issued information, such as social security number, health records, licences issued and denied, tax returns, etc.
- Information classified by the Filipino government.

(NZ personal information: information about an identifiable individual; sensitive personal information determined at time of data breach)

Data Privacy Act of 2012 (PH)

Processing

- Explicit purpose
- Fairly and lawfully
- Obtained only with consent
- Accurate, relevant to the purpose ONLY, and kept up to date
- Retained only for as long as necessary for the purpose

Sensitive personal information is **illegal** to process **without** explicit consent of the person that the information is being collected on.

Data Privacy Act of 2012 (PH)

Storage

- “Organisational, physical and technical measures” to avoid unlawful or accidental disclosure, alteration or destruction.
  - Computer network
  - Security policies
  - Regular monitoring
  - Incident response
- Third-party compliance
- Entitlement to copy of data if requested

Data Privacy Act of 2012 (PH)

Transfer

- Sensitive personal information is illegal without consent
- Necessity to comply with law as a third-party

Data Privacy Act of 2012 (PH)

Data breaches

- Report to National Privacy Commission
  - Nature of breach
  - Any sensitive personal information involved
  - Measures taken to address breach
- Imprisonment and fines for personal and sensitive personal information breaches
  - Unauthorised processing (purposes, consent)
  - Access due to negligence
  - Improper disposal
  - Concealment of security breaches involving sensitive personal information
  - Unauthorised disclosure

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

- Must follow as part of OECD [15]
- Consent, limited collection, lawful
- Purpose, relevance, accuracy
- Security to prevent loss, unauthorised access, usage, destruction and modification
- User access to copies, reasons for denial, and challenge
- Disclosure and transfer only with consent of subject and according to law

https://commons.wikimedia.org/wiki/File:OECD_logo.svg

APEC Privacy Framework

- NZ and PH part of APEC [16]
- Non-mandatory
- 9 Principles

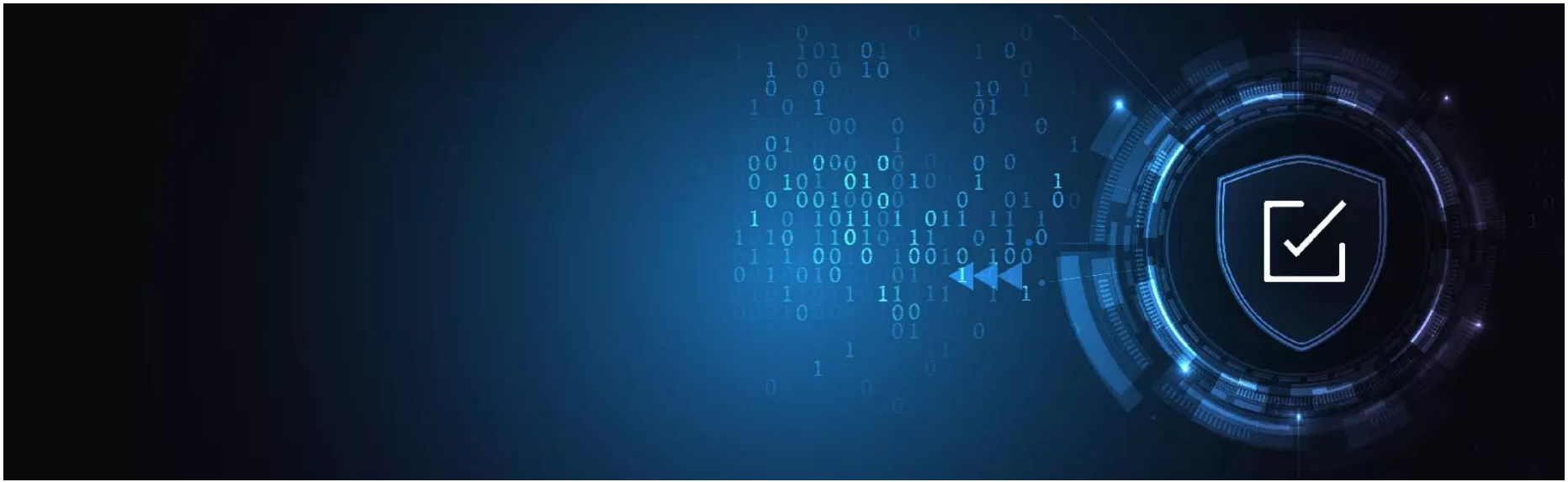
1. Preventing harm
2. Notice
3. Collection limitation
4. Use of personal information
5. Choice
6. Integrity of Personal Information
7. Security safeguards
8. Access and Correction
9. Accountability

https://www.apec.org/about-us/about-apec/apec-logo-use

Data Protection and Use Policy (DPUP) (NZ)

- Non-mandatory but encouraged, endorsed by Cabinet [17]
- 5 Principles
  - He Tāngata
  - Manaakitanga
  - Mana Whakahaere
  - Kaitiakitanga
  - Mahitahitanga
- 4 Guidelines
  - Purpose matters
  - Transparency and Choice
  - Access to information
  - Sharing value

Standards, Frameworks, Guidelines, Certifications



Country Selection and Alignment with International Standards

Why alignment matters?

- Ensures consistent data security and privacy practices across borders.
- Protects sensitive customer information, regardless of where data is processed or stored.

Key benefits of Alignment with Global Standards?

- Mitigate risks (e.g. data breaches, cyber-attacks).
- Meets New Zealand's obligations and supports safe cross-border data transfers.
- Reduces operational risks and ensures business continuity without compromising data integrity.

Compliance with Privacy and Data Standards

New Zealand Privacy Act 2020 [18]

- Ensures strict privacy requirements for handling personal data.

Data Sovereignty Obligations

- Offshore storage in the Philippines must align with NZ Privacy Standards.
- Protects sensitive data regardless of storage location.

Maintaining Data Integrity and Availability

- Cloud providers must comply with both local regulations and global frameworks.
- Examples: ISO Standards [19] and GDPR [20] principles to support privacy and security.

What is GDPR?

- Is a EU Data Protection Regulation that aims to protect personal data.
- Is implemented in the Philippines for enhanced data privacy.
- Benefits to Philippines Organizations:
  - Improved transactions with EU businesses [21].
  - Enhanced data privacy and transparency measures.
- Global Influence:
  - Has driven countries, including the Philippines, to enhance their data privacy regulations [21].
  - Regarded as a significant change in data privacy regulation in 20 years [21].

https://www.loginradius.com/compliance-list/gdpr-compliant/

GDPR: Relevance to New Zealand

- Applicability of GDPR
  - It does not apply within New Zealand but is relevant for international data transfers [22].
- Compliance Obligations
  - New Zealand agencies likely to align with GDPR obligations via the New Zealand Privacy Act [23].
  - Ensures consistent privacy standards for both domestic and international data handling.
- Building Trust and Security:
  - Enhances trust and security for organizations managing data across borders.

https://www.loginradius.com/compliance-list/gdpr-compliant/

GDPR: Selecting Cloud Providers and Ensuring Compliance

- Importance of GDPR Alignment
  - Selecting cloud providers in the Philippines that align with GDPR principles demonstrates commitment to best practices.
- Assurance of Data Protection:
  - GDPR-aligned providers reassure high international standards for data protection.
- Significance of Compliance:
  - Philippines adoption of GDPR principles highlights global recognition of data privacy standards [24].
  - Maintains data integrity and supports safe cross-border data transfers, critical for organizations storing or processing New Zealand data abroad.

https://www.loginradius.com/compliance-list/gdpr-compliant/

Importance of ISO/IEC Standards

ISO/IEC frameworks offer internationally recognized guidelines for cloud providers [25]. Benefits of ISO/IEC implementation in cloud services include:

- Risk Management
- Protection of Sensitive Information
- Compliance

https://www.china-gauges.com/news/What-are-the-main-differences-between-ISO-standards-and-IEC-standards.html

ISO/IEC 27001 - Information Security Management

Focuses on establishing, implementing, and continuously improving an Information Security Management System (ISMS) [26].

Key Objectives [26]

- Data Confidentiality
- Data Integrity
- Data Availability

Benefits of Compliance [26]

- Risk Reduction
- Client Assurance
- Regulatory Compliance

https://zenphi.com/security/iso-iec-27001-compliance/

ISO/IEC 27017 - Security Controls for Cloud Services

27017 standard that provides cloud-specific security controls building on ISO 27001 [27].

What it Provides [27]

- Guidance for mitigating risks.
- Enhanced data security controls in cloud infrastructure.
- Clear guidance on shared responsibility.
- Protection against unauthorized access and data leakage.

https://www.exoscale.com/compliance/iso27017/

ISO/IEC 27018 - Protection of Personally Identifiable Information in the Cloud

27018 standard focuses on the privacy and security of personally identifiable information (PII) in cloud environments [27]

What it Provides [27]

- Measures to protect personal data in compliance with privacy laws and regulations.
- Strengthens customer trust by ensuring data privacy.
- Demonstrates the cloud provider's ability to handle personal data securely.
- Helps align with privacy regulations such as GDPR, New Zealand's Privacy Act and the Philippines Privacy Act.

https://www.akamai.com/legal/compliance#iso27018

ISO/IEC 27701 - Privacy Information Management System (PIMS)

27701 framework builds upon ISO/IEC 27001 and 27018 to focus on privacy management and regulatory compliance [28].

What it provides [28]

- Controls to manage data risks
- Compliance with privacy laws
- Structured approach to managing privacy risks
- Outputs for demonstrating compliance with privacy regulations
- Accountability

https://principledefence.com/product/iso-iec-27701-privacy-information-management-system

SOC - Service Organization Control

SOC is a certification that provides internationally recognized auditing guidelines for assessing controls, processes, and systems of service organizations, including cloud providers.

Provides assurance to clients, vendors, and regulators that a provider operates securely and complies with relevant standards.

https://envoy.com/workplace-compliance-security-safety/visitor-management-and-soc-2-compliance-what-you-need-to-know

SOC 2 Certification

SOC 2 covers security, availability, integrity, confidentiality and privacy of cloud providers [29].

Key Benefits of SOC 2 Certification [29]

- Demonstrates trustworthiness to customers, vendors, and stakeholders [30].
- Ensures secure handling of data throughout the service lifecycle.
- Supports regulatory compliance by maintaining high levels of data integrity and security [30].

https://envoy.com/workplace-compliance-security-safety/visitor-management-and-soc-2-compliance-what-you-need-to-know

CSA STAR Assessment

CSA STAR -> Security, Trust, Assurance and Risk[31]. Certification Builds on ISO/IEC 27001 but focuses on cloud specific risks [32].

Level 1: Self-Assessment [32]

- Provider conducts a self-assessment to provide insight into their cloud security policies.

Level 2: Third-Party Audit [32]

- A third-party audit verifies compliance with ISO standards and cloud-specific security controls from the Cloud Controls Matrix (CCM).

Key Benefits:

- Trust that data is securely managed in compliance with global security standards.
- Reduces risks associated with cloud storage.
- Ensures alignment with New Zealand's privacy requirements and enhances confidence in cross-border data management.

https://www.cloudcarib.com/2023/01/13/cloud-carib-earns-csa-star-certification-one-of-six-companies-globally/

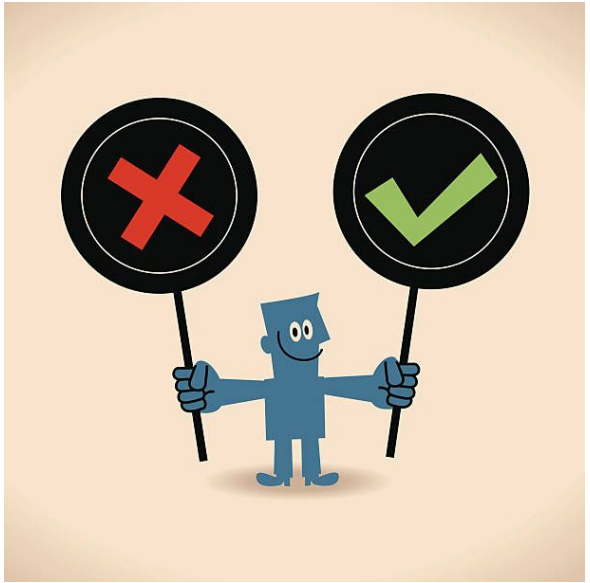
Ethical considerations and responses

Ethics of not having consent to transferring data offshore

- Our customers have a right to know where their data is, and where it moves to whenever there is a change.
- If we do not inform our customers on where the data is relocated to, this takes away their ethical right to make informed decisions with their data.
- This may cause problems for our organisation. We may lose trust and may lose revenue

Response to having no consent of transferring data offshore

- Follow the OECD guideline for transferal of data offshore that states “It should not be disclosed without consent of the subject”.[15]
- Follow Data Protection Use Policy (DPUP) principle of Manaakitanga which is showing people respect on which data is collected.[16]
- Ask our customers consent to transfer the data offshore, this shows Manaakitanga to them
- If they say yes, we continue. Otherwise store their data in a local database in New Zealand
- Stay transparent with our customers



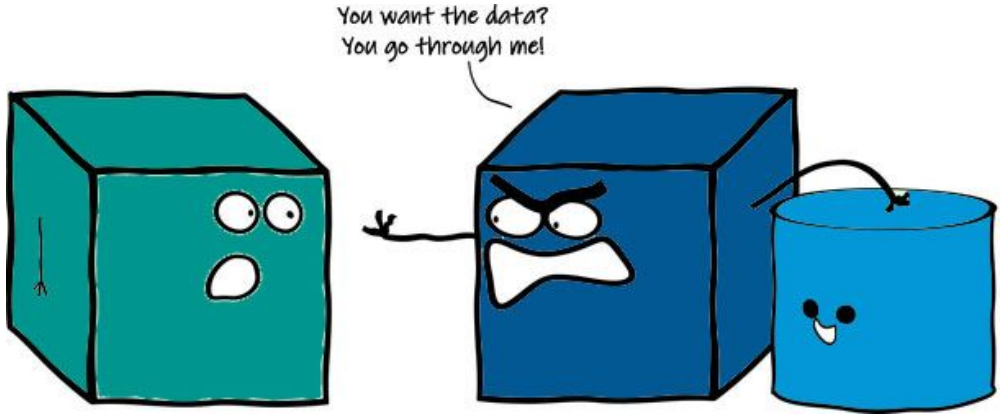
https://www.istockphoto.com/photos/asking-permission

Ethics of data ownership within the cloud

- Terms and services can mean the cloud provider becomes the owner
- Customers should always be the owner of their data
- If the cloud provider runs algorithms and manipulates data
- Question: Who owns this newly manipulated data?
- Accessibility, modification and what happens with their data most likely will be revoked

Response to data ownership in the cloud

- Follow the Data Protection Use Policy principles of Mana Whakahaere and Kaitiakitanga.[16]
- Create a Data Processing Agreement (DPA) that states these main points:
  - What type of data is it?
  - How to process the data?
  - Security measures?
  - Confidentiality
  - Liabilities to be taken
  - Termination of the DPA
- Have backups



https://www.mcg.com/blog/2020/03/31/data-ownership-reading-writing/

Conclusion

Decision:

- Based on our research, we believe it is safe and appropriate to transfer personal information to a Filipino cloud provider in February 2025.
- This is based on legal, ethical and other aspects researched.
- Filipino data privacy laws are similar to New Zealand, helping to guarantee safety of the data.
- It is legal in New Zealand to transfer data to an overseas cloud provider.
- International and local standards and frameworks …
- We have assessed it is ethical to transfer the data to an overseas cloud provider.
- We believe we should notify customers that their data is being outsourced to a different country, even though it is not required under New Zealand law for our particular circumstances.

References (Part 1)

[1] https://www.privacy.org.nz/privacy-act-2020/privacy-principles/ Accessed 17 Oct 2024
[2] https://www.privacy.org.nz/responsibilities/your-obligations/disclosing-personal-information-outside-new-zealand/ Accessed 11 Oct 2024
[3] https://www.privacy.org.nz/privacy-act-2020/privacy-principles/1/ Accessed 17 Oct 2024
[4] https://www.privacy.org.nz/privacy-act-2020/privacy-principles/2/ Accessed 17 Oct 2024
[5] https://www.privacy.org.nz/privacy-act-2020/privacy-principles/3/ Accessed 17 Oct 2024
[6] https://www.privacy.org.nz/privacy-act-2020/privacy-principles/5/ Accessed 17 Oct 2024
[7] https://www.privacy.org.nz/privacy-act-2020/privacy-principles/6/ Accessed 17 Oct 2024
[8] https://www.privacy.org.nz/privacy-act-2020/privacy-principles/7/ Accessed 17 Oct 2024
[9] https://www.privacy.org.nz/privacy-act-2020/privacy-principles/8/ Accessed 17 Oct 2024
[10] https://www.privacy.org.nz/responsibilities/your-obligations/disclosing-personal-information-outside-new-zealand/decision-tree-page/ Accessed 11 Oct 2024
[11] https://www.temanararaunga.maori.nz/ Accessed 11 Oct 2024
[12] https://www.temanararaunga.maori.nz/patai Accessed 11 Oct 2024

References (Part 2)

[13] https://www.legislation.govt.nz/act/public/2020/0031/latest/whole.html#LMS23223
[14] https://privacy.gov.ph/data-privacy-act/
[15]https://www.oecd-ilibrary.org/docserver/9789264196391-en.pdf?expires=1728291169&id=id&accname=guest&checksum=8423CC71499C6311BE069F26BABEF7D5
[16]https://www.apec.org/docs/default-source/publications/2005/12/apec-privacy-framework/05_ecsg_privacyframewk.pdf?sfvrsn=d3de361d_1
[17]https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/data-protection-and-use-policy-dpup

REFERENCES (Part 3)

[18] https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html

[19] https://www.iso.org/standard/27001

[20] https://gdpr.eu

[21] https://www.dti.gov.ph/negosyo/exports/emb-news/gdpr-in-philippines-to-boost-business-dealings-with-eu/

[22] https://www.data.govt.nz/toolkit/privacy-and-security/data-privacy#:~:text=The%20GDPR%20does%20not%20apply,with%20citizens%20of%20the%20EU

[23] https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/public-sector-responsibility/general-data-protection-regulation-gdpr

[24] https://iapp.org/news/a/gdpr-matchup-the-philippines-data-privacy-act-and-its-implementing-rules-and-regulations

[25] https://telarc.org/services/information-security-iso-27001

[26] https://cybercx.co.nz/resource/ten-things-you-should-know-about-iso-iec-27001/

[27] https://www.workstreet.com/blog/iso-27001-27017-and-27018-understanding-the-differences-and-who-needs-themtra#:~:text=ISO%2027017%20builds%20upon%20ISO,providers%20and%20cloud%20service%20customers

[28] https://www.symmetrycompliance.ie/data-protection-services/iso-27701-certification/

[29] https://www.onelogin.com/learn/what-is-soc-2

[30] https://www.truvantis.com/soc-2-certification#:~:text=Empower%20Your%20Sales%20with%20the%20SOC%202%20Certification&text=SOC%202%20(System%20and%20Organization,that%20store%20customer%20data%20online

[31] https://cloudsecurityalliance.org/blog/2023/11/03/csa-star-certifications-what-are-they

[32] https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-csa-star-certification

References (Part 4)

[33]https://link.springer.com/chapter/10.1007/978-3-030-54660-1_6

[34]https://www.blancco.com/resources/blog-philippines-data-privacy-law-what-businesses-must-know-to-comply/

[35]https://teckpath.com/making-the-transition-a-guide-to-switching-it-service-providers-ethically-and-effectively/

[36]https://www.issa.org/issa-code-of-ethics/