Allens

In alliance with Linklaters

Data Protection and Data Privacy

Kenneth Imako

14 November 2024

Data Privacy

The proper handling, processing, storage, and usage of personal information.

Data Protection

Implementing measures to safeguard this information from unauthorized access and breaches.

Challenges

Regulatory Challenges

The absence of a comprehensive legal framework.

Difficult for companies to establish standardized data privacy policies and procedures.

Technological Challenges

Underdeveloped technological infrastructure impedes the adoption of advanced data protection measures.

Companies may lack the necessary resources to invest in cybersecurity technologies.

Awareness and Training

General lack of awareness and training on data privacy issues among corporate entities in PNG.

Lack of prioritization of data protection, often due to a lack of understanding of its importance and the potential consequences of data breaches.

Opportunities

Regulatory Development

Opportunity for the development of a comprehensive data protection framework that aligns with international standards.

Provide clear guidelines for corporate entities and enhance data privacy and protection across the country.

Technological Advancements

Investing in technological infrastructure and cybersecurity can significantly improve data protection capabilities.

Developing partnerships with international technology providers and investing in local IT training can help bridge the technological gap.

Education and Awareness

Raising awareness about the importance of data privacy and protection is crucial.

Corporate entities investing in training programs to educate employees about data protection best practices.

Government and industry collaborations can also play a vital role in promoting data privacy awareness.

Government Perspective

Policy and Legislation

The Legislative and Policy landscape

MEDIUM TERM DEVELOPMENT PLAN IV 2023-2027

NATIONAL CYBERSECURITY POLICY 2021

PNG DIGITAL GOVERNMENT PLAN 2023 – 2027

DATA GOVERNANCE & DATA PROTECTION POLICY [v.5]

Digital Government Act 2022

Evidence Act 1975

Cybercrime Code Act 2016

Criminal Code Act

MEDIUM TERM DEVELOPMENT PLAN IV 2023-2027

- **Enforcement of Cyber Security, Digital Government, and Data Protection Standards in Government Agencies:**
  - This strategy aims to ensure that government agencies adhere to established standards for cyber security and data protection.

- **Protection of Critical Infrastructure for Cyber Security Development:**
  - This strategy focuses on safeguarding essential infrastructure to support the development of cyber security measures.

NATIONAL CYBERSECURITY POLICY 2021

- Protection of National Security
- Economic Growth and Productivity
- Critical Infrastructure Protection
- Public and Private Sector Security:
- International Standards Compliance
- Digital Transformation
- Awareness and Education
- Legal and Regulatory Framework:

NATIONAL CYBERSECURITY POLICY 2021

The policy emphasizes the importance of data privacy and data protection in several areas:

- **Guiding Principles**:
  - One of the guiding principles is to build a strong cyber security environment that safeguards the privacy of citizens as enshrined in the National Constitution.
- **Legislation and Regulations**:
  - The policy highlights the need to develop appropriate legislative and regulatory frameworks to protect society against cybercrime, including the protection of citizens' rights and data.
- **Digital Government Legislation**:
  - This legislation will facilitate and compel cyber security standards and compliance for all public and statutory bodies, ensuring the highest level of security for government systems, information, and data. It will also centralize and streamline the procurement and usage of ICT products and services and facilitate the centralization and sharing of government data and information.
- **National Cyber Security Legislation**:
  - This legislation will include provisions to protect personal data and ensure compliance with international standards and best practices. It aims to harmonize with existing national laws and provide a coordination framework to protect digital services, essential services, e-identification, trust services, and personal data.

PNG DIGITAL GOVERNMENT PLAN 2023 – 2027

- The Digital Government Plan 2023-2027 emphasizes the importance of data privacy and protection.
- It includes the development of a Data Governance Policy and a Data Protection and Privacy policy as part of its strategic initiatives.
- These policies aim to ensure secure data generation, collection, processing, storage, use, and re-use, as well as secure access and sharing based on ownership, need, role, and authority.
- The plan also highlights the need for a secure identification mechanism and the establishment of standards and guidelines to support these efforts.

The (*DATA GOVERNANCE & DATA PROTECTION)* Policy draft is designed to provide a framework for the responsible use, management, and governance of data across public and private sectors. It aims to mitigate the risks associated with increased data usage, such as data breaches and misuse, which can have significant consequences for individuals and society.

DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

DATA GOVERNANCE & DATA PROTECTION POLICY [v.5]

- **Develop and Implement Comprehensive Data Privacy, Protection, and Governance Laws:**
  - To safeguard all types of data, including personal, public, and business data, from unauthorized access, disclosure, or misuse.
- **Educate and Raise Awareness:**
  - To inform government entities, citizens, and businesses about best practices for managing and protecting all types of data, including sensitive information.
- **Establish and Enforce Data Sharing Policies and Mechanisms:**
  - To protect the privacy and security of all citizens and businesses, especially when sharing sensitive information.
- **Create a Data Protection Authority:**
  - To oversee and enforce data management, protection, and privacy regulations, investigate complaints and breaches, and ensure compliance with applicable laws and regulations.
- **Foster International Collaboration:**
  - To exchange best practices and lessons learned on data governance and protection and stay aligned with global standards.

Criminal Code Act

- The *Criminal Code Act* includes offences relating to breaches of privacy.
- Section 191 addresses the violation of secrecy by individuals employed by an ICT licensee.

> **A person who publishes or communicates the contents or substance of a communication sent by an ICT service, other than to a person to whom they are authorized to deliver the communication, is guilty of an offence.**

The penalty for this offence is a fine not exceeding K200.00 or imprisonment for a term not exceeding six months.

Evidence Act 1975

- **Admissibility of Computerized Information (Section 65):**
  - Statements contained in documents produced by a computer are admissible as evidence if it is shown that the document was produced during a period when the computer was regularly used to store or process information for regular activities, and the computer was operating properly during that period.
- **Proof of Computer Statements (Section 66):**
  - Statements in documents produced by a computer can be proved by producing the document or a copy authenticated in a manner approved by the court. A certificate signed by a responsible person regarding the production of the document or the operation of the computer can serve as evidence.
- **Weight to be Attached to Computer Statements (Section 67):**
  - The weight given to computer statements as evidence depends on the circumstances of their creation, including the accuracy of the information supplied to the computer and any potential incentives to misrepresent the facts.

Digital Government Act 2022

The *Digital Government Act* 2022 addresses data protection and data privacy through several provisions:

- **Classifications of Electronic Data (Section 45)**:
  - Electronic data is classified as top-secret data, confidential data, or open data, with specific security controls prescribed for each classification to safeguard against unauthorized use, disclosure, modification, or destruction.
- **Reproduction, etc., of Electronic Data (Section 46)**:
  - Unauthorized access, use, reproduction, or dissemination of top-secret or confidential data is prohibited and penalized.
- **Public Access to Electronic Data (Section 47)**:
  - Access to electronic data stored by a public body requires permission from the public body and, in the case of personal data, written consent from the individual whose data is being accessed.
- **Electronic Data Collection and Storage (Section 48)**:
  - Public bodies must collect and store data in electronic form and ensure compliance with regulations and standards for data collection and storage.
- **Ownership of Electronic Data in Central Electronic Data Repository (Section 49)**:
  - Electronic data stored as backup in the Central Electronic Data Repository is the property of the State, and public bodies must ensure data is backed up in the repository.
- **Electronic Data Sharing (Section 52)**:
  - Public bodies must comply with standards and specifications for secure data sharing to prevent data privacy violations and hacking.
- **Access to Central Electronic Data Repository (Section 29)**:
  - Access to the Central Electronic Data Repository is restricted and requires permission from the public body storing the data, and additional consent for personal data.

Cybercrime Code Act 2016

Data privacy is discussed in the *Cybercrime Code Act* 2016.

Specifically, it addresses:

- unauthorized access or hacking (Section 6),
- illegal interception (Section 7)
- data interference (Section 8), and
- unlawful disclosure (Section 25).

These provisions outline penalties for actions that compromise data privacy, such as unauthorized access to electronic systems or data, interception of non-public transmissions, and disclosure of confidential or classified communications.

Private Sector perspective

Legislative protection, remedies and exposure.

Legal action and remedies for data breaches

Corporate entities have several legal remedies available to address data breaches caused by internal and external actors. Here are some key options:

Against Internal Actors (e.g., Employees)

Disciplinary Action:
Companies can take disciplinary measures against employees who cause data breaches, ranging from warnings to termination, depending on the severity of the breach.

Legal Action:
If the breach involves criminal activity (e.g., theft of data), the company can pursue legal action against the employee, including criminal charges.

Civil Lawsuits:
Companies can file civil lawsuits for damages if the breach results in financial loss or reputational damage.

Against External Actors (e.g., Hackers)

Criminal Prosecution:
Companies can report data breaches to law enforcement agencies, which can investigate and prosecute the perpetrators under relevant criminal laws.

Civil Litigation:
Companies can sue external actors for damages if the breach results in financial loss, reputational damage, or other harm.

Regulatory Penalties:
Regulatory bodies can impose fines and penalties on companies responsible for data breaches, especially if they fail to comply with data protection regulations.

General Remedies

Compensation:
Companies can seek compensation for losses incurred due to the breach, including costs related to data recovery, notification, and remediation.

Injunctions:
Companies can seek court orders to prevent further breaches or to compel the return of stolen data.

Insurance Claims:
Companies with cyber insurance can file claims to cover the costs associated with data breaches, including legal fees, notification costs, and damages.

Claims for breaches of Privacy

Invasion of Privacy

This tort involves an unauthorized intrusion into someone's private life, which causes distress or harm. While not fully established in all jurisdictions, courts have recognized this tort in some cases.

Breach of Confidence

This claim arises when confidential information is disclosed without permission, leading to harm. It's often used in cases where sensitive personal data is mishandled.

Negligence

If a company fails to take reasonable care to protect personal data, resulting in harm to an individual, a claim of negligence can be made.

Misrepresentation

If a company falsely represents its data protection practices, leading individuals to believe their data is safe when it is not, claims of misrepresentation can be made.

Breach of Contract

If there is a contractual agreement between the individual and the company regarding data protection, and the company fails to uphold its obligations, the individual can claim breach of contract.

Recent Australian legal cases involving breaches of data privacy

1. **HWL Ebsworth Lawyers v Persons Unknown [2024] NSWSC 71**:
    - This landmark case involved a data breach at HWL Ebsworth Lawyers, an Australian law firm. Unknown hackers, claiming to be from the group "ALPHV" (also known as "Blackcat"), stole confidential data, including sensitive client records and government information. The Supreme Court of New South Wales granted injunctive relief to restrain the hackers from using the stolen data
2. **Facebook (Meta) and the Cambridge Analytica Data Breach**:
    - The High Court of Australia is deciding whether Facebook is liable for the breach of personal data of approximately 300,000 Australians. This case stems from the infamous Cambridge Analytica scandal, where data was collected through a Facebook quiz and used for psychological profiling and political messaging.
3. **Medibank and Optus Data Breaches**:
    - Several consumer class actions have been commenced against Medibank and Optus in the Federal Court following significant data breaches. These cases highlight the increasing risk and legal consequences for businesses experiencing data breaches.
4. **Australian Clinical Labs Limited**:
    - The Australian Information Commissioner filed proceedings in the Federal Court against Australian Clinical Labs Limited, seeking a civil penalty for the company's response to a data breach that occurred in February 2022.


Allens