Data Privacy Management Policy

Table of Contents

1. Introduction 2
2. Scope 2
3. Principles and Guidelines 2
4. Governance 3
5. Training and Awareness 3
6. Grievance Redressal 3
7. Change in Policy 3

1. Introduction

Cipla is committed to data privacy and data protection. We strive to apply and integrate reasonable and appropriate information security controls within the organization's working environment, to ensure information protection from cyber threats to confidentiality, integrity and availability, thereby enhancing confidence/assurance to all the stakeholders.

2. Scope

This Policy outlines the governance structure for data privacy and protection matters, guidelines for collecting and using personal information, mechanism for monitoring compliance and grievance redressal.

This Data Privacy Management Policy ("Policy") is applicable to Cipla's associates, contractors, consultants, interns, trainees, service providers, customers, and business partners who may have access to or receive Personal Data from Cipla, or who provide Personal Data to Cipla.

This Policy applies regardless of where the processing of Personal Data happens, or whether the Processing is wholly or partly automated, or manually as part of a structured filing system. Wherever the context requires in the Policy, Personal Data shall be construed to also include Sensitive Personal Data.

3. Principles and Guidelines

Cipla shall abide by the following principles when managing Personal Data:

- Processing of Personal Data shall be done lawfully, fairly and transparently, regardless of the source of Personal Data.
- Personal Data shall only be collected and processed for specific, explicit and legitimate purposes.
- Personal Data collected shall be adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected. No more than the minimum amount of data shall be retained for processing.
- Personal Data shall be accurate and up to date. Upon receipt of request from the Data Subject, inaccurate data shall be rectified or erased.
- Personal Data which is no longer required shall be removed or erased.
- Adequate security controls shall be implemented for protection against unauthorized processing, loss, damage, and destruction.

Guided by these principles, Cipla shall:

- uphold rights of Data Subjects and address their concerns through the data protection office;
- inculcate a culture of data protection and privacy to sustain awareness and adhere to global data protection laws;
- embed privacy-by-design in organizational processes;
- retain Personal Data only for as long as necessary to fulfil the purposes of collection or as required by law;

- ensure that access to Personal Data is given only to authorized associates;
- ensure adequate security controls are in place when transferring Personal Data across jurisdictions or to any third party through means of contracts, data transfer agreements, or to the extent allowed by law;
- record and report all data breaches to the data protection office, the relevant regulatory authority, and the affected Data Subjects within prescribed timelines;
- confirm adherence to this policy through regular audits and monitoring systems;
- take timely remedial measures against all breaches to this Policy;
- encourage adherence to this Policy by imbibing this as an inherent part of work culture.

4. Governance

Robust data protection controls and risk response mechanisms are followed to cater to protection of personal data within Cipla ecosystem. The Audit Committee reviews complaints /breaches related to data privacy, and actions taken thereon, as a part of its governance and oversight responsibilities.

Cipla also has a Chief Information Officer (CIO) who is responsible for overseeing the data privacy related matters.

5. Training and Awareness

Employees shall be adequately made aware of their dos and don'ts through awareness trainings. Every manager shall make sure that their respective teams have received all necessary training and are fully aware of their responsibilities in terms of information security.

6. Grievance Redressal

Any query with respect to data privacy can be addressed to globalprivacy@cipla.com. Grievances with respect to data privacy can be reported to the Grievance Officer – Mr. Deepak Viegas at grievance.officer@cipla.com. Upon receipt of the communication, Cipla will examine and address the query/grievance raised as per internal policies and guidelines.

7. Change in Policy

Cipla reserves the right to amend this Policy without prior notice to reflect technological advancements, legal and regulatory changes and good business practices.

This Policy is effective from 12th July 2023.