Table of Contents

1 Introduction

The protection of personal data is important to us. Laurus Labs Limited (Hereafter refereed as Laurus Labs or Organisation) is committed to conducting its business in accordance with applicable data protection regulations, and in line with the highest standards of ethical conduct. This Privacy Policy ("Policy") sets forth the organizational intent and data protection principles which shall be followed by all Laurus Labs entities in its processing and protection of personal data.

2 Applicability

This Policy applies to all associates of the Company that collect and/or process PI/SPI (including PI/SPI of EU residents and citizens). Processing of PI/SPI includes any operation which is performed upon PI/SPI, such as collecting, recording, organizing, storing, adapting, or altering, retrieving, consulting, using, transferring, disclosing through transmission, disseminating or otherwise making available, aligning or combining, blocking, erasing or destroying.

Laurus Labs is the data processor over PI/SPI that it processes for its data controller, as Laurus Labs will be acting on the instructions of the controller in relation to PI/SPI.

3 Purpose

This Policy defines requirements to help ensure compliance with laws and regulations applicable to Laurus Labs' collection, storage, use, transmission, disclosure to third parties and retention of Personal and sensitive personal data.

4 Definitions

Data Subject - means a natural person is an individual who is the subject of certain personal information or whose information is being collected.

Associate means an employee, officer, director, third party, contractual employees, intern, job – candidate, end customer or any representative of the Company.

Personal information (PI) - means any information relating to an identified or identifiable living person ('data subject'). An identifiable living person is one who can be identified, directly or indirectly, from the data items. In particular using a common identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data/ Sensitive Personal Information (SPI)- personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

Breach- a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed

Processing – means any operation or set of operations which is performed on personal information or on sets of personal information, whether or not by automated means, such as collection,

recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, combination, restriction, erasure or destruction

Profiling - means any form of automated processing of personal information consisting of the use of personal information to evaluate certain personal aspects relating to a person, in particular to analyze or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Data Controller - means individual, company, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal information. In some cases, the purpose and means of processing are determined by Union or Member State law.

Data Processor - in relation to personal information, means any person (other than an employee of the Data Controller) who processes the personal information on behalf of the data controller.

Disclosure - means rendering personal information accessible, for example by allowing access to personal information either transferring, distributing, or publishing the personal information.

Data Subject Right - any request received by the firm from a Data Subject or other individual or legal entity who wishes to receive a copy of all the personal information related to it or him the firm is processing about it/him.

European Economic Area (EEA) - the European Union plus Norway, Liechtenstein and Iceland.

Personal profile - means a collection of data that allows the appraisal of fundamental characteristics of the personality of an individual.

Consent - of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, through a statement or using a clear affirmative action, signify agreement to the specific processing of personal information relating to them.

Third party- means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal information

Cross-border processing- means either:

(a) processing of personal information which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(b) Processing of personal information which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

5 Consequence of Non-Compliance

Non-compliance to the mandatory requirement of Privacy may potentially lead to regulatory penalties (if applicable). Thus, it is imperative that the organization abides by all the key requirements of the regulation.

Notwithstanding the above regulatory requirement, HR disciplinary process will be followed.

6 Unanticipated situations

This policy does not anticipate every situation that may arise within Laurus Labs. Therefore, all users are encouraged to carefully consider the actions they take and to contact the DPO if they have any questions, concerns or suggestions relating to this policy.

7 Privacy statement

Laurus Labs' Privacy Policy ("Policy") establishes organization-wide principles and minimum standards designed to mitigate privacy risks. Under this Policy, each operation is required to build and maintain controls over the collection, use, and protection of PI/SPI in order to comply with this Policy and any applicable privacy laws or regulations (including GDPR requirements). Laurus Labs operations processing PI/SPI initially collected in another country, may also be required to comply with the laws and regulations of the country where the PI/SPI was collected. Furthermore, Laurus Labs has many contractual agreements that may impose obligations on the company to protect certain sets of data, including PI/SPI. Failure to comply with applicable legal requirements may damage Laurus Labs reputation and expose the company to legal and regulatory liabilities, including fines and lawsuits.

8 Privacy Management

Data Privacy Policy aligns with Generally Accepted Privacy Principles. In view of the changing legislative and technological environment for data privacy, the Data Privacy Policy will undergo revisions. The guiding privacy principles articulated in this policy document are as follows:

8.1 Management

- A Data Privacy Policy shall be developed and maintained to document the privacy principles and practices followed by Laurus Labs.
- A privacy organization shall be defined for governance of data privacy initiatives.
- A Data Protection Officer (DPO) shall be appointed to process complaints and requests for information related to Laurus Labs privacy practices.
- Establish procedures for the identification and classification of personal information.
- The Privacy Policy statement shall be made available on the internal portal.
- The Data Privacy Policy shall be communicated to the internal personnel.
- Procedures shall be established for disciplinary and remedial action for violations of the Data Privacy Policy.
- Changes or updates to the Data Privacy Policy shall be communicated to all internal personnel when the changes become effective.
- Establish procedures for performing mandatory registration with regulatory bodies.
- Risk Assessment is to be carried out on a periodic basis to ensure risks to personal information are identified and mitigated.
- The potential impact on data privacy is assessed when new processes involving personal information are implemented, or when significant changes are made to such processes.

8.2 Notice and consent

- Notice: Prior to collecting PI/SPI from the associates, the Company will notify the latter about the Company (as applicable) privacy policies and practices, purposes of collecting PI/SPI, usage, retention and disclosure, the contacts details of the Data Protection Officer (DPO) and, including information on how to contact the same.

- Choice and Consent: Prior to collecting PI/SPI from the associates, the Company will obtain an explicit consent from the latter.
  Although Laurus Labs operates in the capacity of a data processor, wherein Laurus Labs is not responsible for obtaining consent or providing notices. However, the principle of notice and consent will be applicable if Laurus Labs is involved in collection of the PI/SPI (including PI/SPI of EU residents and citizens) directly from the data subjects/associates. In such circumstances Laurus Labs should ensure the following:
  - Provide associates, as applicable, with a privacy notice before or during the collection of PI/SPI, and at any other time as prescribed by applicable law and update relevant privacy notices if the business changes the manner in which PI/SPI is used, shared, or processed. The privacy team must draft, review, and approve the language of any privacy notice prior to its use.
  - Obtain consents from associates, in a manner and form required by applicable law, before processing PI/SPI, using PI/SPI in a manner that is inconsistent with any privacy notice previously provided, and/or marketing Laurus Labs goods or services.
  - Stop processing an individual's PI/SPI within the time required by applicable local law if the individual withdraws consent or objects to the processing.
  - Provide associates with access to their PI/SPI for review and update, which may include maintaining an easy and secure way for individuals to contact Laurus Labs, obtain copies of their records, and submit requests to modify, update, or erase their PI/SPI. All individual requests should be fulfilled within the time period required by applicable local law.

8.3 Collection Limitation

The Company will collect PI/SPI of the associates limited to the purposes identified in the notice, furthermore, any such information shall be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the end customer or associate concerned.

Additionally, the company will follow the principle of data minimization and will collect limited and relevant PI/SPI in relation to the purpose for which they are processed.

8.4 Use Limitation

PI/SPI of associates will not be made available or otherwise used for any purpose other than what was agreed with that individual at the time of data collection.

8.5 Access

Associates will be given access to his/ her PI/SPI that the Company has gathered or stored in its systems (if required), and he/she will be provided with an opportunity to correct his/her PI/SPI thereby assuring the associates that their PI/SPI is accurate. Laurus Labs will erase, rectify, complete, or amend the PI/SPI to a justified request.

Associates or Data Controller (e.g. Laurus Labs. -on behalf of data subjects) may request Laurus Labs to review, correct, update, suppress, or otherwise modify any of PI/SPI of the data subjects. All such requests will be routed through the Data Protection Officer. The privacy manager in consultation with the DPO and respective line of businesses will support the closure of the request.

8.6 Security

The Company will protect PI/SPI that it handles, with appropriate technical and organizational safeguards for security, against threats (internal and external security threats), such as loss of

confidentiality, integrity, unauthorized destruction, usage, or other misuses. To protect against the risk that PI/SPI may be compromised by internal and external security threats, the company relies on information protection safeguards:

- Technical safeguards-Firewalls, antivirus, logs, encryption, pseudonymization etc.
- Administrative safeguards -IT security policies and standards, incident management procedure, trainings etc.
- Physical safeguards- CCTV cameras, employee ID badges, access controls etc.

8.7 Disclosure to Third Party

The Company will disclose PI of the associates to a third party only for the purposes identified in the notice and only with the explicit consent of that associates. This may require Laurus Labs to transfer the PI/SPI to countries other than where it operates. For every new engagement with a third party or renewal of existing engagement where the PI/SPI is disclosed to third party, the following must be ensured:

- Procurement team to evaluate risk exposure of all third parties
- Initial due diligence to be conducted by procurement
- Include privacy and data protection provisions in the agreement

Additionally, ongoing due diligence process should be in place for third parties handling PI/SPI of associates (including PI of EU residents/citizens)

8.8 Transparency

The Company will adapt to a general policy of transparency about developments, practices and policies with respect to the PI/SPI.

8.9 Accuracy

The Company will keep the PI/SPI as accurate, complete and up-to date as is necessary for the purpose for which it is processed; and provide appropriate channels for the same.

8.10 Retention and disposal

The Company will retain the PI/SPI in a form that permits identification for no longer than as necessary for the fulfilment of the stated purpose. Also, Laurus Labs will retain and use associates PI/SPI as necessary to comply with the legal obligations, resolve disputes, and enforce our agreement, post which it will be disposed securely.

Each Laurus Labs operation must have policies, procedures, and internal controls in place to comply with recordkeeping requirements established by applicable privacy laws and regulations. Records maintained should, at a minimum, include those relating to data protection impact assessments, privacy notices, consents, privacy complaints, third party relationships (including all due diligence performed on the third party), cross-border data transfers (including any data transfer agreements or other valid transfer mechanism), and any regulatory or customer notification related to a data breach. All such records and supporting documentation must be maintained in an auditable manner and readily retrievable for a period as defined in the Data Retention Standard and Record and Information Management policy of Laurus Labs

8.11 Accountability

The Company shall be accountable to comply with measures that give effect to the principles stated above. Laurus Labs understands its accountability for PI/SPI under its control as a data processor; accordingly, it will

- Have appropriate instructions, guidelines and other measures to be able to demonstrate that the processing of PI/SPI is performed in compliance with this policy, or PI/SPI is managed in compliance with this policy
- Designate individual or individuals who are accountable for Laurus Labs's compliance with the privacy principles
- Ensure the availability of required policies, procedures and contacts for management of PI/SPI; these being reviewed at a minimum annually or as and when there is a change warranted.

8.12 Cross Border Data Transfer

When conducting business, working on Company projects, or implementing new processes or systems, Laurus Labs may require the transfer of PI/SPI to other Laurus Labs entities or third parties that are located outside of the Laurus Labs country of business.

Laurus Labs shall develop a standardized approach for protection of data moving across borders. Laurus Labs will adopt appropriate technical and administrative controls that apply well to cross border data flows to act as an accountability framework for information management as a whole and including natural checkpoints for each step of international transfer.

8.13 Privacy Monitoring and Enforcement

- Procedures shall be established for recording and responding to complaints/ grievances registered by data subjects.
- Each complaint regarding privacy practices registered by data subjects shall be validated, responses documented and communicated to the individual.
- Annual privacy compliance review shall be performed for identified business processes and their supporting applications.
- A record shall be maintained of non-compliances identified in the annual privacy reviews. Corrective and disciplinary measures shall be initiated and tracked to closure, guided by Laurus Labs management.
- Procedures shall be established to monitor the effectiveness of controls for personal information and for ensuring corrective actions, as required.
- Any conflicts or disagreements relating to the requirements under this policy or associated privacy practices shall be referred to the Data Privacy Officer for resolution.

9 Privacy Incident Management

Privacy incident management establishes requirements for monitoring and responding to PI/SPI potential privacy incidents.

The Company establishes requirements for monitoring and responding to PI/SPI potential privacy incidents in accordance to policy requirements and assist associates in understanding their roles and responsibilities in addressing privacy incidents. Privacy incident management covers:

- Associates should be able to detect and report a privacy incident as it occurs within the operational infrastructure and results in deviations from normal services.
- Privacy team in consultation with the Data Protection Officer will regularly update all associates over privacy incidents and breaches happening across the globe and their relevance at the company environment, by means of privacy trainings, emails, posters etc.

- All the privacy incidents shall be reported to DPO through mail ID dpo@lauruslabs.com.
- All privacy incidents shall be recorded and tracked.

10 Privacy Assessment

10.1 PI inventory and Data Protection Impact Assessment

As Laurus Labs is processing a lot of PI/SPI (including PI/SPI of EU residents and citizens) and as technology continues to evolve, it is vital that the Company find ways to integrate privacy into the design phase of projects. PI inventory and Data protection impact assessments have become an essential component of privacy compliance programs. Laurus Labs will prepare PI inventory and conduct DPIA for the privacy related risks applicable to Laurus Labs.

Laurus Labs will adopt the following approach:

- Identify relevant processes and support functions.
- Prepare Personal Information Inventory and roll out DPIA questionnaire.
- Identify the risks and develop mitigation strategies; and
- Monitor closure of identified actions.

The DPO will coordinate with the relevant business processes and support functions to ensure that PII inventorization and DPIA is conducted as per the defined methodology.

11 Communication and Training

Laurus Labs will ensure adequate awareness of data privacy, its importance and implications, through a targeted and relevant training program to all its associates to reduce the risk of a privacy breach. The DPO will monitor that all employees and the relevant associates processing PI/SPI undergo the privacy awareness program as per defined policies and procedures.

12 Exceptions

Any exception to this standard will be in line with the documented and approved Exception process and/ or IT exception procedure.

13 Review and Evaluation

The Laurus Labs privacy policy shall be reviewed at the time of any major change(s) in the existing environment affecting privacy policies and procedures or once every year, whichever is earlier. This document shall be reviewed by the Manager, Privacy in consultation with the DPO and will be approved by the Executive Director.