



CONTRACTUAL DOCUMENT

Data Processing Agreement

Synost - Thomas Filip Lochet EI - Article 28 GDPR

 VERSION 1.0

Issue date 2026-08-28

Contents

Data Processing Agreement	2
Article 1 - Purpose and framework	2
Article 2 - Term	2
Article 3 - Description of processing	2
Article 4 - Documented instructions	2
Article 5 - Confidentiality	2
Article 6 - Security of processing	3
Article 7 - Sub-processors	3
Article 8 - Data location and transfers outside the European Union	3
Article 9 - Assistance to the Controller	3
Article 10 - Personal data breach	4
Article 11 - Fate of the data on termination	4
Article 12 - Records and documentation	4
Article 13 - Audit	4
Article 14 - Controller obligations	4
Article 15 - Liability	5
Article 16 - Contact point	5
Article 17 - Language	5
Annex 1 - Description of the processing	6
Annex 2 - Authorised sub-processors	7
Annex 3 - Technical and organisational measures	8

Data Processing Agreement

Version 1.0 - effective 28 August 2026

This English version is provided for convenience. The French version prevails in the event of any discrepancy (Article 17).

Entered into between:

- **The Customer**, identified in the Specific Terms, acting as **controller** (the “Controller”);
- **Thomas Filip Lochet, sole trader trading under the name Synost**, 42B rue Victor Hugo, 78330 Fontenay-le-Fleury, France, SIREN 935 212 381, acting as **processor** (“Synost”).

Article 1 - Purpose and framework

1.1. This agreement (the “**DPA**”) sets out the conditions under which Synost processes personal data on behalf of the Controller, in accordance with Article 28 of Regulation (EU) 2016/679 (the “**GDPR**”) and French Law no. 78-17 of 6 January 1978 as amended.

1.2. The DPA forms an integral part of the Agreement. **In the event of any conflict with the General Terms and Conditions of Sale, this DPA prevails** in all matters concerning the processing of personal data.

1.3. Terms defined in the GDPR retain their meaning here.

Article 2 - Term

The DPA takes effect on the effective date of the Agreement and remains in force for its duration, and until the complete return or deletion of the data under Article 11.

Article 3 - Description of processing

The nature, purpose, categories of data and data subjects, and duration of the processing are described in **Annex 1**. The Controller warrants the accuracy and completeness of that description and informs Synost of any change.

Article 4 - Documented instructions

4.1. Synost processes personal data **only on documented instructions** from the Controller, including with regard to transfers outside the European Union.

4.2. The following constitute documented instructions: the Agreement, the Specific Terms, this DPA, and any subsequent written request from the contact point designated by the Controller.

4.3. Where Synost is required to carry out a transfer under Union or Member State law, it informs the Controller before processing, unless legally prohibited.

4.4. In accordance with Article 28(3), second subparagraph, GDPR, Synost immediately informs the Controller if, in its opinion, an instruction infringes the GDPR or other data protection provisions.

4.5. Processing instructions falling outside the scope of the Agreement may be charged on a time-and-materials basis, subject to prior notice to the Controller.

Article 5 - Confidentiality

Synost ensures that persons authorised to process the data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and receive the necessary training. Access is limited to persons with a need to know.

Article 6 - Security of processing

6.1. Synost implements the appropriate technical and organisational measures required by Article 32 GDPR, described in **Annex 3**.

6.2. These measures may evolve to take account of the state of the art and identified risks, provided the overall level of security is not reduced.

6.3. The Controller acknowledges that the measures described in Annex 3 are appropriate to the risks presented by the processing described in Annex 1.

Article 7 - Sub-processors

7.1. The Controller grants Synost **general written authorisation** to engage sub-processors, listed as at the effective date in **Annex 2**.

7.2. Synost informs the Controller of any addition or replacement of a sub-processor **at least thirty (30) days before** it takes effect, by email or by publication on a dedicated page whose address is communicated to the Customer.

7.3. The Controller may object to such a change in writing, with reasons, within fifteen (15) days. Failing agreement between the parties on an alternative, either party may terminate the Agreement, for the affected Services only, without indemnity or penalty.

7.4. Synost imposes on each sub-processor, by contract, data protection obligations equivalent to those set out in this DPA. Synost **remains fully liable** to the Controller for the performance of its sub-processors' obligations.

Article 8 - Data location and transfers outside the European Union

8.1. The Controller's data is **hosted within the European Union**. The hosting sites used are listed in Annex 2.

8.2. Some sub-processors listed in Annex 2 are established in the United States. Remote access from that country cannot be excluded and constitutes a transfer within the meaning of Chapter V GDPR. Such transfers rely on the transfer mechanism stated for each sub-processor in Annex 2, namely an adequacy decision under the EU-U.S. Data Privacy Framework or standard contractual clauses.

8.3. These transfers are accompanied by supplementary measures: encryption of data at rest and of backups, management of encryption keys by Synost, and minimisation of the data transmitted.

8.4. Any new transfer outside the European Union is subject to prior notice to the Controller under Article 7.2, giving rise to the right of objection set out in Article 7.3.

Article 9 - Assistance to the Controller

9.1. **Data subject rights.** Synost implements appropriate technical and organisational measures to assist the Controller in responding to requests to exercise data subject rights (Articles 12 to 23 GDPR). Any request received directly by Synost is forwarded to the Controller within five (5) business days, without Synost responding to it itself.

9.2. **Compliance obligations.** Taking into account the nature of the processing and the information available to it, Synost assists the Controller in complying with its obligations under Articles 32 to 36 GDPR: security, breach notification, impact assessments and prior consultation of the supervisory authority.

9.3. Assistance exceeding reasonable efforts and Synost's usual means may be charged on a time-and-materials basis, subject to prior notice to the Controller.

Article 10 - Personal data breach

10.1. Synost notifies the Controller of any personal data breach without undue delay and **no later than forty-eight (48) hours** after becoming aware of it.

10.2. The notification includes, to the extent available: the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed, and a contact point.

10.3. Where the information cannot be provided at the same time, it is provided in phases without undue further delay.

10.4. Synost cooperates with the Controller and documents the breach. It is for the **Controller** to notify the CNIL and inform data subjects where required.

Article 11 - Fate of the data on termination

11.1. On termination of the Agreement, and **at the Controller's choice** expressed in writing within thirty (30) days:

- Synost returns the data in a standard, usable format; or
- Synost deletes it.

11.2. Failing instruction within that period, Synost deletes the data.

11.3. Deletion takes place within thirty (30) days of expiry of the exit period. Data held in encrypted backups is deleted at the end of the current rotation cycle, during which it is subject to no active processing.

11.4. Synost retains data where required to do so by Union or French law, for the duration and purpose of that obligation only.

11.5. A certificate of deletion is issued on written request.

Article 12 - Records and documentation

Synost maintains a record of the categories of processing activities carried out on behalf of the Controller, in accordance with Article 30(2) GDPR, and makes it available on request.

Article 13 - Audit

13.1. Synost makes available to the Controller the information necessary to demonstrate compliance with Article 28 GDPR.

13.2. The Controller may carry out an audit, or mandate an auditor to do so, **once per twelve (12) month period**, subject to thirty (30) days' written notice, during business hours, without disrupting Synost's operations.

13.3. The auditor must not be a competitor of Synost and is bound by confidentiality. The scope is limited to processing carried out on behalf of the Controller and excludes any information relating to other customers.

13.4. Synost may satisfy this obligation by providing a valid audit report or certification covering the relevant scope.

13.5. Audit costs are borne by the Controller. Time spent by Synost is charged on a time-and-materials basis, unless the audit reveals a material breach by Synost of its obligations.

13.6. An additional audit is carried out without delay at the request of the supervisory authority or following a significant data breach.

Article 14 - Controller obligations

The Controller undertakes to:

- have a legal basis for each processing operation entrusted to Synost;
- inform data subjects and obtain any required consent;
- transmit to Synost only the data necessary for the purposes described in Annex 1;
- not entrust data falling under Articles 9 and 10 GDPR without express mention in the Specific Terms and adaptation of the security measures;
- document its instructions and designate a contact point.

Article 15 - Liability

15.1. The allocation of liability between the parties is governed by Article 82 GDPR.

15.2. As between the parties, and without prejudice to the rights of data subjects and the powers of supervisory authorities, Synost's liability under this DPA is subject to the liability cap set out in Article 16 of the General Terms and Conditions of Sale.

Article 16 - Contact point

Requests relating to this DPA are addressed to: **hello@synost.com**.

Article 17 - Language

This DPA is drawn up in French and English. In the event of any discrepancy in interpretation, **the French version prevails**.

Annex 1 - Description of the processing

Item	Description
Nature of processing	Hosting, storage, operation, monitoring, backup, restore, maintenance and technical support of the Controller's systems and applications
Purpose	Provision of the Services defined in the Agreement
Categories of data subjects	Customers, prospects, members, employees, suppliers and users of the Controller's systems
Categories of data	Identification and contact data; connection and technical data (IP addresses, logs, session identifiers); content stored by the Controller and its users; commercial administration and billing data
Special categories	None, unless expressly stated in the Specific Terms
Processing operations	Storage, technical access in the event of an incident, backup, restore, erasure
Duration	Term of the Agreement, plus the exit period provided for in Article 11
Location	France - bare metal infrastructure operated by Synost, carrying the primary workload; additional capacity and backups with the providers listed in Annex 2, within the European Union

Annex 2 - Authorised sub-processors

List in force as at 28 August 2026.

Sub-processor	Role	Establishment	Data location	Transfer mechanism
Thomas Filip Locket EI (Synost)	Self-operated bare metal servers - primary workload	France	France	Not applicable
OVH SAS (OVHcloud)	Object storage (S3)	France	France	Not applicable
Scaleway SAS	Object storage (S3) and email delivery	France	France	Not applicable
Hetzner Online GmbH	Virtual machines (additional capacity)	Germany	Germany	Not applicable
netcup GmbH	Uptime monitoring	Germany	Germany	Not applicable
Vultr Holdings LLC	Virtual machines (additional capacity)	United States	France - Paris region	Standard contractual clauses
Backblaze Inc.	Offsite backup (B2)	United States	Netherlands - eu-central-003 region	Standard contractual clauses
Cloudflare Inc.	Authoritative DNS	United States	Global network	EU-U.S. Data Privacy Framework; standard contractual clauses as a fallback

Actual use of each sub-processor depends on the architecture chosen for the Controller, as described in the Specific Terms.

Annex 3 - Technical and organisational measures

Physical security

- Production servers housed in a dedicated, locked facility under Synost's exclusive control.
- Physical access restricted to authorised persons only.
- Backup power supply and protection against outages.
- Encryption at rest of volumes, rendering media unusable in the event of physical removal.

Logical access control

- Multi-factor authentication mandatory on all administrative access.
- Administrator access by cryptographic keys; password-only authentication disabled.
- Least-privilege principle applied; access rights reviewed at least every six months.
- Named traceability of access to production systems.

Encryption

- Data in transit encrypted using TLS 1.2 or above, configured in line with ANSSI recommendations.
- Encryption at rest of production volumes and backups.
- Secrets managed in a dedicated vault, outside code repositories.

Segregation and operations

- Network segmentation and isolation of environments between customers.
- Ingress and egress filtering; minimal service exposure.
- Security patches applied according to criticality; monitoring of published vulnerabilities.
- Separation of production and test environments.

Backups and continuity

- Encrypted backups, at the frequency and retention set out in the Specific Terms.
- Backup copies held at a site separate from production.
- Restore test carried out at least once a year.
- Recovery objectives (RPO/RTO) defined in the Specific Terms where applicable.

Logging and detection

- Centralised logging of access and security events.
- Log retention for the period set out in the Specific Terms.
- Alerting on significant security events.

Organisation

- Documented incident management and breach notification procedure.
- Confidentiality undertakings from authorised persons.
- Secure erasure or destruction of end-of-life media.
- Periodic review of these measures.

Synost - Thomas Filip Lochet EI - DPA version 1.0 of 28 August 2026