

data protection

This privacy notice explains which personal data VICRONIX processes when you visit our public websites and web applications, use GRID, contact us, receive support or attend a video meeting, apply for a position, or use our community servers. Personal data is information relating to an identified or identifiable person.

It applies to the public production services under vicronix.net and the associated subdomains. Pure development, beta and internal administration areas are excluded from audience analytics, but may generate technically necessary security and server logs.

Last updated: 10 September 2026

01 Controller

The controller responsible for the processing described in this notice is:

VICRONIX – Proprietor David Crump
Hausotterstraße 26
13409 Berlin
Germany

eMail: hello@vicronix.de

Phone: +49 176 64409365

02 Principles and legal bases

We process only data required for a defined purpose, protect it with appropriate technical and organisational measures, and delete or anonymise it when its purpose and applicable retention obligations cease to apply.

Depending on the activity, processing is based on your consent (Art. 6(1)(a) GDPR), a contract or steps taken before entering into a contract (Art. 6(1)(b) GDPR), a legal obligation (Art. 6(1)(c) GDPR), or our legitimate interests (Art. 6(1)(f) GDPR). Our legitimate interests include the secure and stable operation of our systems, prevention of misuse, error analysis, efficient communication, and needs-based improvement of our services.

03 Hosting and delivery

Our production business websites, web applications and central systems are hosted through Hostinger in data centres within the European Union. Depending on the service and technical availability, we use locations in Germany or France.

When a service is accessed, the hosting infrastructure processes in particular the IP address, date and time, requested address, amount of data transferred, referrer, browser, operating system, response status and technical identifiers. This is necessary for delivery, stability, capacity planning and attack prevention. The legal basis is Art. 6(1)(f) GDPR and, for services used under a contract, additionally Art. 6(1)(b) GDPR.

Development servers are operated separately from production customer systems. They are not intended for real production customer data. People testing them may nevertheless generate technical log data. Community servers run on separate infrastructure provided by ZAP-Hosting; details are set out in the “Community servers” section.

Further information: [Hostinger Privacy Policy](#) and [ZAP-Hosting Privacy Policy](#).

04 Server logs and operational monitoring

We consolidate technical server and application logs to detect faults, capacity problems and attacks. Depending on the event, the data may include IP address, timestamp, requested path, response status, referrer, browser and device information, service or container identifier, and technical error and performance data.

Ordinary operational logs are generally deleted after seven days. Data relating to a specific security incident or error may exceptionally be retained for longer where required to investigate and remedy the event, prevent further attacks, or establish, exercise or defend legal claims.

The legal basis is Art. 6(1)(f) GDPR. Our legitimate interest is the secure, available and traceable operation of our services.

05 Cookies and device storage

Our services use technically necessary cookies or comparable storage mechanisms where required for authentication, session control, security, language settings, or a function expressly requested by you. Access to your device is governed by Section 25(2)(2) TDDDG; subsequent processing of personal data is based, depending on the function, on Art. 6(1)(b) or (f) GDPR.

Non-essential cookies or functions are used only with valid consent under Section 25(1) TDDDG and Art. 6(1)(a) GDPR. You may withdraw your consent at any time with effect for the future.

Audience analytics with Umami operates without cookies in the standard configuration used by us. Crisp support chat uses its own functional cookies; details and retention are provided in the “Support chat” section.

06 Audience analytics with Umami

We use a self-hosted instance of the open-source Umami software to understand usage and audience reach across our public production websites and subdomains and to improve our services technically and editorially. Beta, development and private administration areas are excluded from this analysis.

We collect page address and title, referrer, time, browser, operating system, device type, approximate country, anonymous session and visit data, and interaction events defined by us that do not contain form, chat or other content data. Umami does not set analytics cookies. The IP address and user agent are used technically to form an anonymous session identifier; the raw IP address is not stored in the analytics dataset.

Analytics data remains on our EU-based infrastructure, is not used to build personal profiles, and is deleted or permanently anonymised after 30 months. The legal basis is Art. 6(1)(f) GDPR. Our legitimate interest is privacy-friendly audience measurement, error detection and improvement of our public services. You may object to this processing at any time on grounds relating to your particular situation.

Further information: [Umami documentation](#).

07 Contact and eMail

If you contact us by eMail, form or a contact function provided within our services, we process the information you submit. This may include your name, contact details, subject, message, attachments, time, and technical delivery information.

We process this data to handle your request. The legal basis is Art. 6(1)(b) GDPR where the communication concerns a contract or pre-contractual steps; otherwise, it is Art. 6(1)(f) GDPR based on our interest in efficient and traceable communication. Processing that expressly depends on consent is based on Art. 6(1)(a) GDPR.

We manage our business eMail infrastructure ourselves on EU-based hosting infrastructure. Requests are deleted when they have been conclusively handled and there are no remaining contractual, evidentiary or statutory retention grounds.

08 Customer, account and contract data

To prepare, perform and terminate contracts and provide GRID, we process the necessary master, contact, contract, project, account, usage, billing and communication data. The legal basis is Art. 6(1)(b) GDPR. We process records required under tax and commercial law pursuant to Art. 6(1)(c) GDPR.

Operational customer and project data is generally deleted or anonymised no later than six months after the business relationship ends, unless it remains necessary for handover, follow-up support or the defence of legal claims. Statutory retention periods are commonly six, eight or ten years, depending on the document. In particular, Section 147 of the German Fiscal Code and Section 257 of the German Commercial Code apply.

09 Support chat with Crisp

We use Crisp, provided by Crisp IM SAS, France, for setup assistance, support and service-related communication. If Crisp is loaded on an eligible page or you use the chat, it may process your name, eMail address, telephone number and other contact details you provide voluntarily, messages and attachments, IP address, browser and device information, page visited, time, account or project context, support history, segments and service attributes assigned by us.

We use Crisp features to set up, answer, route, automate, quality-check and analyse support cases. These include Hugo AI and Magic Browse. Hugo AI may process the conversation and help context necessary for a request to prepare answers, summaries or routing. You may request human handling at any time. No decision producing legal or similarly significant effects is made solely by automated means.

Magic Browse allows authorised support personnel to view the current state of the page you have open in the context of a specific support request, so they can guide you step by step. It is not used to collect passwords, payment details or unrelated content. Please do not submit special categories of personal data in the chat unless this is expressly necessary and agreed.

Processing is based on Art. 6(1)(b) GDPR where it is required for pre-contractual steps or performance of a contract; otherwise, it is based on Art. 6(1)(f) GDPR. Our legitimate interest is fast, contextual support. Where consent is required to load the service or an optional function, Section 25(1) TDDDG and Art. 6(1)(a) GDPR are the legal bases.

Crisp uses functional cookies with a regular lifetime of six months. Support content is retained until the request has been resolved and, during an existing customer relationship, for as long as it is required to provide traceable support. It is then deleted or anonymised under our deletion rules unless contractual, evidentiary or statutory grounds require further retention.

Further information: Crisp Privacy Policy and Crisp Cookie Policy.

10 Video meetings with Whereby

We use Whereby Embedded for scheduled video and support meetings. The interface surrounding the meeting is embedded in GRID, but the video conference itself is provided as an external service by Whereby AS, Norway.

The data processed may include meeting and room data, a display name provided voluntarily, IP address, browser and device information, connection and quality data, and audio, video and chat data transmitted during the meeting. We do not record or permanently store audio or video content unless recording is expressly announced and enabled for the individual meeting.

The legal basis is Art. 6(1)(b) GDPR for pre-contractual or contractual meetings; otherwise, it is Art. 6(1)(f) GDPR based on our interest in direct and secure remote communication. Norway is part of the European Economic Area.

Further information: Whereby Privacy Policy and Whereby Data Processing Agreement.

11 Error analysis

We use self-hosted error analysis on our EU-based infrastructure to detect and remedy technical faults. Depending on the error, this may process the error type and message, stack trace, requested path, time, browser and device details, and technical request or account identifiers where present in the particular error context.

The transmission of personal content is disabled by default. Error data is generally deleted after 90 days. Required extracts relating to a specific unresolved error or security incident may be retained until the issue has been conclusively resolved and documented.

The legal basis is Art. 6(1)(f) GDPR. Our legitimate interest is the stability, security and continuous improvement of our applications.

12 Protection against attacks and misuse

We automatically analyse security-relevant events to detect and prevent attacks, automated misuse and unauthorised access. This may involve processing suspicious IP addresses, timestamps, the service attacked, recognised attack patterns, technical context data and the resulting blocking decision.

We use CrowdSec for this purpose. Security decisions and related technical indicators may be checked against or transmitted to CrowdSec infrastructure so that known attacks can be detected collaboratively. For contextualised IP addresses processed within the shared network, CrowdSec describes joint controllership with the members of its ecosystem; we decide whether to apply a specific block to our systems. An automated block only restricts technical access to our systems and does not produce legal or similarly significant effects.

The legal basis is Art. 6(1)(f) GDPR. Our legitimate interests are network and information security, protection of customer and company data, and prevention of fraud and misuse. Local events are subject to the periods described in the “Server logs” section. According to CrowdSec, IP addresses involved in an attack are generally retained in full for no more than three months, after which their personal character is progressively reduced.

Further information: CrowdSec Privacy Policy.

13 Encrypted backups

We create encrypted backups of production systems to protect against data loss. Backups are transferred to Cloudflare R2 in encrypted form and configured for storage within the EU data jurisdiction. Cloudflare processes the encrypted backup objects as an infrastructure provider and processor.

Backups follow a rolling backup and deletion schedule. When a record is deleted from the primary system, an encrypted copy may remain until the relevant backup expires as scheduled. Restoration takes place only in the event of a technical failure, security incident or necessary data recovery; the regular deletion rules apply again afterwards.

The legal bases are Art. 6(1)(b) and (f) GDPR and, for records subject to statutory retention, Art. 6(1)(c) GDPR. Further information: Cloudflare Privacy Policy.

14 Community servers

We operate free-to-use community servers for ARK: Survival Ascended, 7 Days to Die, Minecraft, Hytale and Enshrouded, as well as a private World of Warcraft server. These systems are separated from our business production systems and run on infrastructure provided by ZAP-Hosting.

Depending on the game and platform, use may involve processing your IP address, connection time, platform, account, player and character name or identifier, save data, world and gameplay data, chat messages, technical server and anti-cheat logs, and moderation, warning and ban information.

We process this data to provide the server, save game progress, coordinate multiplayer use, troubleshoot issues, moderate the community, and prevent fraud, cheating, harassment and technical attacks. The legal basis is Art. 6(1)(b) GDPR for the requested server service and Art. 6(1)(f) GDPR for security, stability and fair community rules.

Connection and technical security logs are deleted when they are no longer required for operation and protection. Save data generally remains for the active lifetime of the relevant world or participation. Moderation and ban data may be retained for as long as required to enforce a measure, protect the community or defend legal claims. Game and platform providers process data under their own terms when you use their accounts, software or authentication.

15 Recipients and international transfers

Within VICRONIX, access is limited to people who require it for their assigned tasks. Where necessary for the particular activity, external recipients may include hosting and storage providers, communication and support services, video-conferencing providers, security services, tax and legal advisers, payment or billing services, and public authorities where disclosure is legally required.

Service providers are selected carefully and, where they act on our behalf, are bound by contracts under Art. 28 GDPR. Some providers may use technical subprocessors or process individual data outside the European Economic Area. Where no adequacy decision applies, we rely in particular on EU Standard Contractual Clauses and supplementary safeguards. You may request details and copies of available safeguards using the contact information above.

EU-based storage of our core systems therefore does not mean that every technical processing activity associated with every optional communication, security or support feature takes place exclusively within the EU.

16 Retention

Where this notice does not specify a fixed period, we retain personal data only for as long as it is required for the relevant purpose. We then delete or anonymise it unless statutory retention, ongoing contract performance, consent, or the necessary establishment, exercise or defence of legal claims requires further retention.

Our main standard periods are: seven days for ordinary operational logs, 90 days for error data, 30 months for Umami analytics data, six months for Crisp functional cookies, generally six months for operational customer and project data after the contract ends, and six months for applicant data after the recruitment process. Depending on their type, tax and commercial records are commonly retained for six, eight or ten years.

17 Applications

If you apply to work with us, we process the data required to decide whether to establish an employment relationship. This includes in particular your name and contact details, CV, cover letter, references, qualifications and related communication.

The legal basis is Section 26(1) BDSG in conjunction with Art. 6(1)(b) GDPR. If you voluntarily agree to join an applicant pool, the legal basis is Art. 6(1)(a) GDPR; you may withdraw this consent at any time with effect for the future.

After the recruitment process ends, we delete your data no later than six months after notifying you of the decision, unless statutory obligations, legal claims or valid consent to longer retention require otherwise.

18 Your rights

Subject to the statutory requirements, you have rights of access, rectification, erasure, restriction of processing and data portability. You may object to processing based on Art. 6(1)(f) GDPR on grounds relating to your particular situation. You may withdraw consent at any time with effect for the future; this does not affect the lawfulness of processing carried out before withdrawal.

To exercise your rights, an informal message to hello@vicronix.de is sufficient. To prevent data from being disclosed or changed for an unauthorised person, we may request reasonable proof of identity.

You also have the right to lodge a complaint with a data-protection supervisory authority. The authority particularly responsible for us is:

Berlin Commissioner for Data Protection and Freedom of Information
Alt-Moabit 59-61
10555 Berlin
Germany
eMail: mailbox@datenschutz-berlin.de
www.datenschutz-berlin.de

19 Changes

We update this privacy notice when our processing, services or legal requirements change. The current version is always available at this address. We will provide additional notice of material changes where legally required or appropriate to the nature of the change.