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. Policy / Process

Policy Definition

It 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, 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.

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:

- HR systems data storing employee records in terms of name, gender orientation, designation, department, date of joining, compensation and wages details, payroll, health and retirement benefits.
- Employee 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.

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

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.

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.