Data Privacy Policy

Prepared by Metaschool Ltd

Updated March 2025

V1.10

Revision History

Ver No.	Change Description	Prepared By	Reviewed By	Approved By	Sign
1.0	Initial Release	Management	Board of Directors	CE0	
1.10	Update 1	Management	Board of Directors	CE0	

TABLE OF CONTENTS

1. Objective

The objective of Data Privacy Policy (hereinafter referred to as ‘Data Privacy Policy’) is to set standards and/or framework for the usage and protection of confidential data related to the organization. Data Privacy Policy intends to communicate the organization’s commitment in terms of protecting the privacy of user data and protection of consumer data within the organization. It is evidence of the organization’s commitment to data protection principles.

2. Scope & Applicability

The Scope of Data Privacy Policy covers all employee/s, customers, suppliers, external consultants, partners, contractors and any other external entity. The policy defines the types of data and their appropriate usage.

3. Definition & Glossary

Term /Abbreviation	**Definition / Expansion**
IT	Information Technology

4. Policy / Process

4.1 Policy Definition

The Data Privacy Policy is designed to protect “personal data”, which is “any data related to a specific natural person or related to a natural person that can be identified directly or indirectly by linking the data”. This expressly includes an individual’s name, voice, image, identification number, electronic identifier, bio-data, phone number, device identity, and geographical location. It also includes sensitive personal data and biometric data.

The Data Privacy Policy of the organization is set on the lines of the law to be compliant to standardize the use, monitoring and management of data. The main goal is to protect and secure all data consumed, managed and stored by the organization. The Data Privacy Policy includes all data stored by the core infrastructure of the organization, including on-premise storage equipment, offsite locations, and cloud services. It should help the organization ensure the security and integrity of all data—data-at-rest and data-in-transit. The details of the Data Protection Law have been stated in ANNEXURE A.

4.2 Procedures

The Data Privacy Policy implementation is defined via procedures.

Information Technology (IT) department plays a vital role in implementing policy and ensuring adherence to the policy across the organization.

IT department, i.e. the IT Manager and/or chosen representative from the IT department, shall devise a comprehensive inventory cataloguing the storage locations of sensitive company data.

The comprehensive inventory should include the following analysis:

- CRM systems data storing employee and customer records in terms of name, gender orientation, designation, department, date of joining, compensation and wages details, payroll, health and retirement benefits.
- Employee and Customer record/s in the policy is defined as Personal data. Personal data is any information about an identified or identifiable person, known as a data subject, i.e. employee/s**.** Personal data includes any information that can be used to identify someone, alone or in combination with other information. This includes the employee/s name, date of birth, address proof and/or passport details, compensation & benefits, and educational qualifications- all of which can be utilized as identification of employee/s.
- Unstructured data residing in company equipment, remote servers and email accounts)
- Persons with a view or edit access to the data
- The volume of data ageing

The Data Privacy Policy of the organization is implemented by adhering to the following steps:

- Data Life Cycle Management – This refers to a framework that standardizes data processes in the organization, from data creation through storage and archiving until its final deletion.
- Data Risk Management – This includes identifying and assessing all risks and threats that may affect the data and thereby protecting the data confidentiality via undertaking necessary steps as may be deemed to be considered necessary.

- Data Back-up and Recovery – This includes the backup support mechanisms for data once data is created. All organization data is supported by a backup drive that is accessible in the case of an emergency, i.e. all systems failure.
- Data Access Management Controls – This includes that the data related to the organization shall be used only by authorized user/s. The records of the same shall be kept by the organization's IT department.
- Data Storage Management – This includes tasks related to securely moving data on-premises or in external cloud environments. These may be data stores for frequent, high-performance access or archival storage for infrequent access.
- Data Breach Prevention - Data breach prevention measures are implemented for the purpose of preventing unauthorized access to data. The goal is to avoid external malicious viruses or internal threats from gaining unauthorized access to information and systems. Cyber security measures are put in place for the purpose of preventing attacks on internal networks, network perimeters, data-in-transit, and data-at-rest. Typically, these measures include data encryption, implementation of antivirus software, protection against ransomware, perimeter security hardware and software, and access management software.
- Monitoring and Reviewing - Monitoring and reviewing processes help organizations gain visibility into data activities, risks and controls, helping improve protection and respond to threats and anomalies. Monitoring and reviews may also be necessary to meet compliance requirements. Ongoing monitoring provides visibility into all aspects of the data lifecycle, including data creation, storage, transmission, archiving, and destruction. These activities offer essential evidence for internal and external auditors that examine controls for data protection and management.

The organization upholds the highest responsibility in data collection from the subscribers if any, and the data received for job applications.

Therefore data collected from subscribers, if any, job applicants, employee/s, data related to products, new product development and innovations, finance, supply chain and any other data shall be treated with confidentiality.

All data shall be treated in the following manner:

- All data shall be processed within its legal and moral boundaries.
- All data shall be protected against illegal and unauthorized access.
- All data shall be protected against any unauthorized or illegal access by internal or external parties.
- Data shall not be communicated informally.
- The data shall not be stored for more than the specified time.
- Data shall not be distributed or transferred to organizations, states or countries that do not have adequate data protection policies.
- Data shall not be distributed to any other parties other than the agreed upon (exempting legitimate requests from law enforcement authorities)
- Let the employee/s and/or parties involved from whom the data is being collected and keep them informed of how, i.e. how, the data shall be processed/used and who has access to it.

4.3 Responsibility – IT Department / HR Department / Finance Department / Supply Chain

- The IT Manager must formulate an effective governance strategy to keep track of inward or outward data flow.
- The IT Manager and the Supply Chain Manager shall have to maintain oversight of third-party service providers and data processors since the Data Protection Law considers the collecting

party responsible for the safeguarding of personal data even if the information has subsequently been shared with other parties.

- HR Manager/s and/or Business Head/s of the organization are strictly responsible for adhering to and ensuring the culture of data confidentiality with respective teams. Building an enterprise-wide appreciation of good information security practices requires a combination of senior-level buy-in and a commitment to continuous learning.
- The IT Manager should constantly be vigilant in maintaining IT security and controls similar to the adoption of information security frameworks or the ISO/IEC 27701 International Standard for Privacy Information Management.
- Adoption of effective data breach response measures

5. Non-compliance and consequences

In the event of non-compliance with Data Privacy Policy, the concerned Department Manager/s and/or concerned parties involved shall be suspended and/or terminated and/or legal action shall be taken towards parties involved in non-compliance.

6. Special Circumstances and Exceptions

In the event the Manager/s are unable to comply with the Data Privacy Policy due to challenges that involve specific situation/s or circumstances, then the party and/or parties involved shall be exempted in writing by the management from any legal action.

ANNEXURE A

The Data Protection Law creates a framework to ensure confidentiality and protect the privacy of individuals (i.e. data subjects) by requiring organizations that fall within the scope of the Data Protection Law to implement appropriate governance for managing and protecting personal data.

A single national data privacy regulator – known as the Data Office – will be established under a separate statute to regulate the implementation of the Data Protection Law. The Data Office will be responsible for a wide range of tasks that include:

- proposing and preparing policies relating to data protection;
- proposing and approving the standards for monitoring the application of legislation regulating personal data;
- preparing and approving systems for complaints and grievances, and
- issuing guidelines and instructions for the implementation of data protection legislation.

The Data Protection Law will have extra-territorial reach. It will apply to any organization that is established and processes the personal data of data subjects inside or outside the, as well as any organization that is established outside the and processes the personal data of data subjects inside the

The Data Protection Law will not apply to government data, government entities that control or process personal data, personal data held by security and judicial authorities or any processing of personal data for

personal purposes. Additionally, the Data Protection Law does not apply to:

1. Health personal data regulated by the ICT Healthcare Law (Law No.2 of 2019).
2. Banking personal data that is subject to laws regulating the protection of such data.
3. Companies and establishments located in free zones in the that have a specific legislation on data protection, such as Dubai International Financial Centre and Abu Dhabi Global Market.

Accordingly, the Data Protection Law will operate alongside – but not replace – the existing free zone regimes.

The Data Protection Law also provides the Data Office with the ability to exempt certain organizations that do not process a large volume of personal data from some or all of the requirements prescribed by the Data Protection Law in accordance with the standards and controls to be set out in the executive regulations.