vedanta | sesa goa iron ore

Privacy Information Management System (PIMS)

Data Governance and Privacy Policy

Documented information Name: Data Governance and Privacy Policy

Version No: 3.0

Last Updated: 25th July, 2023

Documented information Owner: Sesa Group

Approval Authority: Sesa Group

Documented Information Management Information

Documented Information Title: Data Governance and Privacy Policy

Abstract: This Documented Information highlights the policy for Data Governance and Privacy.

Documented information Publication History

(All revisions made to this documented information must be listed in chronological order, with the most recent revision at the top)

Type of Information	Documented information Data
Documented information Title	Data Governance & Privacy Policy
Documented information Code	SESAIT/ISO27701/Data Governance & Privacy Policy
Date of Release	8 Jan 2019
Documented information Revision	25-July-2023
Documented information Owner	IT Department
Documented information Author(s)	Pricoris LLP
Documented information Change Reviewer	Jyoti Singh
Checked By	Dileep Singh – CISO
Security Classification	Internal
Documented information Status	Final

Documented information Approver List

S. No	Approver	Approver Contact	Signature	Date Approved
1	Shobha Raikar (CDIO)	Shobha.raikar@vedanta.co.in	Electronically Approved	10-Aug 2023

Documented information Change Approver List

Version No	Revision Date	Nature of Change	Affected Sections	Date Approved
1.0	26-Dec-2018	First release		08-Jan-2019
1.1	17-Aug-2019	Section 6 has been added	6	22-Aug-2019
1.2	29-Nov-2019	Section 6 has been updated	6	29-Nov-2019
1.3	17-Jun-2020	Section 6 has been updated	6	25-Jun-2020
1.4	22-Oct-2020	DPIA process and template updated	Sec 4 ,5 ,6.2, 9	27-Oct-2020
1.5	10-Jun-2021	Purpose, Guiding principles, retention details capturing in Data inventory – updated	Sec 1.2, 1.4 & 3	30-Jun-2021

2.1	16 – July-2022	Inclusion of annexures and requirements of PIM	All sections	25-August-2022
2.2	31-August 2022	Updated as suggested during stage 1 PIMS	Added Authority in Section 7 and changed retention period for HR document for consistency Removed Annexure templates	03-September-2022
3.0	25-July-2023	Annual review - Addition of SESA COKE in the scope.	Change in the compliance review – change from PSC to ITSC. In section 3.4 added choice in consent section. Section 7.3 addition of response to DSR.	10-Aug 2023

Documented information Contact Point

S. No	Documented information Author	Email
1.	Dileep Singh	dileep.singh@vedanta.co.in

Table of Contents

1. Introduction

1.1 Scope

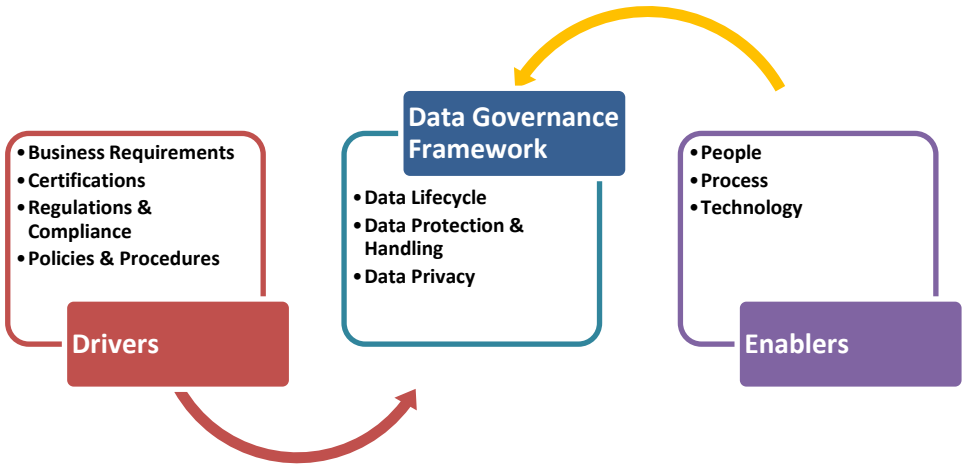
This Policy document is applicable for Vedanta Limited –Sesa Goa Iron Ore Division including SRL and SMCL in Goa, Karnataka, Odisha and Liberia, Pig Iron Division, Met Coke Division, Power Division in Goa, Sesa Coke, FACOR – Odisha, MALCO Energy, VGCB, Visakhapatnam, and Sesa Cement referred as Sesa Group in this document.

The policy is applicable to all employees, vendors, contractors and third parties associated with Sesa Group (through direct contracts) involved in handling, managing, storing and processing of PII (personally identifiable information/ SPI/sensitive business information at Sesa Group. The Policy provides management the direction and support for protecting PII/ SPI handled and processed within Sesa Group's business processes.

1.2 Purpose of the documented information

This document defines Sesa Group's policy to establish authority, management and decision-making parameters related to the data produced or managed by Sesa Goa around all the aspects of data during its lifecycle including data classification and design controls.

Following are the key elements of a data governance framework:



Additionally, this document defines Sesa Group's privacy policy to collect, access, process, store, transmit or destroy PII/ SPI and its intent and commitment to protect the same. The policy presents guidance for various functions within Sesa Group to protect privacy of employees, contractors, clients and partners, and critical organizational information through technical, managerial and procedural controls. The guidelines contained within the document are based on leading practices prevalent across the globe and comply with various regulatory and legal requirements of Sesa Group Information Security Policy and Standards.

1.3 Audience

This policy is applicable to employees who comprise of internal employees, contract employees and vendor employees who are involved in handling, managing, storing and processing data especially of PII/ SPI/sensitive business information at Sesa Group.

2. Policy Statement

Sesa 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.

To support this policy, Sesa Goa shall:

- *Raise, enhance, test and maintain awareness of Privacy through on ongoing education and awareness program for workers,*
- *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.*
- *Maintain data inventory of categories of personal information processed by the organization and records of processing*
- *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 as required by ISO 27701*
- *Implement measures to ensure privacy by design and default, wherever applicable:*
  - *Data minimization*
  - *Pseudonymization*
  - *Anonymization*
- *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.

3. Guiding Principles of Privacy Management:

3.1. Transparency – Privacy Notice

Sesa Group shall provide notice to the information providers about its privacy policies and practices, purposes of collecting personal information, usage, retention, dissemination and destruction, the identity and location in Sesa Group where the personal information resides and, information on whom to contact at Sesa Group on privacy related issues.

3.1.1 Communication to Individuals- All business functions

All business functions shall ensure that while collecting any personal information the information providers are informed about the purpose of collection of the information. The privacy notice provided to the information provider shall include following points:

- If any personal information is collected, the purpose for collection of such information and whether this purpose is a part of a legal requirement;
- Consequences, if any, of not providing the requisite information. The consequences of information provider's refusal to provide the consent or, at a later date, withdrawal of the consent with regard to collection, processing, retention and disclosure of his/her personal information;
- The process to be followed by the information provider to exercise the choices available to them with respect to their personal information (for example signing the consent clause or checking the opt in box for giving consent);
- The options with information provider to change the contact preferences and withdraw consent with regard to processing, retention, dissemination and destruction of the personal information at any later date;
- The retention of personal information for only as long as necessary to fulfil the stated purposes, or for a period specifically required by law or regulation and thereafter is disposed of securely;
- The procedure to be followed by information providers to update and correct their personal information (for example, in writing, by phone, by email, or by using the entity's website);
- Communication of the method of resolution of disagreements related to personal information;
- Information may be disclosed to the authorized third parties for providing service(s) to the information providers;
- Information may be transferred to entities located within or outside India for the purposes of providing service(s) on explicit consent from the information provider or if it is necessary for the performance of the lawful contract between Sesa Group and the information provider and post ensuring the same level of data protection is being adhered to by such entity;
- Notification about the web tools such as web cookies and web beacons which are used by Sesa Group to collect information providers' personal information while they are on Sesa Group's website and about their choice to turn off cookies and beacons and as a result not provide such information to Sesa Group;
- that reasonable physical and logical access controls are implemented to ensure privacy of their personal information; and
- Description of the procedure of registering complaints regarding their personal information including the contact information of the entity privacy officer.

3.1.2 Notice- All business functions

3.1.2.1. Provision of Notice

- Notice shall be provided to the information providers in a timely manner (that is, at or before the time personal information is collected) to enable them to decide whether or not to submit personal information; and
- Notice shall be dated to allow information providers to determine whether the notice has changed recently.
- Following privacy notices should be published by Sesa Goa:

    - Employee notice to be published on intranet by HR – Refer Annexure 1
    - Website notice to be published on Website by Marketing (for enquiries and leads),, for recruitment on career page (HR) and cookies related notice by IT Team. -Refer Annexure 2

3.2 Personal Information Categories

The Policy represents the minimum standards that Sesa Goa has set with respect to data privacy. Personal Information refers to any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with body corporate, is capable of identifying such person.

3.2.1.Data Asset Category

Sr. No.	Data Asset Category	Details
1	Human Resource Data	Human Resource data refers to Sesa Goa's employee data such as employee score card, business card, pay slip, incentives and other such employee information.
2	Technology Data	Technology data includes operations support systems (OSS)/ Business Support Systems (BSS) data, network diagrams, network configurations, minimum baseline security standards, asset inventory, incident reports, root cause analysis reports and other such IT and network information.
3	Financial Data	Information related to the financial health of Sesa Goa such as ledger details, Purchase Orders, Invoice information, expense report, revenue report and other such financial data.
4	Customers Personal Information	Personal Information includes name, address, contact details and other such information related to personal Information.
5	Third Party Data	Information related to third or fourth parties that are collected and used within Sesa Goa including vendor's PII, merchant's sales reports, merchant's incentive reports and other such third-party related data.

3.2.2.Sensitive Data

Sensitive Categories of Personal Data refers to data or information of a person means such personal information which can consists of information relating to:

- Generic Data (Grouping of data)
- Biometric Data
- Racial or Ethnic Origin
- Political Opinion
- Religious Philosophical Beliefs
- Trade Union Membership
- Data Concerning Health
- Data Concerning natural personal's sex life or sexual orientation
- Financial Data
- Aadhar Data
- Passport Details

3.3 Collection

Sesa Group shall collect personal information only for the purposes communicated to the information providers furthermore, any such information shall be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the end customer concerned.

3.3.1 Collection Limited to Identified Purpose

In case the business function needs to collect the personal information, the business function shall:

- Clearly indicate the fields of personal information which are essential for the purpose of providing product or service and differentiate it from the non-essential fields of personal information; and
- Periodically review the business' necessity of collection of personal information and ensure that the fields of information being requested are consistent and limited to those required for providing the product or service. Also, it shall be ensured that all personal information mandated by the applicable laws and regulations is collected before conducting business.

3.3.2 Collection from Third Parties

- Contracts signed with the third parties shall include provisions requiring them to collect personal information fairly and lawfully and in accordance with Sesa Group Data Privacy Policy requirements; and
- Collection methods adopted by the third parties responsible for collecting personal information of the information providers shall be reviewed. Business shall ensure that information providers are provided with the choice and their consent is obtained before collecting such information.

3.4 Consent

Sesa Group shall communicate to the information providers, the choices available to them and obtain explicit consent with regard to collection, processing, retention, dissemination and disclosure of the information.

The legal basis for the processing of PII can include:

- Consent from PII principals
- Performance of contract
- Compliance with legal obligation
- Protection of vital interest of PII principals
- Performance of a task carried out in public interest
- Legitimate interest of the PII Controller

The choices shall be implemented in a timely fashion and respected. If sensitive information is to be used for purposes not identified in the notice/ contract agreements at the time of collection, the new purpose shall be documented, the data subject shall be notified, and implicit or explicit consent shall be obtained prior to such new use or purpose.

The data subject shall be notified if the data collected is used for marketing purposes, advertisements, etc.

3.5 Classification

Data is classified under the following 4 categories:

- Public (C4)– Non-Sensitive Information available for external release. This includes
    - Job posting
    - Press release
    - Service brochures
    - Advertisements
    - Data that is freely can be made public either through direct distribution or accessible through media, and has no significant impact on the Company or employees; should be categorized as Public.

- Internal (C3) – Information that is generally available to employees and approved non-employees such as contractors, trainees. This includes
    - Business information
    - Draft request for proposal
    - Internal guidelines, circulars, instructions
    - Personally Identifiable Information (PII) such as employee details
    - Copying and forwarding to external parties is permitted with approval from Data Owner. However, special security protection has to be placed for transfer of PII.
    - This data can be internally available in its hard copy form or its soft copy form inside the Company's premises and devices or with third-parties as per agreement
- Confidential (C2) – Information that is sensitive and personal information within the company is intended for use only by specified groups of employees. This includes the following:
    - Sensitive personal information on health details, bank details, children's data
    - Personnel files, data, and program files etc.
    - Industrial trade secrets
    - Information on security measures and serious deficiencies, information on internal network topology;
    - Copies, backups and archives of confidential information;
    - Publications which are intended for a restricted group of persons.
    - Copying and forwarding is prohibited, unless approved by the Data Owner.
    - This data must be protected in its hard copy form as well as its soft copy form through the data handling techniques/processes mentioned in the Information Security Standard/Policy and Information.

- Secret (C1) - Information that is highly sensitive or business critical information and is available only to a very restricted set of individuals (or specific positions). This includes:
    - Company strategy
    - Technology and
    - Budget and strategic plans
    - Copies, backups and archives of confidential information

  NOTE: Secret (C1), Confidential (C2) and Internal (C3) data types must be shared with third-parties only after a Non-Disclosure agreement (NDA) is in place. Secret (C1) and Confidential (C2) information is shared strictly on a "Need-to-know" basis and data minimization principle.
    - Copying and forwarding is permitted with only those who need the data to perform the assigned tasks, with approval of the Data Owner.
    - This data must be protected in its hard copy form as well as its soft copy form through the data handling techniques/processes mentioned in the Information Security Standard/Policy and Information.

Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII) should be Classified for the purposes of maintaining mandatory records. Users, processes, systems and third parties handling personal information shall be identified; and the personal information shall be classified based on the sensitivity of the information.

3.6 Privacy Risk Assessment

Privacy assessment of all the functions shall be carried out initially for all processes to identify the risk of leakage of personal information and its criticality. Thereafter, such assessments shall be carried out whenever there is a change in the process or governing laws and regulations and reviewed annually.

DPO with support of entity privacy officer & data protection champion shall carry out the privacy assessment of all the business functions of Sesa Group across all locations.

Following business functions have been identified for privacy risk assessment.

- IT & BU
- Finance
- Legal
- Secretarial
- Commercial
- HR
- Marketing

Additionally, Privacy Impact Assessment (PIA) will be conducted for processing that is likely to result in a high risk to individuals. It shall be completed for any process which requires the processing of personal data. To assess the level of risk, SESA GOA shall consider both the likelihood and the severity of any impact on individuals. The specific template should be followed for PIA by individual department and to be approved by designated DPO. Refer Annexure 3

3.7 Commitments & Contracts - All business functions

Contracts and Service Level Agreements shall be reviewed and updated on periodic basis by the business functions and commercial to ensure consistency with Sesa Group Data Privacy Policy, in case of any PII being involved in new contracts the same shall be duly informed to DPO, subsequently the same shall be added into contracts by commercial team.

Key factors to be considered

- The data protection champions along with entity privacy officer of the respective locations shall assess the impact of new and significantly changed products, services, business processes, and infrastructure on privacy of personal information;
- Documented systems development and change management process shall be used for all information systems and related technology (including manual procedures, application programs, technology infrastructure, organizational structure, and the responsibilities of users), used to collect, use, process, retain, disclose, and destroy personal information;
- Potential effect on privacy shall be assessed for new systems, contracts and changes;
- Changes to system components shall be tested to minimize the risk of any adverse effect on the privacy of personal information.
- All test data involving personal information shall be anonymized;
- Procedures shall be implemented to ensure integrity and protection of personal information during migration from old to new or changed systems;
- Documentation and approval by the data protection champions along with entity privacy officer and IT department shall be taken before implementing changes to systems and procedures that handle personal information, including those that may affect its security.
- Emergency changes shall maintain the same level of protection of personal information; however, they may be documented and approved post implementation;

- The business function shall maintain a listing of all applications / software that process personal information and the respective level, version, and patches that have been applied;
- Where systems are involved, appropriate procedures shall be followed, such as the use of separate development, test, and production libraries to ensure that access to personal information is appropriately restricted; and
- Personnel responsible for initiating or implementing new systems and changes, and users of new or revised processes and applications shall be provided training and awareness sessions related to privacy.

Sample contract is contained in Annexure 4.

3.8 Data Subject Rights

Individuals (who are defined as 'Data Subjects' under the Data Protection Laws) have rights when it comes to handling of their Personal Data. Sesa Goa shall ensure that the following rights of data subjects are upheld in case the data subject opts to exercise any of the following rights except in cases where these rights are conflicting with explicit requests/ guidance from regulatory or legal authorities pursuant to Data Protection Laws.

If the data subject/PII principal is not satisfied with the way in which Sesa Goa has proceeded with any request, or if the data subject/PII principal has any complaint regarding the way in which Sesa Goa process personal data, the data subject/PII principal may lodge a complaint with a Data Protection Supervisory Authority.

Data Subjects have following rights:

- *Right to be informed*: The data controller is required to inform the data subject, prior to or at the time of the collection of the personal data, of required details such as the purpose of the collections, the data retention period, and the rights of the data subject. Refer Section 3.1.1 and 3.1.2 above
- *Right to access*: Data Subject can request supporting/detailed information about their personal data from Sesa Goa. Refer Section 3.9 below
- *Right to rectification*: Data Subject has the right to rectify his/her Personal Information provided to Sesa Goa to ensure that his/her Information is processed based on correct information. Refer section 3.9 below.
- *Right to erasure (Right to be forgotten)*: Data subject have the right to have his or her Personal Information erased and no longer processed.
- *Right to restriction of processing*: For Sesa Goa's, right to restriction would normally only mean restrictions for marketing purposes (i.e., processing based on consent). The fact that processing of personal information is restricted will be clearly indicated in Sesa Goa system/record
- *Right to Data portability*: A data subject shall have the right to receive the Personal Information concerning him or her, which he or she has provided to Sesa Goa (e.g., name, address, email-address, etc.), in a structured, commonly used and machine-readable format and has the right to transmit those data to another controller.
- *Right to Object*: The Data subject shall have the right to object (unless Sesa Goa otherwise has compelling legitimate grounds), on grounds at any time of processing of Personal Information
- *Right not to be subject to automated decision making*: The subject has the right to restrict the use of their personal data in certain circumstances.

3.8.1 Process for response to Data Subject/PII Principal request

- Sesa Goa shall provide the contact details of the DPO on the website and also at the time of consent.
- Sesa Goa shall communicate the rights to the data subjects/PII principals at the time of consent.
- Sesa Goa should respond to a DSR "without undue delay," but at the latest within one month of the request. If their requests are numerous or complex, Sesa Goa can extend the deadline by two

months, but Sesa Goa shall be expected to respond to the request within the first month and explain why the extension is necessary.

- Sesa Goa should maintain all of the subject's/PII principal's requests into a tracker

Following steps shall be taken by Sesa Goa to respond to the request:

Step 1: Verify the Subject's Identity

- Sesa Goa's first step is to verify the identity of the requester so Sesa Goa can determine whether Sesa Goa has the information which the requester is looking for.
- Sesa Goa shall verify the legitimacy of the request by verifying the email address from which the request was made and the address maintained by Sesa Goa.

Step 2: Clarify the Nature of the Request

- Sesa Goa should review the DSR to determine what the requester wants to know. In most cases, subjects simply want to see all the data you have on them, but they may invoke other data privacy rights at the same time. For instance, a subject may request rectification - the correction of inaccurate data.
- Sesa Goa should determine if Sesa Goa can reply to the request within the one-month timeframe. If more time is required to generate a response, Sesa Goa shall explain this to the data subject.

Step 3: Review the Data

- Sesa Goa will review the personal data before processing any request. Sesa Goa should review the personal data before sending it to the data subject/PII principal and verify it doesn't include anyone else's personal information or Sesa Goa will commit a data breach. For business purposes, Sesa Goa can add explanations for why Sesa Goa has their information.

Step 4: Collect and Package the Data

- The response to the data subject/PII Principal will depend on the information Sesa Goa will be providing to the data subject/ PII Principal such as deletion, rectification etc. The response must be easily understandable. Where possible, Sesa Goa shall give data subject/PII principals remote access to a secure system that would provide them with direct access to their personal data.

Step 5: Send the Data to the Subject

- Final step is to submit a response to the subject's request. Sesa Goa shall document communications with requesters so there's an audit trail to demonstrate accountability and compliance.

3.8.2 Access and Correction

Information providers, at all times, shall be able to access their personal information available with Sesa Group. Sesa Group shall provide the information providers with an option to update their personal information.

Internal Access to Personal Information

- All functions handling personal information shall be identified and the relevant processes within these functions shall be reviewed for adequacy of privacy controls of personal information;
- Access to personal information shall be provided to a Sesa Group employee (part time/ full time), contractual employee or third-party employee only after authorizations of the functional head of his/her function. All such authorizations shall be obtained over mail or in hard copy format; and
- Any changes to an individual's personal information shall be efficiently updated in all the systems of Sesa Group. If any third party is facilitating in updating this information on Sesa Group's behalf, it shall be the responsibility of the third party to accurately update the records.

3.8.3 Records of Processing Activities

Sesa Goa will maintain detailed records of all processing activities related to PII processing. Refer Annexure 5 .

3.9 Privacy by design and privacy by default

Objective: To ensure that processes and systems are designed such that the collection and processing of PII (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.

The organization shall conduct periodic verification that unused temporary files are deleted within the identified time period.
The organization shall provide the ability to return, transfer and/or disposal of PII in a secure manner. It should also make its policy available to the customer.

The organization shall ensure that PII transmitted over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.

3.9.1 Collection & Processing Limited to Identified Purpose & Collection from Third Parties

- Contracts signed with the third parties shall include provisions requiring them to collect personal information fairly and lawfully and in accordance with Sesa Goa Data Privacy Policy requirements; and
- Collection methods adopted by the third parties responsible for collecting personal information of the information providers shall be reviewed. Business shall ensure that information providers are provided with the choice and their consent is obtained before collecting such information.

3.9.2 Indirect Collection

- Sesa Goa ensures indirect collection of PII in logs and metadata is also kept to the minimum and if collected will be kept securely.
- Following controls should be implemented at the stage of data collection:
    - Identify whether the data collection is lawful
    - Identify and document purpose of collecting data
    - Identify legal basis of collecting data
    - Determine when and how consent is to be obtained
    - Obtain and record consent
    - Perform a Privacy Impact Assessment.
    - Determine the obligations to PII Principals
    - Determine and provide information to PII Principals
    - Limit collection to what is necessary
    - Determine mechanisms such as deidentification to be used.
    - Contact data privacy champion before engaging in any new collection of PII data.

3.9.3 Data Minimization

Sesa Goa has defined data minimization Objectives as below:

- Sesa Goa should ensure that the specific PII and amount of PII collected and processed is limited by identifying the extent to which PII needs to be associated with the PII Principal for the identified purposes.
- Where the identified purpose does not require the processing of the original PII, the PII should be removed/ deidentified

3.9.4 Accuracy

Sesa Goa shall strive to maintain the completeness and accuracy of the personal information of information providers available with it.

- To maintain the accuracy of the personal information available with Sesa Goa, following points shall be taken into consideration: -
- Sesa Goa shall maintain complete and accurate personal information of information providers, as provided by them, as long as Sesa Goa retains it;
- Sesa Goa shall implement measures such as technical system configurations to respond to instances of inaccurate PII.
- Sesa Goa shall ensure minimization of inaccuracies in the PII it processes throughout the PII lifecycle.
- It shall be communicated to the information providers at the time of collection, that:
    - They are responsible for providing complete and accurate Personal Information;
    - Methodology to contact Sesa Goa in case their Personal Information needs to be updated;
    - If any changes to their personal information are requested by the information providers, such requests shall be processed in a time-bound manner and the record of all such change requests shall be maintained.

3.9.5 Retention of Personal Information

The information provided by an individual to Sesa Group shall be used only for the purposes for which it was provided and consented by the individual and shall be retained for only as long as necessary to serve the purpose or as required by the applicable laws or regulations. Personal information shall be securely disposed of to prevent its retrieval and mishandling post the retention period.
For retention of the personal information, adherence to following controls shall be ensured:

- Retention period shall be defined and implemented as per the business requirement or legal requirements, whichever is later;
- Retention periods of different types of records of personal information shall be defined;
- Third parties should define and implement the “retention policy” for personal information, which should be aligned to the Sesa Group’s retention policy. This policy should clearly define the retention period for various records containing personal information; and
- Any personal information not required for conducting business or mandated by law and captured by Sesa Group’s systems is removed in a timely and secured manner to prevent mishandling.

Sr. No	Function	Records Category	Records	Retention Period	Remarks
1	HR	Employee Personal Information File	• Appointment Letter • Personal details such as PAN, Aadhar, Health records • Salary Details • Yearly compensations details • Any Disciplinary action details • Reward and recognition • Pension Details • Stock option offered	80 years	There have been cases in the past wherein access to HR files both hard and soft copy dated more than 15 years was

			• Resignation Letter • Any other details during the employment period		required for court proceedings.
		Recruitment Records	• Recruitment documents such as Candidates offer letter, • Background verification, • Medical reports, • Psychometric Reports • Competency & Skill mapping and • HR MIS	15 years	
		CVs	• Rejected CVs	10 years	CVs are required because of the niche skills for the industry.
2	Finance	Financial Information	• Audited Financial Details • Loans and Investment details • Audit Findings • Books of Accounts including vouchers and bills. o Annual Returns together with the Annexures. • Register of Transfer and Transmission of shares/Debentures and other securities. • Income Tax Details such as IT Returns • GST records – Invoices and set off claims • Any financial claims by clients, supplier • Any liabilities such as rent, lease rent, infrastructure expense and other expenses meeting day-to-day requirements.	Permanent	
3	Legal	Court Cases	• Court Proceeding • Court Judgement	Permanent	
		Contract vetting	• All Contracts reviewed and signed copy • Any Addendum as part of the contract	10 Years	

4	Secretarial	Statutory Compliance	Statutory Compliance Reports to the regulators as per the submission schedule	Permanent	
		Board Meeting Details	• Intimation of Board Meeting • Agenda, Presentation deck, MOM, Attendance of the Board Meeting • Resolution passed during the meeting • Documents relating to appointment of Director	Permanent	
		SEBI (Listing Obligation and Disclosure Requirements) Regulations, 2015:	• All reports filed with the stock exchange from time to time. • All disclosure of various events and Press Releases.	10 years	
5	IT	All Logs	• All logs relevant for any incident investigation purpose	18 months	
		All Approvals- Hard Copy	• Approval to procure any hardware/software/equipment specific to Infrastructure	5 Years	
		All Approvals - Softcopy	• Approval to procure any hardware/software/equipment specific to Infrastructure	5 Years	
		Licenses & Documentation	• All software Licenses with Expiry date	As per validity + 3 years	
		SIEM/DLP/PIM Raw Logs	• All logs for managing the Incidents	18 months	
6	Commercial	Vendor data	Vendor master records in SAP	Permanent	For legal requirements
7	Marketing	Customer data	Customer data records in SAP	Permanent	Customers are repeat and hence master data has to be maintained.

3.9.6 Disposal and Destruction of Personal Information

While disposing of personal information, following privacy controls shall be adhered to:

- Information is disposed of in accordance with the timelines defined in the retention policy of Sesa Group or its third parties depending upon the ownership of the information;
- Time of disposal is documented to include the details of the disposed-off records containing personal information. For example, document the name of the record owner, date created, date destroyed, method of destruction, fields of personal information contained by it and primary purpose for the creation of the record;
- Destruction of personal information which is no longer required for providing the services or as per applicable laws and regulations; and
- Any information retained by Sesa Group after the expiry of its retention period is retained only after obtaining consent of the information provider.

3.10 Security

Sesa Group shall ensure protection of personal information against unauthorized access, usage and dissemination.

3.10.1 Information Privacy Program

Following shall be taken into consideration while handling personal information: -

- Periodic vulnerability assessment of the physical and technical environment shall be carried out to gauge effectiveness of privacy controls implemented. Apart from this, penetration testing shall be carried out periodically to assess the resilience of websites and other systems of Sesa Group accessible through internet;
- Adequate authentication parameters and access controls, as described in Sesa Group Information Security Standards, shall be implemented at all access points of personal information;
- Access rights of all the employees handling personal information shall be periodically reviewed, at least once bi annually.

3.10.2 Logical Access Controls

- Employees shall not divulge the security procedures followed at Sesa Group to mitigate the risk of compromise of personal information; and
- Access controls, as defined in the Sesa Group Information Security Standards, shall be applicable at all points from where personal information is accessible.

3.10.3 Physical Access Controls

- Sesa Group shall provide adequate protection to its information systems containing any personal information and facilities against unauthorized physical access and environmental threats using measures as described in Sesa Group Information Security Standards;
- Hard copy of any form or any other document containing any personal information shall be secured physically by adopting adequate security measures as described in Sesa Group Information Security Standards; and
- Sesa Group shall log and monitor access areas hosting personal information. Any attempted breach and unauthorized destruction of information shall be dealt with in accordance with Section 1.7 Consequence Management for Non-Compliance.

3.10.4 Environmental Safeguard

Privacy of personal information of any information provider shall be ensured, even at the time of disaster. Business continuity and disaster recovery plans shall be updated to ensure privacy of personal information in such an event.

3.10.5 Transmitted Personal Information

All personal information transmitted to external networks shall be transmitted through secure lines. Any remote access to Sesa Group systems containing personal information shall be according to the Sesa Group Information Security Standards.

3.10.6 Personal Information on Portable Media

- Personal information shall not be stored on portable media or device unless it is required by business. Even if required, an approval shall be taken from the business head and the DPO. If it is stored, care should be taken to mitigate the risk of its leakage by encrypting it and protecting it using password; and
- Mechanisms shall be defined by each business to report loss of media containing personal information and ensure timely documentation of all such incidents. In case of loss of media, business, in consultation with PST and PT shall take mitigating steps to minimize the risk arising from any such incident. To proactively prevent future occurrence of similar incidents, all such incidents shall be investigated and action points from such investigation acted upon.

3.10.7 Transmission of Physical Media

- Avoid printing Restricted Use data unless absolutely necessary.
- Use care when printing to ensure the paper copies are not left unattended on printers.
- Requirements for the creation of digital media are described in the Storing section of this document.
- Ensure mailings are addressed carefully and sent in sealed envelopes.

3.10.8 Electronic Transmission (Email, Fax, websites, cloud storage, etc.)

- Encryption should be used during transmission whenever possible.
- Restricted Use data must be encrypted during transmission.
- Use the secure email service available from IS&T to email Restricted Use data.
- Avoid faxing Restricted Use data unless necessary.
- Use care to ensure the paper copies are not left unattended when using fax machines.
- Compensating controls must be formally documented and an exception approved by Information Security.
- The transfer of the record from one system or one party to another should be kept showing a data flow of where the data was, where the data resides, and the contents of the record. This management of metadata is useful for tracking and managing data in the future and for assuring that data is being handled properly. The transfer system should give a verbose audit facility that can be monitored to ensure reports for the governance of record management.

3.11 PII sharing, Transfer and Disclosure

Data is not stored or transferred outside India. However, it is transferred to entities for processing as part of legal requirement or fulfilment of contract (e.g. payment to vendors, payment of salaries, payment of taxes, GST etc.). Such transfers are recorded in the Record for processing activities.

3.11.1. Disclosure to Third Parties

Any information shared with the third parties shall be shared only after obtaining explicit or implicit consent from the information provider. Additionally, Sesa Group shall ensure that the third-party adheres to all applicable privacy principles and regulations.

Following points shall be kept in mind while disclosing personal information to the third parties or any other agencies:

- Business functions shall disclose the personal information to Government agencies only after verifying that such agencies are lawfully authorized to seek such information. Further, all such requests shall be obtained in writing clearly mentioning the purposes and the powers of such agencies to seek personal information from Sesa Group;
- Personal information shall be disclosed to third parties of Sesa Group on need basis only for the purpose of executing business. Further, business function shall ensure that all such third parties have signed a Non-Disclosure Agreement (NDA) with Sesa Group to ensure privacy of personal information of information providers. Also, the contracts with such third parties shall be updated to include a clause on privacy of personal information of Sesa Group's information providers available with them; and
- Business functions shall document the nature and extent of personal information disclosed to the third parties.

4. Privacy Training & Awareness

Sesa Group shall formalize a privacy awareness and training program to address the continuous training of all the personnel involved in handling the PI/SPI, including employees, contractors and individuals.

5. Monitoring & Enforcement

Sesa Group shall incessantly monitor the compliance of employees, third parties and other direct stakeholders with this policy and shall address privacy related complaints, queries and disputes appropriately.

5.1 Inquiry, Complaint and Dispute Process

5.1.1. The steps to contact Sesa Group management in case of privacy related complaint or queries shall be clearly defined and also be published on Sesa Group's official website;

5.1.2. It is the duty of all employees and third parties of Sesa Group to cooperate with DPO for effective and timely resolution of information provider's complaints and queries;

5.1.3. The information provider shall be intimated of any breach of personal information with all relevant details as per the last communication address shared by the information provider;

5.1.4. All complaints and queries shall be periodically reviewed to ensure their timely resolution (within 60 days) and the unresolved disputes and complaints, pending for more than 60 days, shall be reviewed by DPO for appropriate resolution.

5.1.5. It shall be ensured by the DPO that all complaints and queries are resolved within 60 days; and

5.1.6. Information provider's complaints records shall be periodically reviewed by the DPO to identify trends and Sesa Group Data Privacy Policy and relevant processes shall be updated to address those specific issues.

5.2 Compliance Review

5.2.1. Annual reviews shall be carried out by the Privacy Expert to ensure organization's compliance with Sesa Group Data Privacy Policy, other privacy procedures, applicable data privacy laws and regulations and privacy standards adopted (if any); and

5.2.2. Management shall address the vulnerabilities, cited in the annual review, in a timely manner and it shall be the responsibility of ITSC to ensure remedial controls are implemented at the earliest to prevent any information privacy related incidents;

5.3 Ongoing Monitoring

5.3.1. Employees and third parties shall inform DPO if they observe any privacy vulnerability or security breach; and

5.3.2. If an employee is leaving the organization, his access to the personal information shall be immediately revoked & Whenever an employee's roles and responsibilities change, his access to personal information shall be reviewed.

6. Data and Privacy Protection Guidelines

- Employees shall understand business/contractual requirements of data protection from their respective Managers or HOD
- Employees shall classify information assets according to their level of sensitivity and handle the same accordingly
- Employees shall protect vital physical records which contain business related information
- Employees shall take a backup of their data (mails, personal folders etc.) on a regular basis
- Privacy shall be ensured in relevant legislation, regulations and if necessary, shall be included in the contractual documented information.
- Security controls shall be implemented to protect any kind of Company's information including PII.
- User awareness training shall be conducted to communicate applicable data protection laws and organization policies and procedures.
- Employees shall not send business data related to the department or any third party without approval of their respective HOD and the consent of the data principal.
- Employees shall not use camera mobile phones in secured areas like server rooms/datacenter
- Employees shall not leave confidential documented information on the desk; instead, it should be kept in a locked cabinet

7. Roles, Responsibilities and Authorities

7.1 Privacy Grievance Officer (PGO)

- Manage overall discrepancies and grievances reported by information providers as per the Data Governance & Privacy Policy.
- Ensure compliance with applicable laws and regulations with regard to resolution of complaints and queries of information providers.
- Undertake preliminary investigation, if required, for determining the reason for the grievance reported; assess type, seriousness and impact of the grievance; and assign responsibility for resolution.
- Ensure that the resolution team members understand their roles and are aware of the process for resolution of grievances.
- Co-ordinate with the members of resolution teams to ensure timely resolution of the grievance (within one month of being reported).
- Take adequate steps, including reporting to DPO, in case of delay in resolution of the complaints.
- Ensure that the grievance/ incident is recorded or documented for future reference with adequate information regarding parameters like detection, immediate correction, investigation procedure, results, resolution action and details of the notification given to the customer.
- Conduct periodic reviews of the grievances to determine patterns, if any, and identifying the root cause. Also, take adequate steps to address the root causes identified, including but not limited to identification of systemic deficiencies in policies, rules & regulations, procedures etc. and
- Communicate the action taken for resolution of grievance to the complainant.
- Authority to approve Data Governance & Privacy Policy.

- Authority to approve deviations, if any to the Data Governance & Privacy Policy.
  Note: Currently CITO is undertaking the role of PGO.

7.2 Data Protection Officer

- Protect the data based on data classification not covered within prevailing standard and procedures
- Adhere to controls towards protection and access to data, provide guidelines for access provisioning and revocation
- Perform due diligence while creation of data to ensure correctness, completeness and validity of entered data.
- Enter data into Company's use through authorized means and software
- Adhere to Company's security policy, standard, procedures and guidelines
- Be held responsible for security of the data handled by them
- Exercise due care while accessing sensitive information (Secret or Confidential Data) and securing them from unauthorized use, disclosure, alteration or destruction
- Comply with the protection requirements defined in the Vedanta Information Security Standard
- Ensure data security, integrity, accuracy and consistency across various platforms as prescribed by data owner
- Highlight significant issues to Data Owner and Data Governance working group
- Authority to take actions to strengthen privacy and resilience at Sesa Goa.
- Delegating authority for enforcing the organization's privacy policies.
  Note: Currently CISO is undertaking the role of DPO.

7.3 Entity Privacy Officer (EPO) for each entity – IOB, Facor, VGCB

- Appointment of data protection champions for their functions and assign roles & responsibilities.
- Ensure information classification, labelling & handling.
- Facilitate review of DFD (Data Flow Diagram) & Identification of sensitive key words
- Facilitate review of risk assessment and risk treatment plan.
- Facilitate review of DPIA (Data Protection Impact Assessment) & ROPA (Record of Processing Activities)
- Respond to data subject access rights in a timely manner in consultation with the DPO.
- SPOC for all data & privacy breaches in the respective entities.
- Ensure non-disclosure agreement has to be signed from all the concerned third parties.
- Create awareness of data governance & privacy in their respective entities.
- Review of access rights for electronic & physical records
- Review of users who have access to secure area/record rooms etc.
- Define all applications data owners in their respective entities (If any).
- Ensure implementation of clear desk/clear screen policy.
- Responsible for compliance of data governance & privacy policies/procedures in respective entities.
- Authority to take actions to strengthen and enforce privacy and privacy related regulations at Sesa Goa

7.4 Data Protection Champions (from Each function – HR, Finance, Marketing, IT, Commercial and Secretarial)

- Facilitate to carry out information classification and labelling & handling.
- Facilitate to carry out risk Assessment and prepare a risk treatment plan

- Create awareness of data governance & privacy framework including responding to data subject request in their functions.
- Initiate access rights review for electronic & physical records
- Create list of users who have access to secure area/record rooms etc.
- To create DFD (Data flow diagrams) & identification of sensitive key words with help of DPO
- To create DPIA (Data Protection Impact Assessment) & ROPA (Record of Processing Activities) with help of DPO.
- To inform DPO & EPO regarding any data breach.
- To take consent & provide notices from end users.
- Identify all the vendors where personal & sensitive information shared.
- To ensure non-disclosure agreement with all third parties in their functions.
- Implement privacy by design concept in applications/process.
- To coordinate the compliance of data governance & privacy policies applicable to their functions.
- Participate in the data governance & privacy audits.
- Formulate & ensure implementation of the CCA (Correction and corrective action)
- Authority to take necessary actions such as awareness trainings, conduct Privacy Impact Assessments for any new processes or changes in processes in their scope.

7.5 Role-IT Department

- Ensure data is created, stored and controlled in authorized systems and is in alignment with Vedanta Information Security Standard
- Maintain data security and audit trail (where applicable), where required, across the applications in use by departments
- For the reported / noted incidents; perform root cause analysis, discuss the exceptions with Data Owners and drive the closure of action plans
- Ensure availability, accuracy and consistency of data
- Partner with Data Custodians and Owners for any data issues
- Maintain secure storage of data, based on classification
- Design and maintain infrastructure to create, process, store, utilize and distribute data in a secured manner

NOTE: All roles mentioned above are not mandatory for all kinds of data and in all kinds of scenarios.

8. Policy Communication

Sesa Group Data Privacy Policy shall be made readily available to all the employees of Sesa Group and its associated entities.

- The policy shall be hosted on the intranet for easy reference by employees;
- The policy shall be enforced by the DPO, through regular information privacy related training and awareness campaigns; and
- Trainings shall be conducted for the employees on their roles and responsibilities towards ensuring privacy of personal information on an annual basis.

9. Enforcement

- All employees and third-party staff shall be required to comply with the Sesa Group Data Privacy Policy.
- Non-compliance with Sesa Group Data Privacy Policy shall lead to disciplinary action. The relevant HR processes shall be invoked for carrying out the disciplinary action.
- Actions will be taken as per Sesa Group Data Governance Policy & framework.

10. Policy References

- ISO/IEC 27701:2019

Annexure Details

a. Privacy Notice for Employees (**File name-** Privacy Notice for Employees v2.0)
b. Privacy notice for Website (**File name-** Privacy notice for Website v3.0)
c. PIA Template (**File name –** PIA Template v 2.0)
d. Privacy Impact Analysis Guideline (**File name –** Privacy Impact Analysis Guideline v 2.0)
e. Data Protection Addendum Agreement (**File name** – Data Protection Addendum Agreement v2.0).
f. Records of Processing Activities Template (**File name** - Records of Processing Activities v 2.0)
g. Consent Process (**File name-** Consent process v 2.0)