HFCL Limited

Privacy Information Management System

Policy & Objectives

Version 1.3

Document Control

Sr. No.	Type of Information	Document Data
1	Document Title	Privacy Information Management System Policy & Objectives
2	Document Code	HFCL /PIMSPP/2020/1016
3	Document File Name	1016_HFCL Privacy policy_Objectives v1.3
4	Document Owner	ISMS & PIMS Steering Committee
5	Document Author(s)	ISMS & Privacy Team
6	Document Approver	CISO & DPO

Document Change History

Version Number	Revision Date	Nature Of Change	Date Approved
1.0	03-Dec-20	Initial Release	04-jun-21
1.1	02-Aug-21	After Stage 1	09-Aug-21
1.1	01-Apr-22	Review	08-Apr-22
1.1	02-May-23	Review	08-May-23
1.2	09-Apr-24	Review & update	22-Apr-24
1.3	07-Apr-25	Review & update	18-Apr-25

Table of Contents

1. **About HFCL** 4
2. **Role of Personally Identifiable Information or Privacy** 4
3. **PIMS Policy** 5
   a). Applicability to HFCL 6
   b). HFCL's Role as a Data Fiduciary 7
   c). Key Obligations for HFCL as a Data Fiduciary 7
   d). Rights of Data Principals (HFCL's Customers and Employees) 8
   e). Data Breach Management 8
   f). Penalties for Non-Compliance 8
   g). Implications of the Digital Personal Data Protection Act, 2023 for HFCL 8
4. **Goals** 10
5. **Data Protection Objectives** 10
6. **Measurable Objectives** 11
7. **Data Minimisation Objectives** 11
8. **Methodology** 12
9. **Disciplinary Action** 12
10. **Review** 12

1. About HFCL

Over the past three decades, HFCL has delivered innovative, customized and competitive products and latest solutions in the high technology telecommunications infrastructure sector, thereby enabling its customers to stay ahead of their peers in technology and network efficiency. The Company's activities cover the entire value chain from the manufacturing of leading-edge telecommunication products to implementation of telecommunication networks.

i. **Core Business:** HFCL's main activities revolve around providing end-to-end solutions for data and telecom applications. This includes:

   a. **Manufacturing**: Producing optical fiber and Optical Fiber cables (OFC), including underground, aerial, micro duct, FTTH, and micromodule cables. We also manufacture various telecom equipment like unlicensed band backhaul radios, Wi-Fi access points, routers, managed switches, and 5G products.
   b. **Turnkey Contracts and Services**: Delivering comprehensive telecom infrastructure and communication network systems. This involves system integration services for various clients, including telecom service providers, defense organizations, railways, and smart city projects.

ii. **Products and Solutions:**

   a. **Optical Fiber and Cables**: A wide range of OFC products with varying fiber counts, designed for diverse applications and environments.
   b. **Telecommunications Equipment**: Includes solutions for both licensed and unlicensed spectrums, catering to enterprise, communication providers, and industry verticals. They are notably the first Indian company to launch 5G Fixed Wireless Access (FWA) equipment.
   c. **Passive Networking Components**: High-density cabinets, joint closures, optical splitters, and cable assemblies.
   d. **Defense Products**: The company is expanding its presence in the defense sector, developing electronic fuzes, thermal weapon sights, and surveillance radars, and establishing communication networks for the armed forces.

iii. **Manufacturing**: HFCL has multiple manufacturing facilities in India (Goa, Chennai, Hyderabad & Hosur) and we also planning to set up a manufacturing facility in abroad.

iv. **Global Presence**: Along with a strong pan-India presence, HFCL exports its products to over 45 countries.

v. **Clients:** Prominent clients include major telecom operators like Jio, BSNL, Vodafone Idea, and Airtel, as well as entities in railways and defense.

2. Role of Personally Identifiable Information or Privacy

Information privacy is a branch of data security concerned with the proper handling of data – consent, notice, and regulatory obligations. More specifically, practical data privacy concerns often revolve around:

Whether or how data is shared with third parties.

How data is legally collected or stored.

Regulatory restrictions such as GDPR or any other regulatory.

The purpose of this policy is to **protect** the personally identifiable information or personal data collected and processed by HFCL so that no harm is caused to data subjects (PII Principals). This is also referred to as Data Protection.

PIMS Policy

Policy Statement

HFCL is committed to comply with privacy requirements of ISO 27701 and its personal information management system to adhere to all data protection principles and protect the rights and freedom of data subjects by safely and securely processing their data in accordance with the data protection laws. Secure handling of personal data is extremely important to our company. Availability, confidentiality, and integrity are essential conditions for maintaining and ensuring data protection in all processes of data processing. All internal and external entities involved in the data processing are required to comply with the company-wide specifications.

HFCL shall comply with the principles of data protection enumerated in the EU General Data Protection Regulation and ISO 29100.

i. Lawfulness, fairness and transparency

Personally, Identifiable information (PII) shall be processed lawfully, fairly and in a transparent manner in relation to the PII principal. Data we collect and process shall be fair, supported by a legal basis. PII shall only be collected for specific and legitimate purposes.

ii. Purpose limitation

Personally, Identifiable information shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

iii. Data minimisation

Personally, Identifiable information collected and processed shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. HFCL shall use or offer as default options, wherever possible, interactions and transactions which do not involve the identification of PII Principals, reduce the observability of their behaviour and limit the likability of the PII collected.

iv. Accuracy

Personally, Identifiable information collected and processed shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that the PII that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

v. Storage limitation.

Personally, Identifiable information shall be kept in a form which permits identification of PII principals for no longer than is necessary for the purposes for which the such information is processed;

vi. Integrity and confidentiality (security)

HFCL have an obligation to provide security for the data we collect from users. The level of security matches the sensitivity of the data being collected. PII, we hold shall be kept safe and secure. PII shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

vii. Individual participation and access

Every PII Principal has a right to receive confirmation from us about the PII we collect from or relating to the individual. If such PII exists, the PII Principal has the right to request and receive such PII in a timely manner and at a reasonable cost. Upon granting the request, we deliver the PII to the individual in a format that is intelligible to the PII Principal. If the request for the information is denied, PII Principal have the right to challenge the denial. Furthermore, if upon receipt of the data PII Principal determines that the data is incorrect, he/she has the right to have the data corrected, amended or deleted.

viii. Privacy compliance

We ensure that the processing meets data protection and privacy safeguarding requirements by periodically conducting audits using internal auditors or trusted third-party auditors. We have appropriate internal controls and independent supervision mechanisms in place that assure compliance with relevant privacy law/ regulations.

ix. Accountability

We believe that processing of PII entails a duty of care and the adoption of concrete and practical measures for its protection.

HFCL shall comply with the principles of data protection enumerated in the **Digital Personal Data Protection Act, 2023 (DPDP Act)**

The Digital Personal Data Protection Act, 2023 (DPDP Act) is a comprehensive legislation in India that governs the processing of digital personal data. For a company like HFCL (Himachal Futuristic Communications Limited), which operates in the telecommunications and optical Fibre & Optical fiber cable manufacturing sectors, handling a significant amount of customer, employee, and business partner data, compliance with the DPDP Act is crucial.

It's important to understand that the DPDP Act is a general law applicable to all entities processing digital personal data. Therefore, this document will outline how the provisions of the DPDP Act apply to HFCL and the key responsibilities it would entail.

a). Applicability to HFCL

The DPDP Act will apply to HFCL in the following ways:

- **Processing of Digital Personal Data within India**: Any digital personal data that HFCL collects from its customers (e.g., for broadband services, telecom equipment sales), employees, or business partners within India, and processes, will fall under the Act's purview. This includes data collected online or offline and subsequently digitized.

- **Extraterritorial Application**: If HFCL offers goods or services to Data Principals (individuals) within India, even if the processing of their digital personal data occurs outside India, the Act will still apply. This is particularly relevant if HFCL has international operations or data centers.

b). HFCL's Role as a Data Fiduciary

Under the DPDP Act:

- Data Fiduciary: HFCL will be considered a Data Fiduciary because it determines the purpose and means of processing the personal data of its customers, employees, and other individuals. This means HFCL bears primary responsibility for ensuring compliance with the Act.

c). Key Obligations for HFCL as a Data Fiduciary

HFCL must adhere to the following core obligations:

- **Lawful Processing and Consent**:
  - HFCL must process personal data only for a lawful purpose.
  - It must obtain free, specific, informed, unconditional, and unambiguous consent from Data Principals before processing their data. This consent must be given through a clear affirmative action.
  - HFCL must provide a notice to Data Principals before or at the time of seeking consent, detailing the categories of personal data collected and the specific purposes for which it will be processed.
  - Mechanisms for Data Principals to withdraw consent with the same ease as it was given must be provided.
  - For "legitimate uses" (e.g., voluntary sharing of data, government services, medical emergencies, employment), consent may not be explicitly required, but transparency remains key.
  - Third parties where required by applicable law and regulation – we may be requested or compelled to disclose Personal Data to third parties such as government regulators and law enforcement agencies. We will only provide Personal Data to such parties where there is a legal requirement or permission to do so.
- **Data Minimisation**: HFCL should collect only such personal data that is necessary for the specified purpose for which it is being processed.
- **Accuracy and Completeness**: HFCL must make reasonable efforts to ensure that the personal data it processes is accurate, complete, and consistent, especially if it is likely to be used to make a decision affecting the Data Principal.
- **Security Safeguards**: HFCL is obligated to implement reasonable security safeguards to prevent personal data breaches, including unauthorized access, processing, or loss of personal data. This would involve robust cybersecurity measures, access controls, and regular audits.
- **Data Retention and Erasure**: Personal data should be retained only for as long as necessary for the purpose for which it was collected. HFCL must erase personal data once the purpose is met or upon withdrawal of consent, unless retention is required by law.
- Data Protection Officer (DPO)

    - Appointed a Data Protection Officer (DPO) based in India, responsible for overseeing compliance and acting as a point of contact for Data Principals and the Data Protection Board.
    - Conduct Data Protection Impact Assessments (DPIAs) for certain processing activities.
- Grievance Redressal Mechanism: HFCL must establish a clear and accessible grievance redressal mechanism for Data Principals to raise complaints or concerns regarding their personal data.
- Obligations in relation to Children: If HFCL processes personal data of children (individuals under 18), it must obtain verifiable parental consent. It is also prohibited from tracking, monitoring children's behavior, or directing targeted advertisements at them, if such processing is likely to have a detrimental effect on the child's well-being.

d). Rights of Data Principals (HFCL's Customers and Employees)

HFCL must facilitate and respect the following rights of its Data Principals:

- **Right to Information**: Customers and employees can request information about their personal data being processed, including a summary, processing activities, and identities of other Data Fiduciaries with whom their data has been shared.
- **Right to Correction and Erasure**: Individuals have the right to request correction, completion, updating, and erasure of their personal data.
- **Right to Grievance Redressal**: Data Principals can utilize HFCL's grievance mechanism and, if unresolved, escalate to the Data Protection Board of India.
- Right to Nominate: Individuals can nominate another person to exercise their rights in case of death or incapacity.

e). Data Breach Management

In the event of a personal data breach, HFCL has a critical obligation to:

- Notify the Data Protection Board of India: HFCL must notify the DPBI of the breach in the prescribed manner.
- Notify Affected Data Principals: HFCL must also notify the affected Data Principals of the breach, providing relevant information to enable them to take protective measures.

f). Penalties for Non-Compliance

Non-compliance with the DPDP Act can lead to significant monetary penalties. For instance:

- Failure to take reasonable security safeguards to prevent a personal data breach: Up to INR 250 crore.
- Breach in observance of additional obligations in relation to children: Up to INR 200 crore.
- Failure to notify the Data Protection Board and affected Data Principals in the event of a personal data breach: Up to INR 200 crore.
- Breach in observance of duties of Data Principals: Up to INR 10,000.

g). Implications of the Digital Personal Data Protection Act, 2023 for HFCL

To ensure compliance with the DPDP Act, HFCL should consider the following actions:

- **Conduct a Data Audit**: Map all personal data collected, stored, processed, and shared across all departments and systems (Admin, F&A, HR,SCM, IT, sales, marketing, operations,).
- **Review and Update Privacy Policies**: Ensure privacy notices are clear, concise, easily understandable, and compliant with the consent requirements of the Act.
- **Implement Robust Consent Mechanisms**: Develop systems to obtain valid consent, record it, and allow Data Principals to easily withdraw consent.
- **Strengthen Security Measures**: Enhance cybersecurity infrastructure, implement encryption, access controls, and conduct regular security audits and vulnerability assessments.
- **Establish a Grievance Redressal System**: Create clear channels for Data Principals to exercise their rights and address complaints.
- **Appoint and Train Key Personnel**: Designated a DPO and provide comprehensive training to all employees involved in data processing on their responsibilities under the Act.
- **Review Third-Party Contracts**: Ensure that all contracts with Data Processors and other third parties handling personal data have appropriate data protection clauses aligned with the Act.
- **Develop Data Breach Response Plan**: Create a clear plan for identifying, assessing, reporting, and mitigating data breaches.
- **Monitor Regulatory Updates**: Stay informed about any further rules, regulations, or guidelines issued by the Central Government or the Data Protection Board of India.

By taking these proactive steps, HFCL can establish a strong data protection framework, build trust with its stakeholders, and ensure compliance with the Digital Personal Data Protection Act, 2023.

To support this policy, HFCL shall:

- *Raise, enhance, test and maintain awareness of Privacy through on ongoing education and awareness program for employees,*
- *With regard to the processing of personal data, all statutory requirements must be strictly observed, any exception or associated reduction in protection level is not permitted and must always be approved by management.*
- *ensure, where relevant, that the contract to process PII addresses HFCL 's role in providing assistance with the customer's obligations, (taking into account the nature of processing and the information available to the organization).*
- *ensure that PII processed on behalf of a customer are only processed for the purposes expressed in the documented instructions of the customer.*
- *not use PII processed under a contract for the purposes of marketing and advertising without establishing that prior consent was obtained from the appropriate PII principal. One click shall not make providing such consent a condition for receiving the service.*
- *HFCL shall provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations.*
- *Maintain data inventory of categories of personal information processed by the organization and records of processing.*
- *Provide the ability to return, transfer and/or disposal of PII in a secure manner. It shall also make its policy available to the customer.*
- *facilitate its customers to fulfil their obligations to PII Principals (where HFCL is a processor) and determine and fulfil its obligations to PII Principals in relation to information to be provided to them, fulfil its obligations in relation to PII Principals regarding rights to access, correct and/or erasure, the PII, object to processing PII, provide copy of PII (where HFCL is a controller).*
- *Assign responsibility and accountability to relevant personnel throughout the organization and ensure communication of this policy.*

- *Manage the data protection risks by identifying, evaluating and mitigating current and potential risks.*
- *Fully implement all appropriate technical and organizational measures for security of the PII.*
- *Implement measures to ensure privacy by design and default, wherever applicable:*
    - *Data minimization*
    - *Pseudonymization*
    - *Anonymization*
- *Subject PII transmitted over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.*
- *Monitor and review the compliance to this policy on regular basis.*
- *Management review of all the privacy risk assessments and impacts of the same.*
- *Continually improve the personal information management system through privacy enhancing innovations.*
- *Documenting and communicating as appropriate all privacy-related policies, procedures and practices*
- *When transferring PII to third parties, ensuring that the third-party recipient will be bound to provide an equivalent level of privacy protection through contractual or other means such as mandatory internal policies (applicable law can contain additional requirements regarding international data transfers)*

This Data Protection Policy is in force and binding.

Date: 18/04/25

Signature: .....

4. Goals

To identify through appropriate risk assessment, the degree of protection of personal information, the preparedness against threats, to understand their vulnerabilities and the threats that may expose them to risk.

To manage and minimise the risks to an acceptable level through the design, implementation and maintenance of a formal Privacy Information Management System (PIMS)

To comply with Legislation including (but not limited to):

- Applicable legislation, regulatory and customer requirements;
- Commitment to be in compliance with ISO 27701:2019.
- Commitment to achieve continual improvement by adherence to data protection and governing best practices, wherever applicable.

5. Data Protection Objectives

HFCL has defined the following key privacy objectives:

1. **Fulfilling Customer Contractual Requirements.**
2. **Manage Personally Identifiable Information (PII)** in HFCL Corporate Delhi Office, Goa Office, Hyderabad office & Gurgaon Office
3. To **manage the identified risks** to an acceptable level through the design, implementation and maintenance of a formal Privacy Information Management System.
4. To **raise awareness** of privacy risks in employees and relevant third parties
5. **Gain trust of data subjects (PII Principals)** in an ethical manner & ensure security of the PII.

6. Measurable Objectives

To ensure the continued suitability and effectiveness of the Personal Information Management System within echo, a number of measurable objectives have been established. These objectives shall be monitored and reviewed as part of the ongoing measurement and metrics activities, and the Management Review process. These objectives include:

S.No.	Objective	Measurement
1	**Fulfilling Customer Contractual Requirements**	• Customer Data Protection Requirements • DPIA
2	**Manage PII** : To protect the integrity, availability and confidentiality **of PII** in HFCL system	• Dynamic identification of PII • Changing risk profile
3	**Manage the identified risks** to protect the organization's personal information assets from theft, abuse, misuse and any form of damage	• The number of breaches relating to the loss of personal data or breaches
4	**Raise awareness** to establish responsibility and accountability for privacy in the organization	• Staff awareness activities
5	**Gain Trust of PII Principals** viz. employees, customer's customer, vendors and other interested parties	• Transparency – Providing Privacy Notices • Responding to requests of data subjects in a regular interval.

7. Data Minimisation Objectives

Additionally HFCL has defined the following Data Minimisation Objectives:

S.No.	Objective	Measurement
1	Limit Collection & Processing	• 6 Monthly Review of ROPA to check no excessive collection of PII
2	To Ensure Bitlocker Encryption of All laptops	• 100% by 31-Dec-2022

8. Methodology

Specific policies/practices exist to support the methodology, which includes mandatory requirements of ISO 27701:2019, and a combination of policies, some of which are referred below (not exhaustive):

- ISMS & PIMS performance dashboard
- ISMS & PIMS Roles and responsibilities.
- Procedures for Incident Management and Reporting
- Non-Disclosure Agreement with all employees & vendors
- Statement of Applicability

9. Disciplinary Action

Whenever a privacy incident involving a company employee occurs and is reported, the DPO ensures notification to regulators to data subjects (PII Principals)

Based on the severity of the privacy breach, HFCL can take "disciplinary action(s)" against, an employee.

Where required, HFCL may contact external authorities such as police, cybercrime cells, forensics experts, and/or any other relevant authorities to take the necessary help.

10. Review

DPO/CISO reviews all Data Protection policies at least once a year or whenever major changes are undertaken to ensure their continuing suitability, effectiveness and compliance.

----------: End of the Document: ----------