Data processing agreement Laadruim

Version 1, in force from 1 November 2026. Part of the terms and conditions of Laadruim.

Part 1. In plain language

This is an explanation. What binds us are the clauses in part 2, the arrangements in part 3 and the annexes.

1. **You decide, we carry out.** What you put in Laadruim we process only to make Laadruim work for you, and only the way you want it. If you ask for something we believe is not allowed, we tell you straight away.
2. **Which data, and whose:** see Annex II.
3. **Confidential:** everyone on our side who can reach the data must keep it confidential.
4. **Security:** see Annex III, specific and checkable.
5. **Who we bring in:** see Annex IV. If someone is added, we tell you 14 days in advance. You may object; if we cannot solve it, you may cancel.
6. **Nothing outside Europe** without you knowing and without the legal safeguards.
7. **Help:** if someone asks you for access or erasure, we help. Also with a DPIA.
8. **Data breach:** we tell you within 24 hours after we discover it, with what we know by then. So you can report on time to your supervisory authority (72 hours).
9. **Checking:** you get all the information to see that this is right. An audit or inspection is possible too.
10. **At the end:** you download everything with "Export everything", can still view it for 3 months, and after that we erase everything. We confirm that to you. It is gone from our backups within 40 days after that, and from the emergency copies of our hosting party within 90 days.

Part 2. The clauses

These are the EU standard contractual clauses from Commission Implementing Decision (EU) 2021/915, word for word. Chosen: Article 28 of the GDPR (Regulation (EU) 2016/679), Clause 5 not included, and in Clause 7.7 general written authorisation with a period of 14 days.

Section I

Clause 1. Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2. Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3. Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4. Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5

Not included (optional).

Section II: obligations of the Parties

Clause 6. Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7. Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8. Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

1. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
2. the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
3. the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
4. the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9. Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

1. the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
2. the likely consequences of the personal data breach;
3. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

Section III: final provisions

Clause 10. Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these

Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

1. the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
2. the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
3. the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

Part 3. Additional arrangements

Clause 2 allows us to add to the clauses, as long as this does not conflict with them or with people's rights.

1. **Together with the terms.** This agreement is part of the terms and conditions of Laadruim and applies for as long as those do, plus the period in Annex II (duration).
2. **Data breach within 24 hours.** On top of "without undue delay" (Clause 9.2) we notify you within 24 hours after we discover a breach, at the email address of your company's administrators and at the contact address in Annex I.
3. **Audit.** First we give you the information (Clause 7.6(c)). If you then want an audit or inspection, you announce it 30 days in advance. Once a year, and always in addition when there is an indication that something is wrong. Whoever carries out the audit keeps confidential what they see. The costs are yours, unless it turns out that we did not keep to these arrangements.
4. **At the end.** Your choice under Clause 10(d) is fixed as: first return (the export of article 8 of the terms, 3 months read only), then erasure, with a confirmation by email. If you want erasure sooner, ask us.
5. **Access from abroad.** People of the processor can sign in while travelling, with the same security (Annex III). The data stays on servers in the EU. We make no copies of customer data on a laptop, except encrypted for a planned restore test within the EU, and we erase those the same day.

6. **Liability.** Between us, article 14 of the terms applies. It never limits the rights of people whose data we process (GDPR Article 82).
7. **Transfer.** If your agreement passes to the BV of article 18 of the terms, this agreement goes with it.
8. **Language.** This agreement exists in Dutch and English. If they differ, the Dutch text prevails, except for part 2: the EU standard contractual clauses are official in every EU language.

Annex I: list of parties

Controller: the customer, with the company details from the request or the proposal. Contact: the administrators of the company in Laadruim. Signature: by accepting the terms and conditions, on that date (electronic counts as in writing, GDPR Article 28(9)).

Processor: Laadruim, the supplier in article 1 of the terms and conditions, Oder 20, Postbus E7710, 2491 DC Den Haag, the Netherlands, Chamber of Commerce number 56385404. Contact: Wilfred Boerendans, support@laadruim.nl. If your proposal names another company as supplier, we complete this annex and Annex IV accordingly.

Annex II: description of the processing

Categories of data subjects

1. The customer's users: staff at the level Administrator, Office or Warehouse.
2. Contact persons at the customer's relations (clients, suppliers).
3. People at delivery addresses and destinations, sometimes private individuals.
4. Recipients of reports and discrepancy notices outside Laadruim.
5. People named in messages from connections (such as orders from a carrier) and in files the customer imports.

Categories of personal data

- Name, email address, telephone number, address (street, postcode, town, coordinates).
- Account: level, an own label, who invited, the invitation (email), the passkey. Of the passkey we keep only the public part and the name of the device: the fingerprint or face stays on the person's own device.
- Log: who did what and when, the IP address and the type of device (such as "Safari on iPhone").
- Session: IP address and browser, for as long as someone is signed in (12 hours at most).
- Raw messages from connections, encrypted, with the sender's IP address.
- Laadruim has no note field on stock, inbound, outbound or relations, and no photos, signatures or attachments. There are short text fields the customer fills in, such as a description or an own label.

Sensitive data: none. Laadruim asks for it nowhere, and the customer does not put it in (article 11 of the terms). A passkey is not biometric data with us: that stays on the device.

Nature of the processing: storing, showing, searching and sorting; turning a message from a connection into an inbound or outbound; sending mail on the customer's instruction (invitations, reports, discrepancy notices); making and restoring backups; erasing.

Purposes: providing Laadruim (stock, inbound, outbound, connections, reports), secure sign-in, detecting and solving abuse and faults, and help when the customer asks for it.

Duration of the processing

What	Period
Everything of the customer	for as long as the agreement runs, plus 3 months read only after the end; then erased
IP address in the log	90 days, then empty
Log: sign-ins and access	365 days
Log: connections	90 days
Log: warehouse	7 years after the end of the year of the entry
Deactivated users	anonymous after 12 months, sooner if the customer asks
Security log on the server	90 days
Rejected, unknown or failed messages from connections	90 days
Accepted messages from connections	raw content and IP address gone 13 months after receipt; the inbound or outbound stays
Invitations not used	30 days after expiry
Imported files	2 hours
Reports to download	7 days
Files of "Export everything"	24 hours
Failed tasks in the queue	7 days
Sessions	12 hours at most
Backups (Backblaze)	30 nights, plus 7 days for old versions
Emergency copies of the hosting party	up to 90 days

For sub-processors the same subject matter, nature and duration apply, for the part stated in Annex IV.

Annex III: technical and organisational measures

Signing in and rights

- Only with a passkey; Laadruim does not use passwords. New users by invitation only: the link in that mail, or in a recovery mail, is there only to make a passkey.
- At most 5 sign-in attempts per minute per IP address; after that the door closes for a while.
- Sessions: signed out after 60 minutes idle (240 minutes after a passkey), 12 hours at most.
- Rights per level, checked on the server at every action, not only by hiding a button.
- A deactivated user is locked out at once.

Companies kept apart

- Every database query is limited to one company by default, and closes if no company is known.
- The database itself also ties every row of a company to that company. Automated tests guard this at every change.

Encryption

- Every connection uses TLS 1.2 or 1.3, and the browser may connect only securely for a year (HSTS).
- Stored encrypted: raw messages from connections, imported rows, and queued tasks and mails with data from Laadruim.
- Keys for incoming messages only as a one-way hash, with a list of allowed IP addresses.
- Backups with a password the storage party does not have.

Log and traces

- In the app the log can only grow, not change, except for erasing IP addresses and names according to Annex II. So it can be traced who did what, also after a data breach.

Availability and recovery

- Every night a backup to Backblaze (EU, Amsterdam), plus a daily snapshot at mijn.host.
- We practise restoring every quarter on a separate server, and the test copy is erased afterwards.
- Updates go to the test server first, and to live at night. Only a tested and approved version reaches live.

People and access

- Only Wilfred Boerendans and Ploi can reach the server, each with their own key.
- Team members of Laadruim sign in with a passkey and use their access only for help and for checking requests.
- Whoever has access is bound to confidentiality.
- Signing in is also possible while travelling outside the EU, with the same measures. The data stays on servers in the EU. The computer we manage from is encrypted.
- Our build and management software does not get to see customer data: scripts show only counts, and checks on live use our own test company. A question to the hosting party also goes without customer data.

Sparing with data

- No third-party trackers, no CDN, fonts from our own server. The usage measurement is added up, never per person.

Help for the customer

- Viewing and changing relations and addresses is done by the customer in Laadruim. A relation nothing depends on yet can go. A relation in use stays for the records (statutory retention, GDPR Article 17(3)(b)) and can be set to "On hold"; an address can be switched off.

- Export everything: the customer downloads everything in Excel and CSV; every export goes in the log and the administrators get a mail.
- After the end we erase a whole company, with its users and files, and confirm that by email.
- An administrator can have the data of a deactivated user erased at once ("Erase details", with a passkey; the other administrators get a mail). If a backup is restored, we erase again what had already been erased, with a list outside the database that holds only codes, no names.
- After a data breach: the log and the security log show what happened; we notify within 24 hours.

Annex IV: list of sub-processors

Who	What they do	Where	Safeguard
mijn.host B.V., Pietersbergweg 291, 1105 BM Amsterdam, Chamber of Commerce 89592514	the server, DNS, outgoing mail, daily snapshot and emergency copies up to 90 days	the Netherlands	their sub-processing agreement (version October 2026): data breach within 48 hours, new sub-processor 14 days in advance; their own sub-processors are on mijn.host/trust/subverwerkers
WebBuilds B.V. (Ploi), Amperestraat 16J, 3861 NC Nijkerk, Chamber of Commerce 94117233	managing the server, deployments, scheduling the backups; can reach the server	the Netherlands	their terms for processing in the EEA (version 10 October 2026): Ploi is a processor and acts only on instructions
Backblaze, Inc., San Francisco (California, USA)	storing the encrypted backup	EU Central (Amsterdam)	American company: active on the list of the EU-US Data Privacy Framework (adequacy decision (EU) 2023/1795) and their data processing agreement; Backblaze does not have the password of the copy
B2Next B.V., Zomerbed 24, 8266 LN Kampen, Chamber of Commerce 77362799	helping customers and checking requests; can look along in Laadruim as a team member, not on the server	the Netherlands	agreement with the same obligations

Not a sub-processor, because they get no personal data of customers: UptimeRobot (only whether the site answers), IndexNow (only public addresses of the site), GitHub (only code and fake data in tests), our build software (see Annex III). We use Moneybird and Mollie only for our own invoices and payments, not for what you put in Laadruim. Mail to recipients the customer chooses goes on the customer's instruction and does not make them sub-processors.