Data processing agreement

Version 1.0, effective date 17 September 2026

When you use Eclarion, we process personal data on behalf of your organisation: your colleagues' accounts, and whatever users enter into the platform. This data processing agreement (article 28 GDPR) governs how we handle that data. It is part of our service, applies automatically to every customer and is the same for everyone; there is nothing to sign. For your vendor records, every version is available at the bottom of this page as a PDF signed by us.

Who is who?

Your organisation is the controller: you decide which personal data goes into Eclarion and what it is used for. We are the processor: Eclarion B.V., registered with the Dutch Chamber of Commerce under number 62087282, at Nieuwstad 70 C, 6811 BM Arnhem, the Netherlands. The main agreement means your Eclarion subscription, which is formed under our terms of service.

What do we process, and why?

Subject matter	The operation of the Eclarion platform for your organisation
Duration	The duration of the main agreement, plus 3 months after termination during which you can export your data
Nature and purpose	Authentication and authorisation of users, storage and editing of product specifications and related data, audit logging and communication within the platform
Types of personal data	Name, business email address, phone number, job title, password hash, 2FA data, profile picture (optional), role, language preference, IP address, user activity, audit log entries, and data entered by users themselves (which may include contact details of your suppliers)
Categories of data subjects	Employees of your organisation; when supplier features are used, also contact persons at your suppliers

What do we commit to?

We process personal data only on your documented instructions: what you and your users do in the platform, and what you ask us in writing. We only deviate from this when a legal obligation requires us to, in which case we inform you in advance, unless the law prohibits it. If we think an instruction infringes the GDPR, we say so before carrying it out. You make sure there is a lawful basis for the data you put into Eclarion. We do not use personal data for our own purposes, and not to train AI models.

Everyone at Eclarion with access to personal data is bound to confidentiality. We assist you in meeting your obligations under articles 32 through 36 GDPR, such as security, breach notifications and data protection impact assessments. And we make available all information necessary to demonstrate

compliance with this agreement. An audit starts with our documentation and our sub-processors' reports. If that is not enough, we cooperate with an audit by you or an independent auditor: once a year, announced 30 days ahead, under confidentiality, at your expense.

How is security arranged?

We take appropriate technical and organisational measures in accordance with article 32 GDPR. These include at least:

- Encryption of data in transit (TLS), of the database at rest and of the backups
- Strict separation of customer environments with technically enforced access control, monitored by two automated layers
- Two-factor authentication for all users, mandatory per organisation at the customer's choice, and single sign-on via SAML
- Audit logging of changes, not modifiable after the fact
- Continuous backups with point-in-time recovery, plus daily backups
- Access to production systems limited to the people who need it

What else you can expect from the platform, including availability and recovery, is described in our service level agreement.

Which sub-processors do we use?

We use sub-processors for parts of the service, such as the data centre where our servers run. The current overview, including each party's function and processing location, is on our sub-processors page.

If we add a sub-processor that processes your organisation's personal data, or replace one, we inform you in advance. You then have 30 days to object on substantial privacy grounds. If we have to replace a sub-processor urgently because it fails or suffers a security incident, we do so immediately and notify you within 5 working days; your 30-day objection period then starts at that notification. If you object, we look for a solution together. If that fails, you can terminate the main agreement without notice. Prepaid fees for the remaining period are refunded. With every sub-processor we conclude a data processing agreement with obligations at least equivalent to this agreement.

What happens in case of a data breach?

If we discover a data breach affecting your organisation's personal data, we inform you without undue delay, and no later than 48 hours after discovery. We assist you with any notification to the supervisory authority and to data subjects.

What if a data subject exercises their rights?

Requests from data subjects (access, correction, deletion, data portability, objection) are handled by you as the controller; we assist you. If such a request reaches us directly, we forward it to you within 5 business days.

Does personal data leave the European Union?

The platform, the database and the backups run on servers in the European Union. A limited number of sub-processors process data outside the European Economic Area; this happens exclusively under a valid legal framework: an adequacy decision (such as the EU-US Data Privacy Framework) or the European Commission's Standard Contractual Clauses, with additional safeguards where needed. You can see which parties these are on the sub-processors page.

What happens when it ends?

After the main agreement ends, you can export all data for another 3 months. After that we permanently delete the personal data from our systems; copies in backups disappear within 45 days of that deletion. On request we confirm the deletion in writing. Legal retention obligations, such as the fiscal retention duty for invoice data, remain respected.

Liability and precedence

Liability between the parties is governed by the provisions of the main agreement, with due observance of article 82 GDPR. If this agreement conflicts with the main agreement or the terms of service, this agreement prevails where the processing of personal data is concerned.

Governing law and changes

This agreement is governed by Dutch law; disputes are submitted to the competent court in Arnhem, the Netherlands, unless mandatory law provides otherwise. We announce material changes to this agreement well in advance by email to the administrators of your account. Every version gets its own number and effective date and remains available as a PDF. Instructions, requests and objections go to team@eclarion.com.

Version history

Version 1.0, 17 September 2026: first published version

Signed on behalf of Eclarion B.V.

This is version 1.0 of the data processing agreement of Eclarion B.V., as published at https://www.eclarion.com/data-processing-agreement/. Eclarion B.V. binds itself to this text towards every organisation that uses the Eclarion platform. The organisation accepts it when activating its account. Countersigning is welcome but not required for validity.

W. van den Brink

W. van den Brink, director
Arnhem, 17 September 2026

ELECTRONICALLY SIGNED 2026-09-17 SHA-256 CAEAFE0A953357E0