# Privacy and GDPR

Version 1.7 | Last updated 2 October 2026

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

This policy describes what we do with personal data when you read avanserv.com, when you write to us, send us a project enquiry or join a waiting list, and when you use the app.avanserv.com application. It is written to be read from end to end: it is short because we collect little.

The controller is Avanserv SRL, Rue du Vieux Fermier 6, 5100 Namur (Wierde), Belgium, enterprise number 1019.087.245. For any question, or to exercise your rights: privacy@avanserv.com. We have appointed no data protection officer, the size and nature of our activities not requiring one.

## What we do not do

The site carries no advertising tracker and no analytics tool. We neither sell nor rent any data, we send no newsletter, and we take no fully automated decision producing legal effects concerning you.

## Reading the site

Like every web server, ours keeps technical logs: IP address, page requested, timestamp and browser identification. They serve security, incident diagnosis and abuse prevention alone, on the basis of our legitimate interest in keeping the service working (article 6.1.f of the GDPR). They are hosted by Scaleway in the European Union; their centralised collection, with a 90-day retention, is planned and not yet active: each log stays today on the node that produced it, under that runtime environment's default rotation.

The few cookies in use are all strictly necessary or tied to a preference you expressed; they are set out in the cookie policy.

Everything a page displays, its typefaces and icons included, comes from our own servers. Displaying the site or the application sends your IP address to no one else.

## The contact form

When you send us a project enquiry, we record what you enter: your name, your email address, your company name and technical environment where given, the nature of the need, its description, the time horizon, the budget range and your browser's language. Those answers serve one thing: answering you and drawing up a proposal. The legal basis is taking steps at your request before entering into a contract (article 6.1.b of the GDPR). Your name, email address, the nature of the need, its description, the time horizon and the budget range are necessary to handle your enquiry; without them, we cannot take it further. Your company name and technical environment are optional.

The answers recorded in our database, hosted in the European Union, are permanently deleted twelve months after you send them, by an automated job. Two emails will go out when you submit: an acknowledgement addressed to you and an internal notification that repeats your answers, purely transactional; submitting the form signs you up to no mailing list. The internal notification will land in our business mailboxes, hosted by Google Workspace (see the section on transfers), where it will be kept with our correspondence (see the section on correspondence).

To prevent abuse, the number of submissions is limited per IP address and per email address; those technical counters are short-lived and are not attached to your enquiry.

## Waiting lists

For an offer still being built, a waiting list tells you when it opens. When you join one, we record your email address, the offer you are interested in, the optional line about what you are building, the page's language and the date you joined. That data serves to write to you when the offer opens and, if your project matches what we are looking for in the pilot phase, to write to you directly before then. The legal basis is your consent (article 6.1.a of the GDPR). Your email address is necessary to join the list; without it, we cannot tell you when the offer opens.

You withdraw that consent at any time by writing to privacy@avanserv.com, or through the link in the confirmation email: the link deletes your entry at once, a written request is handled without undue delay. Withdrawal does not affect the processing carried out before it. Without withdrawal, the entry is recorded in our database, hosted in the European Union, and permanently deleted two years after the date you joined, by an automated job.

Two emails will go out when you join: a confirmation addressed to you and an internal notification that repeats your address, the offer chosen and your optional line, kept in our business mailboxes with our correspondence. Leaving the list erases your entry; a request to privacy@avanserv.com also erases this notification once it exists. The number of sign-ups is limited per IP address and per email address, by short-lived counters that are not attached to your entry.

## Booking a call

The contact page offers a link to our booking page (Google Calendar): what you enter there, your name, your email address, what you write in the free-text field and the slot you pick, is recorded directly in our own calendar, hosted by Google Workspace (see the section on transfers). We are the controller of that processing; Google processes it on our behalf. We keep this information as our correspondence (see the section on correspondence).

## Reviews on Google

The site links to the review form of our Google Business Profile. What you write there is published by Google, under its own terms and privacy policy, and under the name of your Google account. We can reply to it publicly, on Google.

## The emails we send

The acknowledgements, the confirmations of joining a waiting list, address verification, password resets and account notifications are automated, transactional emails, and will be sent by Scaleway's transactional email service, in France, once that relay is running; the subprocessors will be updated at that point. The emails that announce an offer's opening or propose the pilot phase are written and sent by hand from our business mailboxes, on the basis of the consent given at sign-up, not a transactional relationship. The email that closes an engagement, sent by hand too, asks for a review on Google, on the basis of our legitimate interest in making our work known (article 6.1.f of the GDPR); you can object to that request by writing to privacy@avanserv.com. Our sending register keeps a record of delivery, with the recipient's address and the message subject, for 30 days; every trace of a message that stayed stuck is gone after 90 days at the latest. The body of messages holding anything sensitive, such as a verification link or the answers a form sent, is erased from

the register as soon as it is delivered; the body of other messages expires with its register row.

## Correspondence

The emails you send us, our replies and the forms' internal notifications are kept in our business mailboxes, hosted by Google Workspace (see the section on transfers). They serve to follow our exchanges, on the basis of our legitimate interest in answering you and keeping a record of what was said (article 6.1.f of the GDPR). A Google Workspace rule deletes each email automatically three years after it was sent or received. Those tied to a contract or an accounting record are filed apart and kept as long as the law requires. You can ask for their erasure sooner at privacy@avanserv.com.

## The application's user account

Your account on app.avanserv.com has one of these origins: an administrator of your client organisation creates it for you, or the identity provider it uses (single sign-on) creates it at your first sign-in; in both cases, we obtain your data from that third-party source (article 14.2.f of the GDPR). We process your identification and contact data (surname, first name, email address, phone where given, language, avatar) and the data needed to keep the account secure, on the basis of our legitimate interest in providing and securing the service (article 6.1.f of the GDPR); this account is not necessarily a contract concluded with you personally. The content your organisation hosts in the application is processed on its behalf, under the data processing agreement that binds us to it.

Your password is never stored in the clear: we keep only a fingerprint of it produced by a robust hashing algorithm (bcrypt). When a password is created or changed, we check that it does not appear in known data breaches by querying the Have I Been Pwned service: only the first five characters of a cryptographic hash of the candidate password are sent, never the password itself and no data that could identify you.

The application's technical logs carry the request's IP address and, for an open session, your account and organisation identifiers; a centralised collection, with a 90-day retention, is planned and not yet active: each log stays today on the node that produced it, under that runtime environment's default rotation. Account data is kept until its erasure is requested after the account closes: a request to privacy@avanserv.com then triggers its erasure, carried out by a person rather than an automated job, which removes your identification, contact and account-security data. It leaves in place the

technical logs on their current rotation, the platform database's backup until its seven-day cycle turns over, and the accounting and tax records the law requires us to keep for seven years.

## Who receives data

Your data is reachable only by the people inside the company who need it and by the technical providers listed in the subprocessors, each bound by a contract meeting article 28 of the GDPR.

Depending on its nature, your data may also reach our internal management tools (the Odoo software, at odoo.avanserv.com, hosted in the European Union), our accountant, our bank and our insurer, each for what their role requires, and our legal advisers when we need to consult them. Our invoices to a VAT-registered client in Belgium reach it over the Peppol network, through the access point Odoo SA operates in Belgium. We pass data to authorities only where the law obliges us to.

## Transfers outside the European Economic Area

Our servers and our storage are in the European Union, as our email sending relay will be. Several services are the exception:

- Google Workspace hosts our business mailboxes and our call-booking calendar; our email exchanges, the forms' notifications and the calls booked land there. Google processes this data in the United States and in the countries where its own subprocessors operate. Google is certified under the EU-US Data Privacy Framework; that framework is under appeal before the Court of Justice of the European Union (case C-703/25 P), so the European Commission's standard contractual clauses remain applicable alongside it.
- Have I Been Pwned, used for the password check described above, is operated from Australia, behind the Cloudflare network; it receives no more than a fragment of a cryptographic hash, which is not data that could identify you.

Our source code host and continuous integration pipeline (GitHub) and the AI tool that reviews our code changes before they merge (Anthropic) receive no data we process for our clients or our visitors: GitHub hosts our code, Anthropic receives only the content of code changes.

## Your rights

You may ask for access to your data, its rectification, its erasure, restriction of processing, portability of the data you gave us, and you may object to processing founded on our legitimate interest. Write to privacy@avanserv.com; we may ask you for something to verify your identity before answering. We answer within the month, free of charge. These requests are handled by a person, not by an automated job.

If you believe we process your data contrary to the regulation, you may lodge a complaint with the Data Protection Authority, rue de la Presse 35, 1000 Brussels, telephone +32 2 274 48 00, contact@apd-gba.be.

## Security

Exchanges with our servers are encrypted (TLS). Internal access follows the principle of least privilege, passwords are hashed, the separation between client environments is logical, on shared infrastructure, and the app.avanserv.com platform database is backed up daily, kept for seven days and encrypted by our infrastructure provider. The number of sign-in and password-reset attempts is limited to contain automated attempts, and an account created by an administrator keeps a record of who created it. An error tracker, in preparation on our own infrastructure, is not yet in service. In the event of a data breach likely to create a risk to your rights, we notify the Data Protection Authority within 72 hours and tell you where the risk is high.

## Changes to this policy

Every version of this policy is dated. Where a change is substantial, a visible note on the site says so; the version online is the authoritative one.