Privacy statement

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.

1. Who is responsible?

Mirobrowse, the sole proprietorship of Kevin Smulders, established at Jennerstraat 74, 7909 EB Hoogeveen, Nederland, Dutch Chamber of Commerce number 77829603, is responsible for the processing described below. Privacy questions may be sent to info@mirobrowse.com.

This privacy statement applies to MiroBrowse and the services, websites, applications, platforms and custom solutions offered, developed, managed or hosted by MiroBrowse. These include websites, the CMS, hosting, domain and email services, ticketing software, event platforms, scoreboard systems and other custom applications.

2. Two different roles

MiroBrowse processes personal data for its own business operations, such as quotations, agreements, accounts, invoices, administration, support, security and its own website. MiroBrowse is the controller for that processing.

When MiroBrowse processes personal data within a customer website, customer environment, CMS, ticketing platform, event platform, scoreboard system or custom application, the customer usually determines why and how those data are used. The customer is then the controller, and MiroBrowse processes the data as processor for hosting, publication, security, backups, maintenance and support. The data processing agreement applies to this processing.

A privacy question about data submitted through a customer website, form, ticket, event, scoreboard or other customer environment should therefore first be addressed to that customer or organisation.

3. What data do we use and why?

MiroBrowse primarily supplies editable websites with CMS and hosting, alongside custom solutions such as ticket sales, event management and equestrian scoreboards. Only features in use process the data listed for them. A static website does not automatically ask visitors for information, but the server may process technical data such as an IP address on a visit. Forms, search and enabled external components may process additional data.

Situation	Data	Purpose and legal basis

Quotation and agreement	Name, organisation, address, contact details, choices, arrangements and communications	To handle enquiries, prepare quotations and perform agreements
CMS account and security	Name, email address, role, permissions, password hash, 2FA status, sessions, IP address, device/browser and security logs	To operate and secure accounts, customer environments and the platform, based on the agreement and our legitimate interest
Hosting and technical management	Website files, content, technical settings, logs, backups and data the customer places in the system	To provide hosting, CMS use, storage, security, maintenance and support. For visitor data, we usually act on the customer’s behalf
Customer websites and forms	Form submissions, contact details, messages, IP address, technical logs and other data entered by visitors or customers	To make the customer website technically available and process data on the customer’s behalf under the data processing agreement
Search and usage statistics	Search text, language, time, website origin, result counts, response time and protected identifiers derived from the IP address and browser	To provide search results, monitor usage limits, prevent abuse and improve our own services. For customer purposes, we process on the customer’s instructions. Our own processing is based on a legitimate interest after assessing necessity and privacy, or on the necessary performance of a contract with the data subject where that actually applies. A search query may contain personal data; protected identifiers are not automatically anonymous
Applications and custom platforms	Account data, roles, permissions, settings, entered content, technical logs, usage data and application data	To supply, secure and manage the selected application or custom service and provide support
Ticket sales and events	Name, email address, ticket details, order, payment status, check-in status, selected event, communications and form data configured by the organiser	To enable registration, ticket sales, access, communications and event management, usually on the organiser’s behalf
Scoreboards and competition systems	Participant data, competition data, start numbers, categories, scores, times, results, jury input and publication status	To enable competition registration, judging, score processing and publication of results, usually on the organiser’s behalf
Community features	Account data, profile data, messages, comments, groups, questions, answers, reports and moderation data	To enable community features, communications, management, safety and moderation

Support and contact	Contact details, message, attachments, technical context and support history	To handle requests, perform the agreement, resolve problems and improve our services
Invoices and administration	Name, address, business details, payment details, invoice data and payment-related communications	To perform the agreement and comply with statutory administration and retention duties
MiroBrowse’s own website	IP address, time, URL, browser, session data, language preference and cookie preferences	For a secure and functioning website. We ask for prior consent for non-essential cookies where required by law
Abuse, security and legal notices	Contact details, relevant URLs, logs, evidence, notice, communications and technical data	To prevent abuse, investigate security incidents, protect rights and comply with statutory duties

Special categories of personal data and personal data relating to criminal convictions and offences are not intended to be processed within MiroBrowse’s standard services. A customer may process such data through a MiroBrowse service only after prior written consultation, with a valid legal basis and appropriate additional measures.

For our own quotations, services and support, we rely on performance of the agreement or your request for pre-contractual information where you are the contracting party. We use organisational contacts’ data based on our legitimate interest in business communications. Security and handling claims rely on our legitimate interest in safe services and protecting legal rights, after assessing necessity and your interests; mandatory records and reports rely on the applicable legal obligation. Where consent is required, we request it separately. Data for account access, performance or invoicing are necessary for that function; without them, we may not be able to provide it. Optional data are not mandatory. For customer processing, the responsible customer determines the legal basis.

We usually receive data from you, your organisation or use of the service. If your organisation creates an account for you, it may provide your name, business email address and role. Where information comes from another source, we inform you about that source and processing when required by the GDPR.

4. Customer environments, CMS use and export

The customer selects in the agreement which development, hosting, storage, CMS functionality, application or other service it purchases. During the term, the customer may receive access to the CMS, application or customer environment to manage its own content and data.

Use of the CMS, hosting environment or an application does not transfer ownership of MiroBrowse’s CMS, source code, database structure, server environment or generic components. This is not a legal basis for processing personal data; it clarifies where customer data are processed and what happens to access and export when the service ends.

5. With whom do we share data?

Mirobrowse uses Hetzner Storage Box for separate backup storage. This storage serves recovery purposes, not advertising. The data included, selected storage location and full backup cycle are recorded for each service. This is a separate facility alongside hosting at STRATO.

MiroBrowse primarily uses STRATO for VPS hosting, email and domain management. The primary hosting used for this is located in Germany. Domain registration may also require data exchange with a registry. The actual suppliers, their roles, backup locations and any additional access or transfers are recorded for each service; this does not mean that every external integration processes data exclusively in Germany.

Only MiroBrowse and suppliers needed for matters such as hosting, infrastructure, domain registration, email, backups, security, administration, payments, monitoring or support receive access to personal data to the extent necessary for their task.

When a public form uses reCAPTCHA or similar spam protection, technical data may be provided to the security supplier to prevent abuse. We do not use this for advertising profiles, selling data or marketing tracking.

We make appropriate arrangements with processors and subprocessors. We do not sell personal data. We disclose data to a government body or supervisory authority only where there is a valid statutory obligation or authority.

Advertising and tracking pixels are disabled in the standard setup. They may be added at a customer’s express request. That customer environment must then identify the supplier, purposes and data sharing, and obtain valid prior consent where required. Not selling data does not mean that no data are sent to an external supplier, for example for a video, spam check or advertising pixel.

6. Processing outside the EEA

Where possible, we choose processing within the European Economic Area. If a supplier processes data outside it, we use a valid mechanism under the GDPR, such as an adequacy decision or standard contractual clauses, with supplementary measures where necessary. You may request information about the applicable safeguards and a copy through our contact address, protecting confidential information where necessary.

7. How long do we retain data?

- contract and customer data: during the customer relationship and afterwards for as long as necessary for administration, evidence or possible claims;
- basic tax records, such as invoices and purchase and sales records: generally seven years under tax retention rules; where a longer statutory period applies to particular records, that longer period applies;
- account data: while the account is active and subsequently during a reasonable deletion and backup cycle;
- security logs: no longer than necessary for security, investigating abuse and evidence;
- support and legal notices: for as long as necessary for handling, evidence and statutory duties;
- data in customer environments: during the customer agreement and afterwards in accordance with the agreed export, deletion and backup periods.

When hosting, CMS use or application use ends, export and termination are handled under the agreement and applicable law. In addition to agreed static website files, the customer may receive available application data, such as participants, orders and results, in an appropriate commonly used format. This export does not include CMS source code, database structure, administration environment or technical infrastructure. Customer data in a database are covered by the return arrangements. Statutory export and switching rights remain applicable.

On termination, the customer chooses return or erasure under the data processing agreement. The customer may communicate or change that choice during the agreed export period; a longer statutory period takes precedence. After that period and the requested return, we erase the data unless retention is required by law. Residual data in protected backups disappear according to the agreed overwrite cycle.

Tax retention duties do not mean that all website content, form submissions, search queries, tickets or competition data are retained for seven years. Those data are subject to their own purpose, the controller’s instructions and agreed retention and erasure periods. The backups actually configured, their contents and retention periods are recorded for each service. A hosting subscription does not automatically mean that the supplier makes daily server or database backups. A copy of a published website is not a complete backup of the database and customer environment.

8. Security

We use appropriate technical and organisational measures to protect personal data, customer environments and systems. Examples include restricted access rights, hashed passwords, session management, two-factor authentication for designated accounts, logging, updates, backups, encrypted connections, abuse prevention and access control.

No security method can eliminate every risk. Customers and users are responsible for safe use of accounts, including safeguarding login details and restricting access to authorised persons.

9. Your privacy rights

You may request access, rectification, erasure, restriction or portability of your data, or object to processing based on legitimate interests because of your particular situation. These rights are subject to the conditions in the GDPR. You may always object to direct marketing. You may withdraw consent without affecting the lawfulness of earlier processing. Send your request to info@mirobrowse.com. We respond without undue delay and within one month of receipt. Only where necessary because of the complexity or number of requests may this be extended by up to two further months; we explain why within the first month. Requests are generally free of charge.

Where there is reasonable doubt, we may ask for information to verify your identity. Do not send a full copy of your identity document without being asked.

If your request concerns data processed through a customer website, customer environment, ticketing platform, event, scoreboard or custom application and we act as processor, we forward the request to the responsible customer without undue delay. We tell you who will handle it and provide the agreed assistance; we do not independently decide on that customer’s behalf unless required by law.

10. Children, automated decisions and changes

For our own customer relationship, we do not make decisions based solely on automated processing that produce significant legal or similarly significant effects.

Minors may also participate or buy tickets in ticketing, event and equestrian applications. The responsible customer or organiser must ensure a valid legal basis, understandable information, limited data collection and appropriate protection when publishing participants and results. Where consent or parental or guardian consent is required, it must be arranged. Consent to processing, consent to publication and capacity to make a purchase are separate questions; a ticket or participation does not automatically constitute consent to all publication.

You may contact us about a complaint, but you may also complain directly to the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) or another competent data protection authority. Contacting us first is not a requirement. We update this statement when our processing, services or the law change and provide the information required by the GDPR for a change. A new statement does not provide consent for new purposes.