Data processing agreement

Version 1.1 | Last updated 29 September 2026

This is a translation of the French original, which governs in case of divergence.

This agreement, concluded under article 28 of regulation (EU) 2016/679 (the GDPR), forms an integral part of the terms and conditions of Avanserv SRL (the "provider"). It applies whenever the provider processes personal data on the client's behalf as part of the services, hosting, managed services and application operation among them. For that processing, the client acts as controller and the provider as processor. Where it contradicts the terms and conditions, this agreement prevails as regards personal data.

Article 1. Description of the processing

The subject matter, duration, nature and purposes of the processing, and the categories of data and of data subjects, are described in annex A, supplemented where applicable by the quote. The provider processes the data for no other purpose.

Article 2. The controller's instructions

The provider processes the data only on the client's documented instruction, including as regards transfers outside the European Union, unless required by Union or member-state law; in that case it tells the client of that requirement before processing, unless the law forbids it. The contract, the quote and the settings the client applies within the services all count as instructions. The provider tells the client immediately where an instruction appears to it to breach the GDPR or another data protection provision. The client warrants that its instructions are lawful and that the data it entrusts to the provider has been collected, and may be processed, in accordance with the GDPR.

Article 3. Confidentiality

The provider ensures that the people authorised to process the data are bound to confidentiality by contract or by a legal obligation, and that they access the data only so far as performing the services requires.

Article 4. Security

The provider puts in place the technical and organisational measures appropriate to the risk, in line with article 32 of the GDPR. The measures in force are described in annex B; the provider may change them, without reducing the overall level of protection.

Article 5. Subprocessors

The client gives general authorisation for the use of subprocessors. The list in force appears in the subprocessors page, which names each one's identity, location and service. The provider gives written notice of any addition or replacement at least 30 calendar days before it takes effect. The client may object in writing within that period, on reasonable data protection grounds; failing an acceptable solution, either party may terminate the service concerned without indemnity. The provider imposes on each subprocessor, by contract, obligations equivalent to those in this agreement, and remains fully liable to the client for their performance. The same notice and objection procedure applies where a subprocessor already authorised takes on a new kind of processing, such as the hosting provider also sending email.

Article 6. Data subjects' rights

Taking the nature of the processing into account, the provider assists the client, by appropriate technical and organisational measures, in responding to requests from data subjects exercising their rights. Where a data subject approaches the provider directly, the provider forwards the request to the client within five working days and does not answer it itself, unless the client instructs otherwise or the law requires it.

Article 7. Assistance to the controller

The provider assists the client in meeting its obligations under articles 32 to 36 of the GDPR, taking into account the nature of the processing and the information available to it: security, breach notification, impact assessments and prior consultation of the supervisory authority. Assistance beyond reasonable effort may be charged at the agreed time-and-materials rate.

Article 8. Data breaches

The provider notifies the client of any personal data breach affecting the processing covered by this agreement, without undue delay and no later than 48 hours after becoming aware of it. The notification describes 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. The provider documents the breach and cooperates with the client on the client's own notifications; it does not notify the supervisory authority or the data subjects in the client's place, unless an obligation of its own requires it. The client sends any question about a breach, or any report of an incident affecting the processing covered by this agreement, to privacy@avanserv.com.

Article 9. Location and transfers

The data entrusted to the provider is processed and stored in the European Union, subject to what follows. Email exchanges with the client's contacts, and the office tools that go with them, travel through the provider's business mail and office suite, whose operator is named in the subprocessors page and may process data outside the Union; that transfer is safeguarded as that list states, and the client, by entering into the contract, accepts it as a documented instruction.

Any other transfer to a third country requires a documented instruction from the client and rests on a mechanism from chapter V of the GDPR: an adequacy decision, or the European Commission's standard contractual clauses (implementing decision (EU) 2021/914) together with supplementary measures where necessary.

Where the client is established outside the European Economic Area, this agreement stands as the European Commission's standard contractual clauses, module four (transfer from the processor to the controller), of implementing decision (EU) 2021/914, with the docking clause (clause 7), under Belgian law, chosen at clause 17, and the jurisdiction of the courts of the judicial district of Namur, chosen at clause 18, as article 21 of the terms and conditions provides, for the transfer of data from the provider to the client. The description of the parties and of the transfer the clauses require is that of annex A of this agreement, the technical and organisational measures are those of annex B, and the list of subprocessors the clauses require is that of the subprocessors page.

Article 10. Audits

The provider makes available to the client the information needed to demonstrate compliance with this agreement. The client may carry out, at its own cost, an audit of the processing covered, no more than once in any twelve-month period save for a confirmed breach or an authority's request, on 30 calendar days' written notice, during working hours and without disrupting the services or compromising the confidentiality owed to other clients. At the client's request, the provider may offer it relevant and recent audit reports or certifications; the client may accept them in addition to, or instead of, an audit, but that option never takes away the client's right to audit and inspect the processing under article 28(3)(h) of the GDPR.

Article 11. Return and deletion

For hosting and managed services, return and deletion of data at the end of the service follow article 9 of the terms and conditions.

For other services covered by this agreement, at the end of the service concerned, the provider, at the client's choice expressed within 30 calendar days, returns the data in a structured, commonly used and machine-readable format, or deletes it, unless the law requires retention. Failing a choice within that period, the data is deleted. Deletion from active environments happens within 60 calendar days.

Where the quote provides for a backup service, backup copies are not restored after a deletion request, unless the law requires it, and they expire on the rotation cycle the quote sets; where a backup holding data due for deletion is restored, the deletion is applied again without delay.

Article 12. Liability and duration

The parties' liability under this agreement follows the regime of article 14 of the terms and conditions, without prejudice to article 82 of the GDPR. This agreement takes effect with the contract and remains applicable for as long as the provider processes data on the client's behalf.

Annex A. Description of the processing

Element	Description
Subject matter	Provision of the services ordered: hosting, managed services, operation and maintenance of applications
Nature	Collection, storage, structuring, consultation, disclosure on instruction, backup, erasure
Purposes	Performing the services and keeping them secure and continuous
Categories of data subjects	End users of the client's applications, the client's staff and contacts, the client's own contacts and clients
Categories of data	Content the client hosts and the technical logs of its processing; no special categories of data within the meaning of article 9 of the GDPR absent specific written agreement
Duration	The length of the service concerned, then return or deletion under article 11

End users' identification, account and sign-in data for the app.avanserv.com application falls outside this agreement: the provider processes it as controller, as the privacy policy describes. Account data of the end users of an application the provider hosts or operates on the client's behalf falls, instead, within this agreement.

Annex B. Technical and organisational measures

The measures below are those in force at the date shown at the head of this agreement. A service's quote may provide for further ones; article 4 governs how they change.

Measure	How it is implemented
Encryption in transit	Exchanges with the services are served over TLS, terminated by the hosting infrastructure. Session cookies "access_token" and "refresh_token" are marked Secure and HttpOnly outside development; the "avanserv_signed_in" cookie, which tells the public site a session exists elsewhere without revealing its content, is deliberately readable by code running in the browser and is not marked HttpOnly.
Encryption at rest	Enabled at the infrastructure vendor for the database. Certain sensitive columns carry dedicated application-level encryption as well.

Measure	How it is implemented
Backups	The app.avanserv.com platform database is backed up daily, kept for seven days. Data the provider hosts on the client's behalf follows the arrangement described below.
Passwords	Never stored in the clear: a bcrypt fingerprint. When the service answers, candidate passwords are checked against known breaches through a hash-prefix lookup, without sending the password.
Access control	A declarative role-based model, applied at record and field level, refusing by default whatever is not explicitly allowed.
Data separation	Only projects and an organisation's single sign-on (SSO) configurations are filtered by organisation on every query, with no way to bypass it from the interface. Other records, such as user accounts, files, the email outbox and public forms, are protected by access control rather than by that filter. The separation is logical, on shared infrastructure.
Logging	Access and operations are logged with the request identifier, the organisation and the source address; email addresses are masked in them.
Software quality	Every change goes through a pull request, apart from one exception reserved for a technical automation account on the repository, and merges only once a blocking continuous integration pipeline (formatting, static analysis, typing, unit and end-to-end tests) passes; an automated review runs on every pull request, without being a condition of merging today.
Secret management	Runtime secrets are supplied by a managed vault (Scaleway Secret Manager) through a controller that copies them into the runtime environment, never committed; secret-leak scanning runs before every commit.
Subprocessors	Selected on the basis of sufficient guarantees and under a contract meeting article 28 of the GDPR, as article 5 states.

For hosting and managed services, the quote further states the backup arrangement chosen, its frequency, its retention period and how often restores are tested, along with how long logs are kept. Absent a statement in the quote, no backup service is owed.

Annex C. Subprocessors

The list in force, kept up to date and dated, appears in the subprocessors page.