DATA PROCESSING AGREEMENT (DPA)

SvereSystems

Last updated: March 2026

This Data Processing Agreement ("DPA") forms part of the Terms of Service and governs how SvereSystems processes personal data on behalf of its customers where SvereSystems acts as a **processor** under applicable data protection law, including the EU General Data Protection Regulation ("GDPR"). For the purposes of this DPA, the Processor is **Sveresa tmi (Y-tunnus 3592316-3), Finland**, operating under the brand **SvereSystems**.

---

1. Parties and incorporation

This Data Processing Agreement ("DPA") is between:

- the customer that has entered into the SvereSystems Terms of Service or another relevant agreement ("Controller"), and
- **Sveresa tmi (Y-tunnus 3592316-3), Finland**, operating under the brand **SvereSystems** ("Processor").

This DPA forms an integral part of the **Terms of Service** or other applicable main agreement (the "Main Agreement"). In case of conflict between this DPA and the Main Agreement regarding data protection, this DPA shall prevail to the extent of the conflict.

2. Subject matter and duration

This DPA governs the Processor's processing of personal data on behalf of the Controller in connection with the provision of the SvereSystems Service where the Processor processes personal data for the Controller.

The duration of this DPA is the same as the duration of the Main Agreement. It applies for as long as the Processor processes personal data on behalf of the Controller and continues to apply to any post-termination obligations described in this DPA.

3. Nature and purpose of processing

The Processor processes personal data only to provide, maintain, secure, and support the Service and to perform its obligations under the Main Agreement, including:

- hosting, storing, and organising lead, contact, and account data;
- enriching contact data where applicable;
- enabling communication and outreach workflows configured by the Controller;
- providing customer support and troubleshooting;
- performing security, logging, and usage monitoring in connection with the Service.

Processing may include the operations listed in Article 4(2) GDPR, such as collection, recording, organisation, storage, adaptation, retrieval, consultation, use, disclosure, erasure, and destruction, to

the extent necessary for the Service.

4. Categories of data and data subjects

The types of personal data processed may include, depending on how the Controller uses the Service:

- identification and contact details (such as name, email address, job title);
- business-related information (such as company name, role, industry, website);
- communication data and notes created by the Controller in the Service;
- usage and log data associated with users of the Controller's account;
- other personal data uploaded or entered into the Service by the Controller at its discretion.

The categories of data subjects may include:

- the Controller's leads, prospects, and customers;
- employees, contractors, or representatives of the Controller;
- other individuals whose data is entered into the Service by or on behalf of the Controller.

The Service is not intended for processing special categories of data under Article 9 GDPR (for example health data, political opinions, or similar sensitive data) or data relating to criminal convictions. The Controller shall not intentionally use the Service for such data.

5. Controller obligations

The Controller is responsible for:

- ensuring that it has a valid legal basis for all personal data processed via the Service;
- providing appropriate privacy notices to data subjects where required;
- ensuring that instructions provided to the Processor are lawful and consistent with the Main Agreement and this DPA;
- configuring the Service in a privacy-compliant manner, including respecting opt-outs and marketing preferences where applicable;
- cooperating with the Processor to maintain security and confidentiality of personal data.

6. Processor obligations

The Processor shall:

- **Process personal data only on documented instructions** from the Controller, including regarding transfers of personal data to a third country, unless required to do so by EU or Member State law; in such a case, the Processor shall inform the Controller of that legal requirement unless the law prohibits such notification.
- **Maintain confidentiality** and ensure that persons authorised to process personal data are subject to a duty of confidentiality.

- **Implement appropriate technical and organisational measures** to protect personal data as described in Section 9 of this DPA and Appendix 2.
- **Assist the Controller**, insofar as possible, in fulfilling the Controller's obligations to respond to data subject requests and to comply with Articles 32-36 GDPR (security, breach notification, DPIAs, and consultations).
- **Inform the Controller** if, in its opinion, an instruction infringes the GDPR or other applicable data protection provisions.
- **Keep records** of processing activities carried out on behalf of the Controller, where required by law.

7. Sub-processors

The Controller grants the Processor a general written authorisation to engage sub-processors to provide the Service. Such sub-processors may include:

- infrastructure and hosting providers, including any underlying white-label SaaS platform provider where applicable;
- content delivery networks (CDNs);
- payment processors;
- analytics and logging providers;
- customer support and communication tools.

The Processor shall:

- ensure that sub-processors are bound by written agreements imposing data protection obligations no less protective than those in this DPA;
- remain responsible for the acts and omissions of sub-processors to the same extent as for its own acts and omissions;
- maintain a list or description of current sub-processor categories and make it reasonably available, for example through its website or upon request.

Where required by law, the Controller may object to a new sub-processor on reasonable grounds relating to data protection. In such a case, the parties will work together in good faith to find a solution. If no solution is possible, the Controller may terminate the affected part of the Service in accordance with the Main Agreement.

8. International transfers

The Processor may process personal data in countries outside the European Economic Area ("EEA"), including through sub-processors that provide infrastructure or supporting services.

Where personal data is transferred outside the EEA or the UK to a country that does not provide an adequate level of data protection as determined by the European Commission, the Processor shall ensure that an appropriate transfer mechanism is in place, such as:

- the use of Standard Contractual Clauses (SCCs); and/or
- other appropriate safeguards permitted under Chapter V of the GDPR.

Further details about international transfers may be provided in the Processor's Privacy Policy or upon reasonable request.

9. Security measures

The Processor shall implement and maintain appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access, taking into account:

- the state of the art;
- the costs of implementation;
- the nature, scope, context, and purposes of processing;
- the risk to the rights and freedoms of natural persons.

Such measures may include, as appropriate:

- use of encrypted connections (HTTPS) for data in transit;
- logical access controls and authentication mechanisms;
- segregation of environments and data where reasonable;
- logging and monitoring to detect unusual activity;
- data backup and recovery procedures;
- security awareness for personnel with access to personal data.

The Controller is responsible for implementing appropriate technical and organisational measures within its own systems and for configuring and using the Service securely.

10. Data subject requests

If the Processor receives a request from a data subject relating to personal data processed on behalf of the Controller, the Processor will, where reasonably possible:

- advise the data subject to direct the request to the Controller; and
- notify the Controller and, where necessary, assist the Controller in responding to the request.

The Controller is responsible for handling and responding to data subject requests, such as rights of access, rectification, erasure, restriction, portability, and objection, in accordance with applicable law.

11. Personal data breaches

In the event of a personal data breach affecting personal data processed on behalf of the Controller, the Processor shall:

- notify the Controller without undue delay once it becomes aware of the breach; and
- provide the Controller with information reasonably required to comply with its legal obligations, including any obligations to notify supervisory authorities or data subjects.

The Processor will cooperate with the Controller to mitigate the effects of the breach and to support any required notifications, taking into account the nature of processing and the information available to the Processor.

12. Audits and compliance information

Upon a reasonable written request and subject to confidentiality, the Processor shall make available to the Controller the information necessary to demonstrate compliance with this DPA and Article 28 GDPR. This may include:

- summaries of security measures and policies;
- responses to reasonable security and privacy questionnaires;
- other documentation that the Processor normally makes available to customers.

Where such documentation is not sufficient, the Controller may, at its own cost and upon reasonable notice, conduct or mandate an audit limited to what is necessary to verify compliance with this DPA. Audits shall:

- be conducted during normal business hours and in a manner that minimises disruption;
- respect the confidentiality of other customers and the Processor's trade secrets;
- take into account any audit reports or third-party certifications already available.

13. Return and deletion of personal data

After the end of the provision of the Services relating to processing, the Processor shall, at the choice of the Controller:

- delete personal data; or
- return personal data to the Controller,

unless Union or Member State law requires storage of such data.

Unless otherwise agreed, the default approach is that personal data is deleted from active systems within a reasonable period after account closure and then from backups in accordance with the Processor's data retention policies and technical constraints.

14. Liability and hierarchy

The limitations of liability and indemnities set out in the Main Agreement apply to this DPA, subject to any mandatory provisions of applicable law.

In the event of a conflict between this DPA and other documents, the following order of precedence shall apply:

- this DPA (with respect to data protection and privacy);
- the Main Agreement (Terms of Service);
- any other agreements between the parties.

15. Governing law and contact

This DPA is governed by the laws of **Finland**, without regard to conflict-of-laws rules. Any disputes arising out of or relating to this DPA shall be resolved in accordance with the dispute resolution provisions set out in the Main Agreement.

If you have questions about this DPA or wish to request a signed enterprise version, you can contact:

- **SvereSystems - Privacy & Legal**
- Processor: **Sveresa tmi (Y-tunnus 3592316-3), Finland**
- Email: info@sveresystems.com

Appendix 1. Processing details (GDPR Article 28)

Subject matter: Provision of the SvereSystems Service where personal data is processed on behalf of the Controller, including lead/contact management, enrichment, outreach workflows, account administration, and related support.

Duration: For the term of the Main Agreement, plus any post-termination periods required for deletion and backup cycles as described in this DPA.

Nature and purpose: Hosting, storage, organisation, enrichment (where applicable), user access management, logging, security, and support.

Types of personal data: Names, business emails, job titles, company and role information, communication notes and metadata, user account and login data, usage/log data.

Categories of data subjects: The Controller's leads/prospects/customers, and the Controller's users (employees/contractors) using the Service.

Special categories: Not intended. The Controller shall not intentionally upload or process special categories of data via the Service.

Appendix 2. Security measures (TOMs)

The Processor maintains appropriate technical and organisational measures, which may include:

- encryption in transit (HTTPS/TLS);
- access control and authentication mechanisms;
- least-privilege access for operational needs;
- logging and monitoring for security events;
- backup and recovery procedures;
- change management and incident response practices.

Note: Specific technical implementation details may evolve over time. The Processor will ensure that measures remain appropriate to the risk and aligned with GDPR Article 32.