Cohance

INFORMATION SECURITY MANAGEMENT SYSTEM

DATA PRIVACY & PROTECTION POLICY

VERSION 1.1

20TH MAY 2025

DOCUMENT CONTROL

Document Information

Document No.	Title	Version No.	Description
Cohance-ISMS-PY-15	Data Privacy & Protection Policy	1.1	This document provides policy direction to stop the exfiltration of data and intellectual property and to prevent unintentional data leaks or data breaches.

Responsibilities

	Name	Role	Sign & Date
Prepared by	Sarath Kumar Reddy Gaddam	Sr. Manager, IDS	20/05/2025
Reviewed & approved by	Pavan Boddapati	Information Security Manager	20/05/2025
Authorized by	Nitin Kumar Shantha	Chief Information Officer	20/05/2025

Version History

Version No.	Release Date	Prepared by	Reviewed By	Version Description
1.0	15th July 2024	Sarath Kumar Reddy Gaddam	Pavan Boddapati	First Release
1.1	20th May 2025	Sarath Kumar Reddy Gaddam	Pavan Boddapati	Logo change, Second Release

Contents

1. INTRODUCTION

As part of its business operations, Cohance collects, processes and uses certain information that is confidential or private. Therefore, it prioritizes data privacy and is committed to protecting personal information from unauthorized access, ensuring that sensitive data such as personal identities (social security numbers), financial records, and health information remains secure. This Data Privacy & Protection Policy provides policy direction and security strategy that safeguards sensitive data to ensure safety, security, compliance, privacy, ethical requirements, and brand reputation to enable business effectiveness and efficiencies.

2. OBJECTIVE

The objective of this Policy is to:

- to identify data/information that is confidential or private,
- to ensure effective procedures are in place to safeguard individuals' personal information from unauthorized access in compliance with applicable Data Privacy Laws that include:
    a. India's Digital Personal Data Protection Act 2023, and
    b. European General Data Protection Regulation (EU GDPR).

3. SCOPE

This Policy applies to all employees, contractors, and other people working for Cohance and its partners and service providers.

4. POLICY

4.1 Accountability and Responsibilities for Data Protection

4.1.1 The Board of Directors is ultimately accountable for ensuring Cohance meets its legal obligations. It will ensure that responsibilities for relevant roles are assigned and communicated within Cohance. The Board will appoint a competent person as the Data Protection Officer (DPO) who will be responsible for overseeing the privacy and security requirements of personal information processed and be the point of contact for privacy and security matters.

4.1.2 Everyone who works for or on behalf of Cohance (meaning permanent, fixed term, or temporary staff, any third-party representatives, interns engaged with Cohance) and who has access to Cohance's information systems shall be responsible for ensuring personal data is handled and processed in line with this Policy.

4.1.3 All members of staff have an obligation to report actual or potential data protection compliance failures as specified in our Acceptable Use and Incident Management Policies so that Cohance's

obligation of informing the Regulators and affected customers / data subjects can be fulfilled within statutory time frames.

4.2 Identifying and Recording uses of Personal Data

4.2.1 An Information Assets Register shall be established and maintained. The Register shall capture, among other things, relevant details about personal data that includes identification of:

- Key business processes that utilise personal data
- Sources of personal data
- Categories of personal data processed, including identification of high-risk and special category personal data
- The purpose for which each category of personal data is used, including subsequent secondary purposes over and above the initial purpose collected
- Potential recipients of personal data
- Key systems and repositories of personal data
- Offshore transfer, retention and disposal requirements.
- Whether Cohance is acting as a data controller or data processor

4.2.2 Regular data reviews to manage and mitigate risks shall be conducted through updates to the information assets register. This includes information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

4.3 Collection and Processing of Personal Data

4.3.1 Fair, lawful and transparent processing:

- Personal data shall only be processed based on a legal basis which is recorded in the Information Assets Register
- Information shall be provided to the data subjects in an appropriate format which clearly communicates the following:
    - the purpose for which their personal data can be processed
    - the legitimate interest of Cohance
    - types of personal data collected
    - information about disclosure to third parties
    - transfer of such personal data outside the country and safeguards in place
    - rights of the data subject
    - the retention period for their personal information
    - Any other information to make the processing fair and transparent
- The means by which an individual can object to data processing by Cohance shall be clearly explained in the following circumstances:

- where the personal data is collected for marketing purposes or might be so used in future
- where profiling by automated means is used for marketing purposes

- Any information presented to an individual shall be in a format easily accessible and understood by the intended audience.
- A record of privacy information (including privacy notices and online privacy statements) provided to individuals shall be maintained.

4.3.2 Processing for Specific Legitimate Purposes

- Any use of personal data shall be justified using at least one of the conditions for processing that are specifically documented. All staff members who are responsible for processing personal data shall be aware of the conditions for processing.
- Personal data obtained for one purpose shall not be used for any unconnected purpose unless the individual concerned has explicitly agreed to this or a relevant exemption applies.

4.3.3 Adequate, Relevant and in line with data minimisation principles

- Any personal data collected shall be adequate for its purpose. Regular reviews of the technology and processes shall be conducted to ensure that the personal data continues to be adequate for its purposes.
- Cohance's systems and processes shall be reviewed annually to ensure the personal data being processed is relevant and not excessive.

4.3.4 Data Accuracy and Data Currency

- Integrity and accuracy of personal data being processed shall be ensured.
- Any request by the individual to correct their personal data is promptly acted upon.
- If any personal data is found to be inaccurate or out of date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate

4.3.5 Secure Processing

- All personal data collected, held, and processed shall be kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.
- Detailed descriptions of all technical and organisational measures taken by Cohance shall be maintained to ensure the security of personal data.
- Where Cohance shares personal data with a third party, the responsibilities of both parties with regard to personal data shall be formally documented in a written agreement or contract as appropriate.

4.3.6 Processing in accordance with the Individual's Rights

- Personal data shall be collected and processed lawfully, fairly, and transparently without adversely affecting the rights of the data subject.
- Any request from an individual to not use their personal data for direct marketing purposes shall be honoured and recorded in the relevant systems.
- Direct marketing material shall not be sent to someone electronically (e.g., via email) unless Cohance has an existing business relationship with them in relation to the services being marketed or valid consent has been obtained from the subjects who are recipients of such marketing material.
- Guidance of the Data Protection Officer shall be sought on direct marketing before starting any new direct marketing activity.
- A data subject may request that any information held about them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

4.3.7 Subject Access Requests

- A data subject may make a subject access request (SAR) at any time to find out more about the personal data which Cohance holds about them.
- Subject access requests can be made in writing/email, by phone, in person, or on social media.
- Cohance shall respond to such requests within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases, the data subject shall be informed of the need for the extension).
- All subject access requests received must be forwarded to Cohance's Data Protection Officer.
- No fee shall be charged for the handling of normal SARs. A reasonable fee may be charged for additional copies of information that has already been supplied to a data subject and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

4.4 Data Retention

4.4.1 Personal data shall not be kept for any longer than is necessary for the purposes for which that data was originally collected and processed.

4.4.2 The Information Asset Register shall identify the retention period for each type of personal data and shall:

- include any minimum retention period required by law, as well as the retention period set by Cohance.
- include justification and basis for the retention periods.

4.4.3 When the data is no longer required, all reasonable steps will be taken to erase it without delay in accordance with the *Information Classification Scheme* and in line with the level of security appropriate to the sensitivity of the personal data.

4.5 Processing of personal data outside India

4.5.1 Cohance shall not transfer personal data for processing to such country or territory outside India as may be so notified by Government of India.

4.6 Data Governance

Cohance shall focus data governance primarily on the following Generally Accepted Privacy Principles (GAPP). These privacy principles are essential to the proper protection and management of personal information.

4.6.1 Management:

- Cohance shall define, document, communicate, and assign accountability for its privacy policies and procedures.

4.6.2 Notice:

- Cohance shall provide notice about its privacy policies and procedures and identify the purposes for which personal information is collected, used, retained, and disclosed.

4.6.3 Choice and consent:

- Cohance shall describe the choices available to the individual and obtain implicit or explicit consent with respect to the collection, use, and disclosure of personal information.

4.6.4 Collection:

- Cohance shall collect personal information only for the purposes identified in the notice.

4.6.5 Use, retention and disposal:

- Cohance shall limit the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent.

- Cohance shall retain personal information for only as long as necessary to fulfil the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.

4.6.6 Access:

- Cohance shall provide individuals with access to their personal information for review and update.

4.6.7 Disclosure to third parties:

- Cohance shall disclose personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

4.6.8 Security for privacy

- Cohance shall protect personal information against unauthorized access (both physical and logical).

4.6.9 Quality:

- Cohance shall maintain accurate, complete, and relevant personal information for the purposes identified in the notice.

4.6.10 Monitoring and enforcement:

- Cohance shall monitor compliance with its privacy policies and procedures and have procedures to address privacy related inquiries, complaints and disputes.

4.7 Personal Data Breach

4.7.1 Cohance shall protect personal data, including any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent Personal Data Breach.

4.7.2 In the event of a Personal Data Breach, Cohance shall notify the Data Protection Board of India and each affected Data Principal of such breach in a timely manner.

4.8 Security Assessments

4.8.1 The Data Protection Officer shall ensure that regular security assessments are undertaken to establish whether existing security controls around personal data are adequate and make recommendations for improvements if necessary.

4.9 Employee Education

4.9.1 Regular training for employees and contractors shall be conducted on this Policy. New joiners will receive training as part of the induction process. Further training will be provided annually or whenever there is a substantial change in the law or our policy and procedure.

4.9.2 Such training will be provided through an in-house seminar or via online learning portals. Completion of training is mandatory.

4.9.3 Such training shall cover the following:

- The laws relating to data protection and privacy
- Cohance's data protection and privacy and related policies and procedures

5. POLICY COMPLIANCE

5.1 Compliance Checks

Compliance with this Policy is mandatory. The Information Security Manager shall verify compliance to this policy through various methods, including but not limited to, security monitoring, business tool reports, internal and external audits, and provide feedback to the Leadership team / Policy Owner.

5.2 Review

This Policy shall be reviewed every two years or whenever there are technology / business changes impacting the policy implementation.

5.3 Exceptions

Any exception to this policy must be approved in writing by the Policy Owner in advance.

5.4 Non-Compliance

An employee / contractor found to have violated this policy may be subject to disciplinary action, up to and including termination of employment / contract.

6. RELATED PROCEDURES

The following procedures assist in implementing this Policy:

S.No.	Name of the Related Procedure	Reference Section
1.	IT Roles and Responsibilities	Entire document
2.	Incident Management Procedures	Entire document

7. ABBREVIATIONS AND TERMS

Acronym / Term	Definition
GAPP	Generally Accepted Privacy Principles
GDPR	General Data Protection Regulation
ISO	International Standards Organization
NDA	Non-Disclosure Agreement
SAR	Subject Access Request
DPO	Data Protection Officer

***