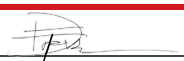
DIGICALL

A18 - Privacy Risk Management Policy

DOCUMENT CLASSIFICATION	Internal Use Only
VERSION	1.3
DATED	01 September 2024
DOCUMENT AUTHOR	Ameet Ranchod
DOCUMENT OWNER	Johan Kriel

Approval

NAME	POSISTION	SIGNATURE	DATE
Donald Fraser	IT Security & Compliance Manager		04/10/2024
Ameet Ranchod	IT Infrastructure Manager		07/10/2024
Johan Kriel	Group CIO		09/10/2024

This policy supersedes and replaces all previous versions of this policy.

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
0.1	24.02.2021	Ameet Ranchod	Document Creation
0.9	17.03.2021	Ameet Ranchod	Final Draft
1.0	17.03.2021	Ameet Ranchod	Version 1.0
1.1	31.05.2022	Celeste Ramnarayan	Version 1.1
1.2	01.07.2023	Donald Fraser	Updated personnel & roles
1.3	01.08.2024	Donald Fraser	2024 Revision, updated template

Table of Contents

1 Policy Scope

This policy applies to all employees and contractors during the performance of company related business and duties.

2 Policy Statement

Issues of privacy are associated with the management of Personally Identifiable Information (PII), which describes much of the data collected by an organization regarding its employees, prospects and customers. Its hallmark is that it can be linked to an identifiable individual, either directly or indirectly. While all PII is to be respected, some elements are considered especially sensitive (i.e., financial information, etc.), warranting special care and therefore, presenting added risk to business.

3 Purpose

In order to service our clients, we need to collect personal data from our clients and /or potential clients and employees. Considering this, the Digicall Group wants to ensure a high level of data protection as privacy is a cornerstone in gaining and maintaining the trust of our clients, employees and suppliers and thus, ensuring the Digicall Group's future business. Protection of personal data requires that appropriate technical and organizational measures are taken to demonstrate a high level of data protection. Additionally, the Digicall Group will monitor, audit and document internal compliance with the data protection policies and applicable statutory data protection requirements.

4 General

"Personal data" is any information which may be related to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, location data, phone number, age, gender, an employee, a job applicant, clients, suppliers and other business partners. This also includes special categories of personal data (sensitive personal data) and confidential information such as account number, identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Although information regarding companies/businesses is not as such personal data, please note that information relating to contacts within such companies/businesses, e.g., name, title, work email, work phone number, etc. is considered personal data.

The Digicall Group uses personal data for a variety of legitimate business purposes, including establishment and management of customer and supplier relationships, completion of purchase agreements, recruitment and management of all aspects of terms and conditions of

employment, communication, fulfilment of legal obligations or requirements, performance of contracts, providing services to clients, etc.

Personal data shall always be:

a. Processed lawfully, fairly and in a transparent manner in relation to the data subject.
b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
d. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
e. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
f. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Processing of personal data requires a legal basis. The most predominant legal basis for processing personal data within The Digicall Group are:

a. Consent from the data subject(s) for one or more specific purposes.
b. The performance of a contract to which the data subject is party.
c. A legal obligation or requirement.
d. Legitimate interests pursued by The Digicall Group.

4.1 Consent

If the collection, registration and further processing of personal data on clients, suppliers, other business relations and employees are based on such a person's consent to the processing of personal data for one or more specific purposes. Consent shall be: freely given, specific, informed and unambiguous.

The data subject must actively consent to the processing of personal data by a statement or by a clear affirmative action.

A request for consent shall be presented in a manner, which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language.

To process special categories of personal data (sensitive personal data) the consent shall also be explicit.

The data subject is entitled to withdraw his/her consent at any time and upon such withdrawal, we will stop collecting and/or processing personal data about that person unless we are obligated or entitled to do so based on another legal basis.

4.2 The Digicall Group as Data Processor

Digicall as a data processor company, processes personal data on behalf of our clients and in accordance with client's instructions.

When the Digicall Group outsources the processing of personal data to third party data processors, The Digicall Group ensures that said companies, as a minimum, applies the same degree of data protection as The Digicall Group itself. If this cannot be guaranteed, by the said companies, The Digicall Group will choose another data processor.

4.3 Data processing agreements

Prior to transfer of personal data to a third-party data processor, The Digicall Group shall enter into a written data processing agreement with the data processor. The data processing agreement ensures that The Digicall Group controls the processing of personal data, which takes place outside The Digicall Group for which The Digicall Group is responsible.

4.4 Disclosure of personal data

Before disclosing personal data to others, it is the responsibility of The Digicall Group to consider whether the recipient is employed by us or not. Furthermore, we may only share personal data within The Digicall Group if the disclosure is based on a legitimate business purpose.

It is The Digicall Group's responsibility to ensure that the recipient has a legitimate purpose for receiving the personal data and to ensure that the sharing of personal data is restricted and kept to a minimum.

The Digicall Group must show caution before sharing personal data with persons, data subjects or entities outside of The Digicall Group. Personal data shall only be disclosed to third parties acting as individual data controllers if a legitimate purpose for such transfer exists.

4.5 Data Protection by Design

All new products, services, technical solutions, etc. in the Digicall Group must be designed so they meet the principles of data protection by design by default settings.

4.6 Data Protection by Default

Data protection by default requires that relevant data minimization techniques are implemented.

The Digicall Group shall implement appropriate technical and organizational measures ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed.

This minimization requirement applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

Such measures shall ensure that by default, personal data is not made accessible without careful consideration.

4.7 Deletion of personal data

Personal data shall be deleted when the Digicall Group no longer has a legitimate purpose for the continuous processing or storage of the personal data, or when it is no longer required to store the personal data in accordance with applicable legal requirements.

Detailed retention periods with respect to various categories of personal data are specified in the Digicall Group's Data Retention policy.

In compliance with privacy regulation, the Digicall Group's clients/potential clients have the right to request personal information relating to their account with the Digicall Group be deleted or anonymized when their client relationship with the Digicall Group has ended.

The Digicall Group will balance the privacy rights of its clients/potential clients with other requirements of applicable regulations taking precedence over the deletion requirement. The registration of personal data in the Digicall Group's systems is regulated by a wide range of various legal requirements.

Personal data will be deleted or anonymized when there is no longer any legal basis for keeping it. The typical deletion deadline for clients is current year plus 5 years after the end of a client relationship.

For the Digicall Group's potential clients, personal data relating to their engagement with the Digicall Group will delete or anonymized upon their request and as soon as possible, but please be advised that it may take up to 1 month to comply with such request.

Personal information about the Digicall Group's clients/potential clients who have incurred a loss to the Digicall Group may be stored for a longer period to protect the Digicall Group from further loss or for the purpose of pursuing a legitimate financial claim.

After any such period as stated above, the Digicall Group will permanently delete or anonymize all personal data.

5 Responsibilities

The IT Security and Compliance Manager is responsible for maintaining this policy and providing support and advice during its implementation in line with the IT Risk Management Policy

All Managers are directly responsible for implementing the policy and ensuring staff compliance.

Compliance with this Information Security and all subsequent policies is mandatory.

6 Policy Compliance Monitoring

6.1 Compliance

Group IT will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

If any user is found to have breached this policy, they may be subject to the Digicall Group's disciplinary procedures. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

6.2 Exceptions

Any exception to this policy must be approved by the Group Chief Information Officer in advance.

6.3 Non-compliance

All users (employees, contractors, vendors) are required to adhere to this Policy. Failure to comply may result in disciplinary action up to and including termination from employment, termination of contract, and civil penalties and/or criminal sanctions, depending on the circumstances.

6.4 Remediation of Non-compliance

Where non-compliance has been identified, dependent on the severity, criticality, and impact, opportunities may be provided to correct identified non-compliance. This corrective action will be evaluated on a case-by-case basis and timelines will be imposed and strictly enforced to ensure timeous remediation.

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Human Resources Department or the IT Security and Compliance Manager.

7 Policy Governance

The following table identifies who within the Digicall Group is **Accountable, Responsible, Informed** or **Consulted** with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	IT Security and Compliance Manager
Accountable	Group Chief Information Officer
Consulted	IT Infrastructure Manager, Regional IT Infrastructure Managers
Informed	All Employees, All Temporary Staff, All Contractors, All Vendors and All Suppliers

8 Audit and Review Process

This policy and compliance there to, will be audited and reviewed internally at least once every 12 months depending on the changes or requirements within the group which will be reviewed by Management, or as required by significant changes in business operations or regulatory requirements.

For Group companies' pursuing certification, policies are required to be audited externally at least once in a 36-month cycle or sooner depending on changes or requirements within the group. Any employees or contractors with suggestions should refer these to their line manager in the first instance so they can be considered for implementation. Whenever changes are made to this policy the final draft will be shared with the Group CIO, IT Infrastructure Manager and the IT Security & Compliance Manager for review and approval before publication.

The IT Security and Compliance Manager will undertake annual policy reviews.

9 Appendices

None included with this policy.