Data Retention Policy

Purpose

The purpose of this policy is to specify SEDNA's guidelines for retaining different types of data, and to ensure that records that are no longer needed are discarded at the proper time.

Note that the need to retain certain information can be mandated by country specific requirements, industry regulations, applicable law and compliance with General Data Protection Regulations (“GDPR”). Where this policy differs from applicable regulations, the regulations specified in applicable law will apply.

Scope

This policy applies to all company data stored on company-owned, company-leased, and otherwise company-provided systems and media, regardless of location, as well as physical records.

Reasons for Data Retention

The company does not wish to simply adopt a "save everything" approach. Some data, however, must be retained in order to protect the company's interests, preserve evidence and generally conform to good business practices. Some reasons for data retention include:

- Business operations and strategic planning;
- Performance of service offerings to comply with contractual obligations;
- Trade, service and warranty cycles;
- Billing and account maintenance;
- Profile and predictive analytics;
- Intellectual property preservation;
- Security incident investigation and dispute resolution; and
- Regulatory requirements and compliance with legal obligations.

If any information retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained.

Data Destruction

Personal data will be destroyed in accordance with secure destruction arrangements and the Data Retention Schedule found as an appendix to this policy. All copies of personal data will be either anonymized for profiling, predictive analysis and statistical reporting, or destroyed appropriately and securely. When SEDNA destroys data upon instruction from the customer, we will provide confirmation and documentation to the customer, subject to local law requirements and blocking and security and back-up obligations. If local law prevents us from destroying all or part of the data, we will inform the customer and warrant that the data will remain confidential.

Storage

SEDNA uses Amazon AWS servers for data storage and hosting. The specific cloud services we use are in line with the legal requirements set out in applicable law. We also employ security and encryption methods to protect the data, both while in transit and at rest.

When processing personal data, we use processes and tools that integrate privacy from their inception (privacy-by-design), and perform privacy impact assessments as required by applicable law.

SEDNA will seek to store as few copies of the same documentation and data as possible. The location of data and storage will comply with the GDPR.

Third Party Data Sharing

Where data is shared with third parties, we will ensure that these third-party vendors follow our Data Retention Policy. This will be enforced through legally binding contracts.

Exceptions

For personal data, there are the following exceptions to this policy:

- Where consent is required for the storage and processing of data, the withdrawal of consent means that the data will be erased and/or processing will cease.
- Where data or documentation needs to be retained for establishment or defence of legal claims.
- Where data or documents needs to be retained to comply with applicable laws.

Enforcement

This policy will be enforced by the DPO, if any, and/or the company management team. Violations may result in disciplinary action up to and including termination of employment. Where unlawful

activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

Last updated: Feb 1, 2024

Appendix A - Data Retention Schedule

Record Type	Retention Period
Customer Data - including Personally Identifiable Information (PII)	7 years after end of customer relationship
Employee Personal Data	7 years after end of employment
Employee Contracts	7 years after end of employment
Planning Data	7 years
Health and Safety	7 years
Public Data	3 years
Operational Data	Current year plus 7 years, or longer if required for legitimate business reasons.
Call Centre Records:	2 years after current year
Critical Data including Revenue, Tax and VAT	7 years after current year
Confidential Data:	7 years
Data Breach Records	2 years after incident resolution, or longer if required to meet business obligations.