PYES Software
Coba Kellingstraat 50 · 7558 ZA Hengelo · The Netherlands

Data processing agreement

Verwerkersovereenkomst · EstiMate · version 14 October 2026

Parties

The customer, as Controller
Name: _____
Address: _____
Chamber of Commerce: _____

Arnold Velzel, as Processor
trading as A-Vision Software and PYES Software
provider of the EstiMate service
Coba Kellingstraat 50, 7558 ZA Hengelo, The Netherlands
Chamber of Commerce (KvK) 68806027
info@a-vision.software

The Controller uses EstiMate, an online service of the Processor for estimating software projects (the "Service"). While providing the Service, the Processor processes personal data on behalf of the Controller. This agreement sets out how, as required by Article 28 of the General Data Protection Regulation (GDPR). Words such as "personal data", "processing", "controller", "processor", "sub-processor" and "personal data breach" have the meaning they have in the GDPR.

1. Subject and instructions

1. The Processor processes the personal data described in Annex 1 only to provide the Service to the Controller, and only on the Controller's documented instructions. Using and configuring the Service, such as adding users, inviting estimators, sharing an estimate summary, connecting an AI assistant through the MCP server or turning on written AI reports, counts as such an instruction, as does this agreement.
2. The Processor does not use the personal data for its own purposes, does not sell it and does not use it for advertising.
3. If an instruction in the Processor's opinion breaks the GDPR or other data protection law, the Processor informs the Controller straight away and may suspend that instruction until the Controller confirms or changes it.
4. If the law requires the Processor to process personal data in another way, it informs the Controller before doing so, unless the law forbids that.

2. Confidentiality

Everyone who works for the Processor and can access the personal data is bound to confidentiality, and only accesses the data as far as their work for the Service requires.

3. Security

The Processor takes appropriate technical and organisational measures to protect the personal data against loss and unlawful processing, taking into account the state of the art, the cost and the risks for the people involved. Annex 2 describes the current measures. The Processor may change them, as long as the level of protection does not go down.

4. Sub-processors

1. The Controller gives the Processor general permission to use sub-processors. The sub-processors in use when this agreement is signed are listed in Annex 1.
2. The Processor informs the Controller by email at least 30 days before it adds or replaces a sub-processor. The Controller may object within that period on reasonable grounds. If the parties do not find a solution, the Controller may end its use of the Service, and the Processor refunds any amount paid in advance for the period after it ends.
3. The Processor gives each sub-processor data protection obligations that provide at least the same level of protection as this agreement, in a written contract, and remains responsible to the Controller for the sub-processor's work.

5. Transfers outside the EU

The EstiMate server, database and backups are in the European Union. Personal data leaves the European Economic Area in two cases. When the Controller turns on written AI reports, Anthropic processes the report data in the United States, as onward processing under Anthropic's data processing terms, which use the EU standard contractual clauses. Microsoft 365, which sends the emails, may process limited data outside the EEA under Microsoft's own data protection terms. Any other transfer requires the Controller's permission and a safeguard under Chapter V of the GDPR.

AI assistants that the Controller's users connect to EstiMate themselves, such as Claude or ChatGPT, are not sub-processors of the Processor. Their use falls under the Controller's or user's own agreement with that provider.

6. Requests from data subjects

The Processor helps the Controller answer requests from people who use their GDPR rights, such as access, correction and deletion. Most of this the Controller can do in the Service itself. When a person contacts the Processor directly about data it processes for the Controller, the Processor passes the request on to the Controller without undue delay and does not answer it itself, unless the Controller asks it to.

7. Personal data breaches

1. The Processor informs the Controller without undue delay, and at the latest within 48 hours after discovering it, of a personal data breach that affects the Controller's data.
2. The Processor gives the Controller what it knows and what the Controller needs to report the breach to the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) and, where needed, the people involved: what happened, which data and how many people are affected, the likely consequences, and the measures taken or proposed. Information that is not yet available is given as soon as it is.
3. The Processor takes reasonable measures straight away to limit the consequences of the breach.

8. Help with other obligations

Taking into account the information it has, the Processor helps the Controller with its obligations under Articles 32 to 36 of the GDPR, such as a data protection impact assessment or prior consultation with the supervisory authority.

9. Information and audits

1. The Processor gives the Controller the information needed to show that it meets its obligations under this agreement.

2. The Controller may have this checked by an independent auditor who is bound to confidentiality, at most once a year and with at least 30 days' notice, or sooner after a personal data breach. The audit must not disturb the Service or give access to other customers' data. The Controller pays the costs of the audit.

10. Duration, deletion and return

1. This agreement applies as long as the Processor processes personal data for the Controller.
2. At the Controller's choice, the Processor deletes the Controller's personal data or returns it, when the Controller asks for it. The Controller can export its project results from the Service itself, and can ask for a full export of its data. The Processor deletes the data within one month after the request. Deleted data disappears from the backups within 14 days after that.
3. The Processor keeps data it needs for its own legal obligations, such as invoices, which Dutch tax law requires it to keep for 7 years. For that data, the Processor is the controller, as described in its privacy policy.
4. Obligations that by their nature continue after the end, such as confidentiality, stay in force.

11. Final provisions

1. This agreement is part of the terms of service of the Service and is accepted together with them. A signed copy is available on request. If this agreement and another agreement between the parties about the Service conflict on data protection, this agreement prevails. The limitations of liability in the terms of service also apply to this agreement.
2. Changes to this agreement are only valid when both parties agree in writing; email is enough.
3. Dutch law applies to this agreement. Disputes are submitted to the competent court in the Netherlands.

Signatures

For the Controller

Name

Position

Place and date

Signature

For the Processor

Arnold Velzel

Name

Position

Place and date

Signature

Annex 1: Description of the processing

Purpose and nature	Providing EstiMate: user accounts, running estimations in which estimators independently rate work packages, reviewing and finalising estimates, sharing estimate summaries, connecting AI assistants and, when turned on, writing AI reports. The processing consists of storing, organising, showing, sending and deleting data.
People involved	The Controller's users: its owner, admins, project managers, team leads and estimators, including estimators from outside the company whom the Controller invites.
Types of personal data	• Account details of users: name, email address, role, hashed password and two-factor settings • Project data: projects, work packages, invitations, ratings, anchor hours, final complexities and the explanations users write • AI connections: the apps a user connects and their access tokens • Written AI reports, when the Controller turns them on • Sessions: IP address and browser of logged-in users No special categories of personal data are needed for the Service. The Controller makes sure users don't enter them in project texts.
How long	As long as the Controller uses the Service, or until it asks for deletion, as described in article 10.

Sub-processors

Sub-processor	Task	Location	When
Amazon Web Services EMEA SARL	Hosting of the EstiMate server, database and backups	Frankfurt, Germany (EU)	Always
Microsoft Ireland Operations Ltd (Microsoft 365)	Sending emails such as invitations and password resets	EU; limited processing outside the EEA possible	Always
Anthropic Ireland, Limited	Writing AI reports about an estimate. Estimator names and the company name are not sent.	Ireland (EU); onward processing in the United States under Anthropic's data processing terms and the EU standard contractual clauses	Only after the Controller turns on written AI reports

Annex 2: Security measures

Location	The server, database and backups run in a data centre in Frankfurt, Germany.
Encryption in transit	All traffic to EstiMate uses HTTPS.
Passwords	Stored as one-way hashes, never in readable form. Repeated failed logins are slowed down.
Separation of customers	Every company only sees its own projects and users, and each user's role limits what they can see and do.

Independent estimates	Estimators never see each other's ratings. Only project managers, team leads, admins and the company owner see all ratings in the review.
Estimate links	Each invitation has its own random 64-character link that cannot be guessed. Closing the invitation stops it from being used.
Shared summaries	A link to share a finalized estimate never shows individual ratings or estimator names, and stops working after 30 days or sooner when turned off.
AI connections	AI assistants connect through OAuth, never get more rights than the user who connected them, and can be disconnected at any time.
Access by the Processor	System managers log in with two-factor authentication. Support only looks into a company's account with its permission, for at most 24 hours, and every support session is logged.
Backups	The database is backed up daily, and backups are kept for 14 days in the EU.