Langslide

Anonymization and Pseudonymization Policy

Version 1.0

PURPOSE

Rudramsa Systems Pvt. Ltd. (herein referred to as organization) is committed to protecting the privacy and security of your personal information. This Anonymization and Pseudonymization Policy ("Policy") seeks to provide all personnel and employees who use, collect, process, or store Personal Data with guidance to safeguard the confidentiality, integrity, and availability of information, systems, and data. This Policy also aims to provide and apply anonymization or pseudonymization techniques to help protect personal and sensitive data.

SCOPE

The Policy applies to all employees, workers, members of staff, and contractors who receive, handle, or process Personal Data during their employment. It applies to processing Personal Data collected from our customers (end users), employees, business partners, and other third parties. This Policy applies whenever employees and third parties engage in the anonymization and pseudonymization of personal information. When doing so, you must abide by the process and principles set out in the Policy.

DEFINITIONS

- Controller shall mean the party responsible for determining the purposes and means of processing the Personal Data.
- Data Privacy Officer means, where applicable, an individual or individuals who are responsible for the protection of Personal Data at the organization.
- Data Subject means a natural person whose Personal Data is processed by a controller or processor.
- Personal Data Breach means 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.
- Personal Data shall include any information relating to an identified or identifiable natural person.
- Processor shall mean the party that processes Personal Data on behalf of the Controller.
- Processing includes any operation performed on Personal Data, whether or not by automated means, including collection, use, recording, etc.
- Regulations shall mean EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, The California Consumer Privacy Act of 2018 (CCPA).
- **Supervisory Authority** shall have the meaning assigned to it under the GDPR.
- **Pseudonymization** means processing personal data so that it can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
- **Anonymization** means processing personal data to irreversibly prevent the identification of the individual to whom it relates. Data can be considered anonymized when it does not allow identification of the individuals to whom it relates and when it is not possible for an individual to be identified from the data by any further processing of that same data or by processing that same data together with other data that is available or likely to be available. For most companies, complete anonymization is not feasible.

ROLES AND RESPONSIBILITIES

The Privacy Officer is responsible for ensuring that appropriate security measures are taken to protect Personal Data. The DPO will ensure that proper measures are developed, implemented, followed, and enforced to ensure anonymization and

pseudonymization.

All employees working for the organization are responsible for ensuring that all information is pseudonymized and anonymized wherever identifiers are not required to use Personal Data.

Pseudonymizing and Anonymizing Personal Data

Chief Information Security Officer (CISO) must decide if pseudonymization and anonymization techniques are appropriate for particular data processing activities. Chief Information Security Officer (CISO) is responsible for choosing the most suitable technology and implementing these techniques. Below is a non-exhaustive list of techniques for anonymization and pseudonymization.

Anonymization

The purpose of anonymizing personal data is to make it impossible to identify an individual in the anonymized data set, even with the aid of the original data. Thus, anonymized data is not considered personal data. It is important to note that there is no prescriptive standard for anonymization within EU legal frameworks. Hence, choosing appropriate anonymization methods rests with the Data Protection Officer.

The company will use the following methods, considering the degree of risk and the intended use of the data.

- **Directory replacement –** Modifying the name of individuals integrated within the data while maintaining consistency between values, such as "postcode + city" and "age + gender."
- **Scrambling** involves mixing or obfuscating letters. The process can sometimes be reversible. For example, Robert could become Betror.
- **Masking –** Allows a part of the data to be hidden with random characters or other data.
- **Blurring –** An approximation of data values to render their meaning obsolete and/or render the identification of individuals impossible.
- **Differential privacy –** This method might be used whenever the Company gives a third party access to an anonymized data set. A copy of the original data remains with the Company, and the third-party recipient only receives an anonymous data set.
- **Aggregation –** A data subject is grouped with several other data subjects sharing personal data.

Pseudonymization

Pseudonymizing enhances privacy by replacing identifying fields within a data record with one or more artificial identifiers or pseudonyms. As such, pseudonymization reduces, but does not entirely remove, the ability to link a dataset with the identity of a data subject.

The Data Protection Officer, together with the Chief Information Security Officer (CISO), will establish the appropriate pseudonymization methods such as:

- **Encryption (using a secret key) –** Data is encrypted using a secret key. The secret key holder can easily re-identify data subjects by decrypting the data set.
- **Hash functions –** Used to map data of any size to fixed-size codes (note that multiple hashing techniques exist (e.g., salted hashes, keyed hashes, etc.).
- **Tokenization** is a process for substituting a sensitive data element with a non-sensitive equivalent, referred to as a token. The token is a reference (i.e., identifier) that maps back to the sensitive data through a tokenization system. The tokenization system provides data processing applications with the authority and interfaces to request tokens or detokenize back to sensitive data.

ENFORCEMENT

An employee's violation of the above procedure or any provisions shall invite disciplinary action. Any personnel found to have violated the Policy may be subject to disciplinary actions, including termination of employment and applicable penalties.

MONITORING AND REVIEW

The Privacy Officer will monitor and review this policy every three years or when changes to the applicable Regulations occur.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Mar 14 2026	Initial Release	Pronoy	Kartikeya	Kartikeya