Data processing agreement

Last updated: 25 September 2026

Version: 2026.09.25

These documents describe Mirobrowse’s services, including websites, custom applications, event and ticket systems, communities and equestrian scoreboards. The applicable agreement specifies the services provided. They do not replace the customer’s own privacy information, sales conditions or event rules.

Parties: the customer identified in the main agreement, quotation, order confirmation or service order (“Controller”) and Mirobrowse (“Processor” or “MiroBrowse”).

This data processing agreement forms an integral part of the main agreement and applies as soon as and for as long as MiroBrowse processes personal data on behalf of the Controller. It takes effect no later than the start of processing.

1. Definitions

In this data processing agreement:

- **GDPR:** Regulation (EU) 2016/679, including applicable national implementing legislation;
- **Service:** any website, application, platform service, hosting service, API, CMS solution, custom solution or other digital service supplied by MiroBrowse to the Controller;
- **Main Agreement:** the agreement, quotation, order confirmation, service order and applicable service schedules between the Parties;
- **Processing Specification:** the description of the specific processing, including the Service, purposes, processing operations, personal data, data subjects, duration, retention periods and additional instructions;
- **Customer Data:** all data entered, sent, received, stored, generated or otherwise processed within the Service by or on behalf of the Controller;
- **Personal Data:** Customer Data that constitute personal data under the GDPR;
- **Personal Data Breach:** a security incident leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data;
- **Subprocessor:** another processor engaged by MiroBrowse for processing covered by this data processing agreement;
- **EEA:** the European Economic Area.

Terms not defined in this agreement have the meaning given to them by the GDPR.

2. Roles and scope

1. The Controller determines the purposes and essential means of processing Personal Data. MiroBrowse processes those Personal Data solely on the Controller's behalf and in accordance with its documented instructions.
2. This data processing agreement applies to every current or future Service to the extent MiroBrowse acts as processor. The main text need not be signed again when a new Service is added. The new Service and associated processing must, however, be included in the Main Agreement or Processing Specification.
3. The actual allocation of roles is decisive. Merely using the terms "Controller" and "Processor" does not change that allocation where the actual circumstances differ.
4. This agreement does not apply to processing for which MiroBrowse independently determines the purposes and essential means. This may include MiroBrowse's own contract administration, invoicing, statutory obligations, own security interests and business communications. The MiroBrowse privacy statement applies to that processing.
5. If MiroBrowse independently determines the purposes and essential means of processing contrary to the instructions, it may be regarded as controller for that processing under the GDPR.

3. Processing Specification

1. The subject matter, nature, purpose and duration of processing, the categories of Personal Data and the categories of data subjects are recorded in the Processing Specification.
2. The Processing Specification may be included in:
    - the Main Agreement;
    - a separate service or privacy schedule;
    - an order confirmation approved by the Parties;
    - the configuration of the purchased Service;
    - a customer account or administration environment recording the selected processing.
3. Only features actually purchased, activated or used form part of the processing. A general description of possible features does not mean that all those features or categories of data are actually used.
4. If the Processing Specification is insufficiently clear, the Parties consult before new or materially changed processing begins.

4. Documented instructions

1. The Main Agreement, Processing Specification, Service settings and written directions from authorised contacts constitute documented instructions.
2. MiroBrowse processes Personal Data only in accordance with those instructions, including instructions on transfers to a third country or international organisation.

3. If EU or Dutch law requires MiroBrowse to process Personal Data differently, MiroBrowse informs the Controller of that legal requirement before processing, unless the law prohibits this information on important grounds of public interest.
4. MiroBrowse immediately informs the Controller if, in its opinion, an instruction infringes the GDPR or other applicable data protection law.
5. MiroBrowse may suspend implementation of a potentially unlawful instruction until its lawfulness has been sufficiently clarified or the instruction has been amended or withdrawn. Confirmation by the customer alone does not make an unlawful instruction lawful. If the Controller continues to insist on a manifestly unlawful instruction, MiroBrowse may suspend or terminate the affected part of the Service.
6. MiroBrowse may take reasonable temporary measures without a prior instruction where immediately necessary to prevent or limit a security incident, data loss, abuse or serious disruption. MiroBrowse informs the Controller as soon as possible.
7. Additional instructions outside the agreed operation of the Service are discussed in advance. MiroBrowse may charge reasonable costs for them where those costs have been communicated and agreed beforehand.

5. Nature and purposes of processing

Depending on the purchased Service, MiroBrowse may collect, receive, record, organise, structure, store, update, consult, display, publish, combine, transmit, export, secure, back up, restore, restrict and erase Personal Data.

Processing may be necessary for:

- providing and operating the Service;
- hosting, storage, publication and data transmission;
- account, session, role and access management;
- processing forms, transactions, registrations and other actions;
- calculations, summaries, reports and output requested by the Customer;
- security, monitoring, logging and prevention of abuse;
- backup, recovery, continuity and troubleshooting;
- maintenance, updates, support and problem resolution;
- export, transfer and erasure on termination.

The precise purposes and operations of each Service are included in the Processing Specification.

6. Controller’s obligations

1. The Controller is responsible for the lawfulness of processing, including valid legal bases, information to data subjects, purpose limitation and data minimisation.

2. The Controller determines which Personal Data are necessary, how long they are retained and which persons receive access.
3. The Controller ensures that its instructions, configurations, forms, datasets and use of the Service comply with the GDPR and other applicable legislation.
4. The Controller is responsible for the accuracy and quality of supplied Personal Data and their timely correction or erasure.
5. The Controller handles data subject requests and notifications to the supervisory authority unless otherwise agreed in writing.
6. The Controller keeps contact details for privacy matters and data breach notifications up to date.
7. The Controller does not use the Service for special categories of personal data, criminal conviction and offence data, national identification numbers or systematic processing of highly sensitive data unless recorded in the Processing Specification and appropriate additional measures have been agreed in writing.
8. If the Service processes data about children or other vulnerable data subjects, the Controller ensures the required legal bases, information and safeguards.

7. Confidentiality and access

1. MiroBrowse ensures that persons acting under its authority who have access to Personal Data process them only according to the instructions and to the extent necessary for their tasks.
2. Those persons are bound by contractual or statutory confidentiality obligations.
3. MiroBrowse applies appropriate procedures for granting, reviewing, changing and withdrawing access rights.
4. Access is restricted on a need-to-know and least-privilege basis.
5. Access rights are withdrawn when a task, assignment or employment relationship ends or access is no longer necessary.

8. Technical and organisational measures

1. MiroBrowse takes appropriate technical and organisational measures under article 32 GDPR, taking into account:
    - the state of the art;
    - the costs of implementation;
    - the nature, scope, context and purposes of processing;
    - the likelihood and severity of risks to data subjects.
2. Depending on the Service and risks, measures may include:
    - unique accounts, roles and restricted access rights;
    - strong authentication and, where appropriate, multi-factor authentication;

- secure password storage and hashing;
- encrypted data transmission;
- logical separation of customer environments and data;
- logging, monitoring and detection of abuse or unusual access;
- technical updates, security patches and vulnerability management;
- secure development, testing and production processes;
- backups and recovery procedures;
- measures for availability, continuity and recovery;
- restricted administrator privileges;
- incident response and data breach procedures;
- secure erasure and overwriting of data;
- periodic evaluation and, where appropriate, testing of measures.

3. Any additional or different security measures are included in the Processing Specification or security schedule.
4. Further information about applicable security measures may be provided on reasonable request, to the extent this does not harm security or other customers' interests.
5. MiroBrowse may adjust security measures where necessary for improvement, continuity, technical development or security. The overall level of security is not materially reduced.
6. The Controller remains responsible for the security of its own devices, accounts, credentials, users, integrations and configurations outside MiroBrowse's managed environment.

9. Personal Data Breaches

1. MiroBrowse informs the Controller without undue delay after becoming aware of a Personal Data Breach. Where reasonably possible, this is within 24 hours of MiroBrowse becoming aware of the breach.
2. The initial notification includes, to the extent known at that time:
   - the nature of the breach;
   - the affected systems or Services;
   - the categories and approximate number of data subjects;
   - the categories and approximate number of personal data records;
   - the likely consequences;
   - the measures taken or proposed;
   - a contact point for further information.
3. If not all information is immediately available, MiroBrowse provides it in stages as it becomes available.

4. MiroBrowse takes reasonable measures to investigate, contain and remedy the breach and help prevent recurrence.
5. The Controller decides whether notification to the Dutch Data Protection Authority or data subjects is necessary. MiroBrowse provides reasonable assistance.
6. MiroBrowse does not independently notify data subjects or the supervisory authority on the Controller's behalf unless instructed in writing or required by law.
7. A notification or investigation does not constitute an admission of liability, fault or breach of an obligation.
8. The Controller reports security incidents within its own environment, accounts or systems to MiroBrowse without undue delay if they may affect the Service.

10. Data subject rights

1. Taking into account the nature of processing, MiroBrowse provides reasonable technical and organisational assistance with data subject requests.
2. If MiroBrowse directly receives a request concerning the Controller's Personal Data, it forwards the request to the known contact point without undue delay.
3. MiroBrowse does not respond substantively on the Controller's behalf unless instructed in writing or required by law.
4. Where supported by the Service, the Controller may itself access, correct, export, restrict or erase data.
5. Additional work outside the normal operation of the Service may be performed as additional work where agreed in advance and permitted by law. A dispute about additional costs does not suspend necessary statutory assistance and may not prevent the exercise of privacy rights or compliance with statutory deadlines.

11. Assistance with compliance

Taking into account the nature of processing and information available to MiroBrowse, MiroBrowse provides reasonable assistance with:

- the security obligations under article 32 GDPR;
- data breach notifications under articles 33 and 34 GDPR;
- data protection impact assessments under article 35 GDPR;
- prior consultation with the supervisory authority under article 36 GDPR;
- investigations or requests of a competent supervisory authority.

The Controller remains responsible for carrying out a DPIA and deciding whether processing is acceptable. If extensive assistance outside normal services is required, the Parties may agree reasonable additional costs.

12. Subprocessors

1. The Controller grants MiroBrowse general written authorisation to engage Subprocessors for the performance of the Service.
2. The current list of Subprocessors, including their identity, contact details, function and processing location, is provided to the Controller before processing.
3. MiroBrowse keeps the identity, contact details, function and processing location of all engaged Subprocessors in the processing chain up to date and available to the Controller, including where a list is provided through a website.
4. MiroBrowse informs the Controller at least 30 days before a proposed addition or replacement of a Subprocessor processing Personal Data.
5. Within 14 days of notification, the Controller may raise a reasoned objection where the change creates demonstrable risks to the protection of Personal Data.
6. In the event of a justified objection, the Parties seek a reasonable solution, such as an alternative Subprocessor, additional measures or disabling the affected component.
7. If no reasonable solution is possible, the Controller may terminate the part of the Service dependent on that Subprocessor. Other parts of the agreement remain in force where possible.
8. In an urgent security, continuity or legal situation, the Parties consult on a shorter notice period. The required prior authorisation and opportunity to object remain applicable. An emergency does not provide a general exemption from article 28 GDPR.
9. MiroBrowse imposes materially the same obligations on each Subprocessor as in this agreement, to the extent applicable to the processing concerned.
10. Under article 28(4) GDPR, MiroBrowse remains responsible to the Controller for the Subprocessor’s performance of its obligations.
11. An external party acting as an independent controller for its own purposes is not a Subprocessor for that processing. MiroBrowse identifies such recipients in the privacy information or Processing Specification where relevant.

13. Processing locations and international transfers

1. Where possible, MiroBrowse processes Personal Data within the EEA.
2. The known primary processing locations and relevant international transfers are included in the Processing Specification or subprocessor list.
3. Transfers outside the EEA take place only in compliance with Chapter V GDPR, for example on the basis of:
    - an adequacy decision;
    - approved standard contractual clauses;
    - binding corporate rules;

- another legally permitted transfer mechanism.

4. Where necessary, supplementary technical, organisational or contractual measures are taken and a transfer assessment is performed.
5. MiroBrowse informs the Controller of a legally binding request by a public authority for access to Personal Data unless prohibited by law.
6. Where reasonably and legally possible, MiroBrowse assesses the legality and proportionality of such a request and challenges manifestly unlawful or disproportionate requests.

14. Information, supervision and audits

1. MiroBrowse makes available information reasonably necessary to demonstrate compliance with article 28 GDPR and this agreement.
2. Where appropriate, MiroBrowse may first provide documentation, security information, questionnaires, audit reports, certifications or other available evidence.
3. The Controller may perform or commission one audit per calendar year. An additional audit is permitted:
   - after a relevant Personal Data Breach;
   - at the request of a competent supervisory authority;
   - where there are specific and reasonable indications of a material failure;
   - where required by a statutory obligation.
4. An audit is normally announced at least 30 days in advance unless urgency or a supervisory authority requires a shorter period.
5. The audit takes place during normal working hours and must not unnecessarily harm continuity, security, trade secrets or other customers' personal data.
6. The Controller may perform the audit itself or appoint an independent expert. The auditor must be bound by confidentiality and have no direct conflict of interest.
7. MiroBrowse may impose reasonable security conditions on access to systems and premises, but must not make the statutory audit right effectively impossible.
8. The Controller bears the cost of a regular audit. If a material failure attributable to MiroBrowse is established, MiroBrowse bears the reasonable costs of the relevant part of the audit. Costs or conditions must not be manifestly excessive or discouraging.

15. Return, export and erasure

1. After processing services end, the Controller chooses whether Personal Data are returned or erased, unless that choice is already recorded in the Main Agreement or Processing Specification.
2. The Controller may change its choice in writing during the agreed export period. The standard retrieval period is 30 calendar days after the applicable switching period, or from termination if there is no switching

period. Longer statutory rights and earlier valid erasure instructions take precedence.

3. An export includes available Personal Data and Customer Data in an appropriate, commonly used and, where technically possible, machine-readable format.
4. An export does not include MiroBrowse's source code, generic software, database structure, security information, administration environment, server configuration, trade secrets or other intellectual property. This does not exclude customer data held in a database or necessary explanations of export fields, and does not limit mandatory export or switching rights.
5. After the agreed export period, MiroBrowse erases Personal Data and existing operational copies unless:
    - the Controller requested return in time and it has not yet been completed; remaining operational copies are also erased after return;
    - EU or Dutch law requires further retention.
6. If the Controller does not communicate a choice within the export period, erasure is the default choice agreed in advance.
7. Personal Data in protected backups are isolated, not reused for ordinary operational purposes and erased or overwritten according to the backup cycle in the Processing Specification.
8. If a backup must be restored, previously erased data are erased again before being used for ordinary operational purposes.
9. On reasonable request, MiroBrowse confirms that the agreed erasure has been performed.
10. Data retained by law remain accessible only for the purpose requiring retention and are erased once that obligation ends.

16. Records, documentation and supervisory authorities

1. To the extent required by article 30(2) GDPR, MiroBrowse keeps a record of categories of processing activities carried out on behalf of customers.
2. MiroBrowse cooperates within reasonable limits with investigations and supervision by a competent data protection authority.
3. The Parties provide each other without undue delay with information needed to meet their own statutory obligations.
4. Contact about privacy, this agreement or a data breach may be made through info@mirobrowse.com.

17. Anonymised data

1. This agreement does not apply to data anonymised so that a person can no longer reasonably be identified, directly or indirectly.
2. MiroBrowse may use genuinely anonymised and aggregated data for security, capacity planning, statistics and service improvement.

3. MiroBrowse does not use merely pseudonymised data for this purpose where they must still be regarded as Personal Data.
4. MiroBrowse does not attempt to re-identify individual persons from anonymised data.

18. Changes and new Services

1. A new Service or feature may be added to this agreement by amending the Main Agreement or Processing Specification. The general provisions need not be redrafted for that purpose.
2. Material changes to this agreement are communicated to the Controller in writing and become part of an existing agreement only under the Main Agreement's amendment procedure or after written acceptance.
3. Merely publishing a new version on the website does not automatically amend an existing data processing agreement.
4. Operational changes to Subprocessors and security measures are made under articles 12 and 8 respectively.
5. If a change is required by new mandatory legislation, the Parties inform each other and reasonably cooperate in making timely amendments.

19. Duration, suspension and termination

1. This agreement applies for as long as MiroBrowse processes Personal Data on behalf of the Controller.
2. Provisions on confidentiality, audits, liability, return, erasure and statutory retention continue after termination for as long as necessary for their purpose.
3. If processing can no longer be performed lawfully or securely, the Parties consult on additional measures, suspension or termination of the affected part of the Service.

20. Order of precedence, liability and law

1. In a conflict concerning processing of Personal Data, this data processing agreement takes precedence over the general terms and the Main Agreement.
2. The Processing Specification takes precedence where it expressly records different or additional privacy arrangements for a specific Service, without reducing obligations under the GDPR or other mandatory law.
3. The Main Agreement remains decisive for commercial, financial and non-privacy matters.
4. Liability follows the Main Agreement and general terms to the extent compatible with article 82 GDPR and other mandatory law.
5. This agreement is subject to the same applicable law and dispute resolution provisions as the Main Agreement.