Privacy Framework

TABLE OF CONTENTS

1 PURPOSE AND OBJECTIVES

Telkom SA SOC Limited (hereinafter referred to as “Telkom”) has a commitment to their clients, employees, third party contractors and customers to ensure that personal information that Telkom has collected, acquired, processed or stored either by themselves, or through a third party, or on behalf of a third party is treated as confidential and is protected throughout the lifecycle. The purpose of this framework is to provide the guiding principles on what is deemed acceptable and ethical behaviour by any of our employees, contractors, or third parties, when personal information is identified, assessed, monitored, utilised and disposed of.

Mitigation of privacy risks within programs or activities that are involved in the collection, retaining, use, disclosure and disposal of personal information should be considered through its lifecycle. This Privacy Framework will inform the following areas within Telkom: service design and delivery, information management, internal and external controls and monitoring, employee education, privacy risk and compliance management, and privacy breach management.

2 APPLICABILITY AND SCOPE

The principles in this framework apply to Telkom employees, suppliers, contractors or third parties that are in any way involved or privy to personal data. This applies throughout its lifecycle, whilst driving the education of employees for them to clearly understand their responsibilities and the impact of a privacy breach due to their negligence and or ignorance of certain aspects.

3 CONTEXTUAL BACKGROUND

The Protection of Personal Information Act as well as the Payment Card Industry Standard have provided organisations that process personal data in any format with regulatory guidance on the processing thereof and guides on how it may be legally obtained, processed and disposed of. Data in Telkom is classified and treated throughout its lifecycle as per the data classification standard. Personal data that is collected, when properly analysed and enriched can be accurately used within the algorithm systems to assist Telkom in automating certain decisions based on variables without being subject to any unjust biases.

4 FRAMEWORK FOR PRIVACY MANAGEMENT

This framework will leverage from the ethics principles and values as contained within the Ethics handbook, which consists of: Competence, Responsibility, Accountability, Fairness and Transparency. These principles and values shall be applied in all domains where personal information may be identified, assessed, monitored, utilised and disposed of.

5 SERVICE DESIGN AND DELIVERY

The design, development, operation and management of services or products shall follow privacy by design principles, to ensure that we design our technology offerings around the

protection of data. Sensitive assets, such as personal information should be protected by delivering effective and dependable services, which consider the security and safety aspects.

5.1 Competence

Employees should be competent and knowledgeable in understanding what the privacy requirements are, in relation to the type of personal information being designed, and ensure that the security of the service is competent in the identification and protection of information through authentication and identity management.

Telkom should proactively educate service users in order to ensure that they are competent in the usage of the service and in identifying possible fraudulent correspondence or threats related to the service, and how they should report or escalate such suspected threats.

5.2 Responsibility

Each participant in the information management lifecycle should clearly understand the type of information, their duty to protect, as well as the applicable controls that will enable them to protect the data from unauthorised access and or unethical treatment.

5.3 Accountability

Telkom shall ensure that applicable governance exists that will monitor the management of information within service design and delivery and ensure that adequate protection and security within the service design will protect against information being breached or treated unethically. Privacy controls should be assessed, and any risks should be communicated and treated as per the IT Risk Management Framework and associated process.

5.4 Fairness

Personal information should be processed fairly when collected and if utilised within an algorithmic system that no unfair bias exists, that will influence the outcome or decision of an automated process.

5.5 Transparency

Services should be designed to be user centric and transparent from beginning to end. Effective and transparent communication is done to ensure that users are aware of what type of personal information will be collected and how it will be assessed and utilised.

6 INFORMATION MANAGEMENT

In certain instances, Telkom may be required to make available information to third parties or law enforcement agencies in order to facilitate the effective management of a service or to comply with laws and legislation. With information sharing, Telkom should identify applicable risks and ensure appropriate controls are in place to mitigate those risks. When sharing information, the potential impact on the user or owner should be considered.

6.1 Competence

Telkom should ensure that users and customers are competent to authorise the collection, use or sharing of their personal information for algorithm system utilisation as well as to third parties or partners and understand what their information will be utilised for.

6.2 Responsibility

Any party with whom information is shared should understand the responsibility they have towards Telkom's users and customers and towards the protection of the information that has been shared with them. We shall ensure that we know what our responsibilities are with regards to the information we act as custodian of, with regards to sharing of information with legal and regulatory entities as prescribed by legislation.

6.3 Accountability

Telkom as well as any party that we share information with, shall ensure that they have controls in place, in order to ensure that the information will be protected throughout its lifecycle and there are controls in place that can monitor how information is shared and protected, that is aligned to legislation and laws, but also according to the values of Telkom and our responsibility towards our users or other forms of data owners.

6.4 Fairness

We shall protect, use and share information in a manner that is fair to the user and free from any bias or altering. In order to ensure that we treat our users fair, we will provide them with a user-friendly avenue, in which they are able to report or complain on any perceived breach or threat and query our processes that relate to how their personal information is treated, protected, shared and used.

6.5 Transparency

We should always be transparent to users from whom personal information has been collected if the information will be shared with a third party, and the reason why it will be shared. The reasons for sharing information should be if collaboration will enable us to meet our obligations in order to provide a quality service or enhance the quality or availability of a service or product, or when so required due to legislation, or based on a court order.

7 INTERNAL AND EXTERNAL CONTROLS AND MONITORING

Telkom shall ensure that that they have a robust Information Security Management System that is utilised for the protection of information through controls internally and externally.

7.1 Internal Controls

Telkom shall ensure that it has identified Information Systems that collect, transfer, store, process or manage personal information and shall ensure that these systems are integrated with automated solutions that are able to detect, identify and query questionable behaviour or anomalies on these systems and ensure that these events are logged for investigation and security intelligence. We shall ensure that users have minimum access as per the Access Governance Standard and that need-to-know access is granted based on the role and responsibilities of the contractor, employees or third party.

7.2 External Controls

We shall ensure we will protect our entrusted personal information from external threats related to cyber-attacks or phishing that is intended to steal, modify or infect information. Protection of information is achieved through making use of adequate and up to date

firewalls, malware detection, encryption, and intrusion prevention tools and by conducting threat intelligence monitoring to detect and respond to breaches.

7.3 Competence

Telkom shall ensure that controls, systems, and tools used as protection from internal and external threats are competent to withstand any known threats. We shall ensure that employees, contractors, , or any other parties that are involved in the prevention or the management of threats or incidents to information are adequately trained and aware of the newest threats and risks, and how they can be prevented, managed and mitigated.

7.4 Responsibility

Telkom will be responsible for protecting the personal information throughout its lifecycle and pro-actively identify any potential risks and threats to information, and adequately mitigate these threats and risks if and when they are identified.

7.5 Accountability

Telkom shall be responsible for assessing a suspected information breach and if the breach has been verified or confirmed and the information affected determined, shall report the incident to the Information Regulator as per the Protection of Personal Information Act 4 of 2013.

7.6 Fairness and Transparency

In the event that a security incident has taken place which has had an effect that personal information has been stolen or altered in any manner, we shall ensure that any user that may possibly be affected by the breach are made aware of the potential impact and the type of information that has been breached, in order to ensure that additional awareness and security matters can be incorporated by the users.

8 EMPLOYEE EDUCATION

Employees and contractors should at all times act in such a manner that they are a line of defence in the protection of Telkom's information assets, therefore we continuously update our employees and other parties on their role.

8.1 Competence and responsibility

Telkom should perform awareness training and communication to ensure that all parties have an awareness related to their responsibility in not enabling malicious or accidental information theft, loss, or altering due to their behaviour or negligence, whether it is intentional or unintentional. Telkom should also ensure that resources are equipped in performing the roles they are employed for and aware of any regulatory or legal implications if their behaviour, intentional or unintentional, leads to an incident pertaining to information.

9 PRIVACY RISK AND COMPLIANCE MANAGEMENT

Telkom shall at all times ensure that we pro-actively identify and manage risks or threats related to information or privacy compliance and have adequate mitigation controls in place for the prevention of incidents or threats to personal information.

9.1 Responsibility

Telkom is responsible for ensuring the accuracy of information and that the information is only used to fulfil our mandate and in alignment to legislation on the period for which it can be stored. Telkom shall ensure that a retention policy is applied to personal information and deletion of information should take place at adequate intervals to ensure we comply to legislation related to information retention.

9.2 Accountability and Transparency

In an effort to ensure our compliance to privacy requirements, Telkom will ensure that our handling of personal information is regularly validated, either by self-assessment, Internal Audit or continuous monitoring. According to the log and event management standard, we should be able to trace activities of users when accessing information. This is an additional effort to identify a point in time or specific information that may have been accessed with malicious intent and adequately investigate the event.

9.3 Fairness

Telkom shall ensure that data collected for use in Artificial Intelligence for algorithm systems or analytics are managed according to the Digital Ethics Framework, to ensure it is free from any unfair bias, and that controls and protection controls for information is in place. We shall continue to ensure that users are aware of the personal information that we will be collecting and how it will be used, shared and protected and ensure that we have proof of consent and adhere to the usage of information in alignment to the consent provided.

10 PRIVACY BREACH MANAGEMENT

While Telkom adopts a pro-active approach to the protection of information by identification and assessment of potential threats and using mitigating controls therefore, Telkom shall ensure that an effective and appropriate response process has been documented. The process shall ensure that there are effective controls in place to identify, assess and respond to an incident, in order to mitigate and minimise the impact and loss or theft of information.

10.1 Competence and Responsibility

Telkom shall ensure that any resource that has been tasked with a role or responsibility in the management of a perceived, active or mitigated threat or incident has the competence to act in the prescribed role and has been fully informed of their role and responsibility.

11 APPENDIX A: DEFINITIONS, ACRONYMS, REFERENCE DOCUMENTS, LAWS & REGULATIONS

11.1 Definitions

Definitions	Description
Algorithm	The process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer.
Algorithmic Systems	Systems comprised of one or more algorithms used in a software to collect and analyse data as well as draw conclusions as part of a process designed to solve a pre-defined problem.
Ethics	Moral justification for what is morally just, fair and right.
Transparency	To be open and without secrets regarding intent and subsequent processes.

11.2 Acronyms

Acronyms and Abbreviations	Description
IT	Information Technology
POPIA	Protection of Personal Information Act

11.3 Reference Documents

I. Ethics Handbook
II. King IV Report on Corporate Governance
III. Digital Ethics Framework
IV. Disaster Recovery Framework
V. Data Classification Standard
VI. Log and Event Management Standard
VII. Information and Data Management Policy

11.4 Laws and Regulations

I. Protection of Personal Information Act 4 of 2013
II. Cybercrimes Act 29 of 2020