

Datenschutz

Diese Datenschutzerklärung erläutert, welche personenbezogenen Daten VICRONIX beim Besuch unserer öffentlichen Websites und Webanwendungen, bei der Nutzung von GRID, bei Kontakt-, Support- und Videoterminen, im Bewerbungsverfahren sowie auf unseren Community-Servern verarbeitet. Personenbezogene Daten sind Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen.

Sie gilt für die öffentlichen produktiven Angebote unter vicronix.net und den zugehörigen Subdomains. Reine Entwicklungs-, Beta- und interne Administrationsbereiche sind nicht Bestandteil der Reichweitenanalyse, können aber technisch notwendige Sicherheits- und Serverprotokolle erzeugen.

Stand: 10. September 2026

01 Verantwortlicher

Verantwortlich für die in dieser Erklärung beschriebene Verarbeitung ist:

VICRONIX – Inh. David Crump
Hausotterstraße 26
13409 Berlin
Deutschland

eMail: hello@vicronix.de
Telefon: +49 176 64409365

02 Grundsätze und Rechtsgrundlagen

Wir verarbeiten nur Daten, die für einen festgelegten Zweck erforderlich sind, schützen sie durch angemessene technische und organisatorische Maßnahmen und löschen oder anonymisieren sie, sobald Zweck und Aufbewahrungspflichten entfallen.

Je nach Vorgang beruht die Verarbeitung auf Ihrer Einwilligung (Art. 6 Abs. 1 lit. a DSGVO), auf einem Vertrag oder vorvertraglichen Maßnahmen (Art. 6 Abs. 1 lit. b DSGVO), auf einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. c DSGVO) oder auf unseren berechtigten Interessen (Art. 6 Abs. 1 lit. f DSGVO). Berechtigte Interessen sind insbesondere der sichere und stabile Betrieb unserer Systeme, die Abwehr von Missbrauch, die Fehleranalyse, eine effiziente Kommunikation und die bedarfsgerechte Verbesserung unserer Angebote.

03 Hosting und Bereitstellung

Unsere produktiven geschäftlichen Websites, Webanwendungen und zentralen Systeme werden über Hostinger in Rechenzentren innerhalb der Europäischen Union betrieben. Je nach Dienst und technischer Verfügbarkeit verwenden wir Standorte in Deutschland oder Frankreich.

Beim Abruf eines Angebots verarbeitet die Hosting-Infrastruktur insbesondere IP-Adresse, Datum und Uhrzeit, angeforderte Adresse, übertragene Datenmenge, Referrer, Browser, Betriebssystem, Antwortstatus und technische Kennungen. Dies ist zur Auslieferung, Stabilität, Kapazitätsplanung und Abwehr von Angriffen erforderlich. Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO; bei vertraglich genutzten Diensten zusätzlich Art. 6 Abs. 1 lit. b DSGVO.

Entwicklungsserver werden getrennt von produktiven Kundensystemen betrieben. Sie sind nicht für echte produktive Kundendaten vorgesehen. Testende Personen können dort dennoch technische Protokolldaten erzeugen. Community-Server werden auf gesonderter Infrastruktur von ZAP-Hosting betrieben; Einzelheiten

finden Sie im Abschnitt „Community-Server“.

Weitere Informationen: Datenschutzhinweise von Hostinger und Datenschutzhinweise von ZAP-Hosting.

04 Serverprotokolle und Betriebsüberwachung

Zur Erkennung von Störungen, Kapazitätsproblemen und Angriffen führen wir technische Server- und Anwendungsprotokolle zusammen. Verarbeitet werden je nach Ereignis IP-Adresse, Zeitstempel, aufgerufener Pfad, Antwortstatus, Referrer, Browser- und Geräteangaben, Dienst- oder Containerkennung sowie technische Fehler- und Leistungsdaten.

Normale Betriebsprotokolle werden grundsätzlich nach sieben Tagen gelöscht. Daten zu einem konkreten Sicherheits- oder Fehlerfall können ausnahmsweise länger gespeichert werden, solange dies zur Aufklärung, Behebung, Abwehr weiterer Angriffe oder zur Geltendmachung und Verteidigung von Ansprüchen erforderlich ist.

Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO. Unser berechtigtes Interesse liegt in einem sicheren, verfügbaren und nachvollziehbaren Betrieb unserer Angebote.

05 Cookies und Gerätespeicher

Unsere Angebote verwenden technisch notwendige Cookies oder vergleichbare Speichermechanismen, wenn dies für Anmeldung, Sitzungssteuerung, Sicherheit, Spracheinstellungen oder eine ausdrücklich gewünschte Funktion erforderlich ist. Der Zugriff auf Ihr Endgerät richtet sich dabei nach § 25 Abs. 2 Nr. 2 TDDDG; die anschließende Verarbeitung personenbezogener Daten beruht je nach Funktion auf Art. 6 Abs. 1 lit. b oder lit. f DSGVO.

Nicht notwendige Cookies oder Funktionen werden nur eingesetzt, wenn eine wirksame Einwilligung nach § 25 Abs. 1 TDDDG und Art. 6 Abs. 1 lit. a DSGVO vorliegt. Eine Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Die Reichweitenanalyse mit Umami erfolgt in der eingesetzten Standardkonfiguration ohne Cookies. Der Support-Chat Crisp verwendet eigene funktionale Cookies; Einzelheiten und Speicherdauer finden Sie im Abschnitt „Support-Chat“.

06 Reichweitenanalyse mit Umami

Wir verwenden eine selbst gehostete Instanz der Open-Source-Software Umami, um Nutzung und Reichweite unserer öffentlichen produktiven Websites und Subdomains zu verstehen und unser Angebot technisch und inhaltlich zu verbessern. Beta-, Entwicklungs- und private Administrationsbereiche sind von dieser Analyse ausgenommen.

Erfasst werden Seitenadresse und Seitentitel, Referrer, Zeitpunkt, Browser, Betriebssystem, Gerätetyp, ungefähres Land, anonyme Sitzungs- und Besuchsdaten sowie von uns definierte Interaktionsereignisse, die keine Formular-, Chat- oder sonstigen Inhaltsdaten enthalten. Umami setzt dabei keine Analyse-Cookies. IP-Adresse und User-Agent werden technisch zur Bildung einer anonymen Sitzungskennung verwendet; die rohe IP-Adresse wird nicht im Analysedatensatz gespeichert.

Die Analysedaten verbleiben auf unserer EU-basierten Infrastruktur, werden nicht zur Erstellung personenbezogener Profile genutzt und nach 30 Monaten gelöscht oder dauerhaft anonymisiert. Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO. Unser berechtigtes Interesse liegt in einer datensparsamen Reichweitenmessung, Fehlererkennung und Verbesserung unserer öffentlichen Angebote. Sie können dieser Verarbeitung aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit widersprechen.

Weitere Informationen: Dokumentation von Umami.

07 Kontakt und eMail

Wenn Sie uns per eMail, Formular oder über eine innerhalb unserer Angebote bereitgestellte Kontaktfunktion schreiben, verarbeiten wir die von Ihnen übermittelten Angaben. Dazu können Name, Kontaktdaten, Betreff, Nachricht, Anhänge, Zeitpunkt und technische Zustellinformationen gehören.

Die Verarbeitung erfolgt zur Bearbeitung Ihrer Anfrage. Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO, wenn es um einen Vertrag oder vorvertragliche Maßnahmen geht, andernfalls Art. 6 Abs. 1 lit. f DSGVO aufgrund unseres Interesses an einer effizienten und nachvollziehbaren Kommunikation. Eine ausdrücklich einwilligungsabhängige Verarbeitung beruht auf Art. 6 Abs. 1 lit. a DSGVO.

Unsere geschäftliche eMail-Infrastruktur wird selbst verwaltet und auf EU-basierter Hosting-Infrastruktur betrieben. Anfragen werden gelöscht, sobald sie abschließend bearbeitet sind und keine Vertrags-, Nachweis- oder gesetzlichen Aufbewahrungsgründe mehr bestehen.

08 Kunden-, Konto- und Vertragsdaten

Zur Anbahnung, Durchführung und Beendigung von Verträgen sowie zur Bereitstellung von GRID verarbeiten wir erforderliche Stamm-, Kontakt-, Vertrags-, Projekt-, Konto-, Nutzungs-, Abrechnungs- und Kommunikationsdaten. Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO. Steuer- und handelsrechtlich notwendige Unterlagen verarbeiten wir nach Art. 6 Abs. 1 lit. c DSGVO.

Operative Kunden- und Projektdaten werden grundsätzlich spätestens sechs Monate nach Ende der Geschäftsbeziehung gelöscht oder anonymisiert, sofern sie nicht mehr zur Übergabe, Nachbetreuung oder Rechtsverteidigung benötigt werden. Gesetzliche Aufbewahrungsfristen betragen je nach Dokument regelmäßig sechs, acht oder zehn Jahre. Maßgeblich sind insbesondere § 147 AO und § 257 HGB.

09 Support-Chat mit Crisp

Für Einrichtungshilfe, Support und servicebezogene Kommunikation verwenden wir Crisp, angeboten von Crisp IM SAS, Frankreich. Wenn Crisp auf einer dafür vorgesehenen Seite geladen oder der Chat genutzt wird, können Name, eMail-Adresse, Telefonnummer und weitere freiwillige Kontaktdaten, Nachrichten und Anhänge, IP-Adresse, Browser- und Geräteinformationen, besuchte Seite, Zeitpunkt, Konto- oder Projektbezug, Supportverlauf, Segmente und von uns hinterlegte Serviceattribute verarbeitet werden.

Wir verwenden Crisp-Funktionen zur Einrichtung, Beantwortung, Zuordnung, Automatisierung, Qualitätssicherung und Auswertung von Supportvorgängen. Dazu gehören Hugo AI und Magic Browse. Hugo AI kann den für eine Anfrage notwendigen Gesprächs- und Hilfekontext verarbeiten, um Antworten, Zusammenfassungen oder eine Weiterleitung vorzubereiten. Sie können jederzeit die Bearbeitung durch eine Person verlangen. Es finden keine ausschließlich automatisierten Entscheidungen mit rechtlicher oder vergleichbar erheblicher Wirkung statt.

Magic Browse ermöglicht autorisierten Supportmitarbeitenden, den aktuellen Zustand der von Ihnen geöffneten Seite im Rahmen einer konkreten Supportanfrage einzusehen, um Sie schrittweise zu unterstützen. Die Funktion wird nicht dazu eingesetzt, Passwörter, Zahlungsdaten oder sachfremde Inhalte zu erfassen. Bitte übermitteln Sie im Chat keine besonderen Kategorien personenbezogener Daten, sofern dies nicht ausdrücklich erforderlich und vereinbart ist.

Die Verarbeitung beruht auf Art. 6 Abs. 1 lit. b DSGVO, soweit sie für vorvertragliche Maßnahmen oder die Vertragserfüllung erforderlich ist, andernfalls auf Art. 6 Abs. 1 lit. f DSGVO. Unser berechtigtes Interesse liegt in einem schnellen, kontextbezogenen Support. Soweit für das Laden oder eine optionale Funktion eine Einwilligung erforderlich ist, sind § 25 Abs. 1 TDDDG und Art. 6 Abs. 1 lit. a DSGVO die Rechtsgrundlagen.

Crisp verwendet funktionale Cookies mit einer regulären Speicherdauer von sechs Monaten. Supportinhalte werden bis zur Erledigung der Anfrage und – bei einem bestehenden Kundenverhältnis – solange gespeichert,

wie sie für den nachvollziehbaren Support benötigt werden. Danach werden sie nach unseren Löschregeln gelöscht oder anonymisiert, sofern keine Vertrags-, Nachweis- oder gesetzlichen Gründe entgegenstehen.

Weitere Informationen: Datenschutzerklärung von Crisp und Cookie-Hinweise von Crisp.

10 Videotermine mit Whereby

Für vereinbarte Video- und Supporttermine nutzen wir Whereby Embedded. Die Benutzeroberfläche rund um den Termin ist in GRID eingebettet; die eigentliche Videokonferenz wird jedoch von Whereby AS, Norwegen, als externer Dienst bereitgestellt.

Verarbeitet werden können Termin- und Raumdaten, ein freiwillig angegebener Anzeigename, IP-Adresse, Browser- und Geräteangaben, Verbindungs- und Qualitätsdaten sowie während des Termins übertragene Audio-, Video- und Chatdaten. Audio- und Videoinhalte werden von uns nicht aufgezeichnet oder dauerhaft gespeichert, sofern eine Aufzeichnung nicht im Einzelfall ausdrücklich angekündigt und aktiviert wird.

Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO für vorvertragliche oder vertragliche Termine, andernfalls Art. 6 Abs. 1 lit. f DSGVO aufgrund unseres Interesses an einer direkten und sicheren Fernkommunikation. Norwegen gehört zum Europäischen Wirtschaftsraum.

Weitere Informationen: Datenschutzerklärung von Whereby und Datenverarbeitungsvereinbarung von Whereby.

11 Fehleranalyse

Zur Erkennung und Behebung technischer Fehler verwenden wir eine selbst gehostete Fehleranalyse auf unserer EU-basierten Infrastruktur. Je nach Fehler werden Fehlertyp und -meldung, Stacktrace, aufgerufener Pfad, Zeitpunkt, Browser- und Geräteangaben sowie technische Anfrage- oder Kontokennungen verarbeitet, sofern diese im konkreten Fehlerkontext vorhanden sind.

Die Übermittlung personenbezogener Inhalte ist standardmäßig deaktiviert. Fehlerdaten werden grundsätzlich nach 90 Tagen gelöscht. Für einen konkreten, noch offenen Fehler- oder Sicherheitsfall können erforderliche Ausschnitte bis zur abschließenden Behebung und Dokumentation länger aufbewahrt werden.

Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO. Unser berechtigtes Interesse liegt in der Stabilität, Sicherheit und fortlaufenden Verbesserung unserer Anwendungen.

12 Schutz vor Angriffen und Missbrauch

Wir analysieren sicherheitsrelevante Ereignisse automatisiert, um Angriffe, automatisierten Missbrauch und unberechtigte Zugriffe zu erkennen und abzuwehren. Dabei können auffällige IP-Adressen, Zeitstempel, angegriffener Dienst, erkannte Angriffsmuster, technische Kontextdaten sowie die daraus abgeleitete Sperrentscheidung verarbeitet werden.

Hierfür nutzen wir CrowdSec. Sicherheitsentscheidungen und die zugehörigen technischen Indikatoren können mit der CrowdSec-Infrastruktur abgeglichen oder dorthin übermittelt werden, damit bekannte Angriffe gemeinschaftlich erkannt werden. Für die gemeinschaftlich verarbeiteten kontextualisierten IP-Adressen beschreibt CrowdSec eine gemeinsame Verantwortlichkeit mit den Mitgliedern seines Netzwerks; über die konkrete Sperre auf unseren Systemen entscheiden wir. Eine automatische Sperre begrenzt ausschließlich den technischen Zugriff auf unsere Systeme und entfaltet keine rechtliche oder vergleichbar erhebliche Wirkung.

Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO. Unsere berechtigten Interessen sind die Netzwerk- und Informationssicherheit, der Schutz von Kunden- und Unternehmensdaten sowie die Abwehr von Betrug und Missbrauch. Lokale Ereignisse unterliegen den im Abschnitt „Serverprotokolle“ beschriebenen Fristen. CrowdSec speichert IP-Adressen, von denen ein Angriff ausging, nach eigenen Angaben grundsätzlich

höchstens drei Monate in vollständiger Form und verringert danach schrittweise ihren Personenbezug.

Weitere Informationen: Datenschutzerklärung von CrowdSec.

13 Verschlüsselte Backups

Zum Schutz vor Datenverlust erstellen wir verschlüsselte Backups produktiver Systeme. Die Sicherungen werden verschlüsselt an Cloudflare R2 übertragen und für eine Speicherung innerhalb der EU-Datenjurisdiktion konfiguriert. Cloudflare verarbeitet die verschlüsselten Sicherungsobjekte als Infrastruktur- und Auftragsverarbeiter.

Backups folgen einem rollierenden Sicherungs- und Löschkonzept. Wird ein Datensatz im Primärsystem gelöscht, kann eine verschlüsselte Kopie bis zum planmäßigen Ablauf des jeweiligen Sicherungsstands enthalten bleiben. Eine Wiederherstellung erfolgt nur bei einem technischen Ausfall, Sicherheitsvorfall oder einer notwendigen Datenwiederherstellung; anschließend greifen die regulären Löschregeln erneut.

Rechtsgrundlagen sind Art. 6 Abs. 1 lit. b und lit. f DSGVO sowie – bei gesetzlich aufzubewahrenden Unterlagen – Art. 6 Abs. 1 lit. c DSGVO. Weitere Informationen: Datenschutzerklärung von Cloudflare.

14 Community-Server

Wir betreiben kostenfrei nutzbare Community-Server für ARK: Survival Ascended, 7 Days to Die, Minecraft, Hytale und Enshrouded sowie einen privaten World of Warcraft-Server. Diese Systeme werden von unseren geschäftlichen Produktivsystemen getrennt auf Infrastruktur von ZAP-Hosting betrieben.

Bei der Nutzung können IP-Adresse, Verbindungszeit, Plattform-, Konto-, Spieler- und Charaktername oder -kennung, Spielstand, Welt- und Gameplaydaten, Chatnachrichten, technische Server- und Anti-Cheat-Protokolle sowie Moderations-, Verwarnungs- und Sperrinformationen verarbeitet werden. Welche Daten konkret anfallen, hängt vom jeweiligen Spiel und der verwendeten Plattform ab.

Wir verarbeiten diese Daten zur Bereitstellung des Servers, Speicherung des Spielfortschritts, Multiplayer-Koordination, Fehlerbehebung, Moderation sowie zur Abwehr von Betrug, Cheating, Belästigung und technischen Angriffen. Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO für die angeforderte Servernutzung und Art. 6 Abs. 1 lit. f DSGVO für Sicherheit, Stabilität und faire Community-Regeln.

Verbindungs- und technische Sicherheitsprotokolle werden gelöscht, sobald sie für Betrieb und Schutz nicht mehr erforderlich sind. Spielstände bestehen grundsätzlich für die aktive Laufzeit der jeweiligen Welt oder Teilnahme. Moderations- und Sperrdaten können solange aufbewahrt werden, wie dies zur Durchsetzung einer Maßnahme, zum Schutz der Community oder zur Verteidigung von Ansprüchen erforderlich ist. Spiel- und Plattformanbieter verarbeiten Daten nach ihren eigenen Bedingungen, wenn Sie deren Konten, Software oder Authentifizierung nutzen.

15 Empfänger und internationale Übermittlungen

Innerhalb von VICRONIX erhalten nur Personen Zugriff, die ihn für ihre jeweilige Aufgabe benötigen. Externe Empfänger sind – soweit für den konkreten Vorgang erforderlich – insbesondere Hosting- und Speicheranbieter, Kommunikations- und Supportdienste, Videokonferenzanbieter, Sicherheitsdienste, Steuer- und Rechtsberatung, Zahlungs- oder Abrechnungsstellen sowie Behörden bei gesetzlicher Verpflichtung.

Dienstleister werden sorgfältig ausgewählt und, soweit sie in unserem Auftrag handeln, durch Verträge nach Art. 28 DSGVO gebunden. Einige Anbieter können technische Unterauftragnehmer einsetzen oder einzelne Daten außerhalb des Europäischen Wirtschaftsraums verarbeiten. Soweit kein Angemessenheitsbeschluss besteht, stützen wir solche Übermittlungen insbesondere auf EU-Standardvertragsklauseln und zusätzliche Schutzmaßnahmen. Einzelheiten und Kopien verfügbarer Garantien können Sie über die oben genannten Kontaktdaten anfordern.

Die EU-basierte Speicherung unserer Kernsysteme bedeutet daher nicht, dass bei jeder optionalen Kommunikations-, Sicherheits- oder Supportfunktion ausnahmslos jede technische Verarbeitung ausschließlich innerhalb der EU stattfindet.

16 Speicherdauer

Sofern in dieser Erklärung keine feste Frist genannt ist, speichern wir personenbezogene Daten nur solange, wie sie für den jeweiligen Zweck benötigt werden. Danach werden sie gelöscht oder anonymisiert, sofern keine gesetzliche Aufbewahrung, laufende Vertragsabwicklung, Einwilligung oder notwendige Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen entgegensteht.

Wesentliche Regelfristen sind: sieben Tage für normale Betriebsprotokolle, 90 Tage für Fehlerdaten, 30 Monate für Umami-Analysedaten, sechs Monate für Crisp-Funktionscookies, grundsätzlich sechs Monate für operative Kunden- und Projektdaten nach Vertragsende sowie sechs Monate für Bewerbungsdaten nach Abschluss des Verfahrens. Steuer- und handelsrechtliche Unterlagen werden abhängig von ihrer Art regelmäßig sechs, acht oder zehn Jahre aufbewahrt.

17 Bewerbungen

Wenn Sie sich bei uns bewerben, verarbeiten wir die für die Entscheidung über ein Beschäftigungsverhältnis erforderlichen Daten. Dazu gehören insbesondere Name und Kontaktdaten, Lebenslauf, Anschreiben, Zeugnisse, Qualifikationen sowie die zugehörige Kommunikation.

Rechtsgrundlage ist § 26 Abs. 1 BDSG in Verbindung mit Art. 6 Abs. 1 lit. b DSGVO. Für eine freiwillige Aufnahme in einen Bewerberpool ist Art. 6 Abs. 1 lit. a DSGVO die Rechtsgrundlage; die Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Nach Abschluss des Bewerbungsverfahrens löschen wir die Daten spätestens sechs Monate nach Mitteilung der Entscheidung, sofern keine gesetzlichen Pflichten, Rechtsansprüche oder eine wirksame Einwilligung in eine längere Speicherung entgegenstehen.

18 Ihre Rechte

Unter den gesetzlichen Voraussetzungen haben Sie das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragbarkeit. Sie können einer Verarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO aus Gründen widersprechen, die sich aus Ihrer besonderen Situation ergeben. Eine Einwilligung können Sie jederzeit mit Wirkung für die Zukunft widerrufen; die Rechtmäßigkeit der bis zum Widerruf erfolgten Verarbeitung bleibt unberührt.

Zur Ausübung Ihrer Rechte genügt eine formlose Nachricht an hello@vicronix.de. Damit wir Daten nicht an Unbefugte herausgeben oder verändern, können wir einen angemessenen Identitätsnachweis verlangen.

Sie haben außerdem das Recht auf Beschwerde bei einer Datenschutzaufsichtsbehörde. Für uns ist insbesondere zuständig:

Berliner Beauftragte für Datenschutz und Informationsfreiheit

Alt-Moabit 59-61

10555 Berlin

eMail: mailbox@datenschutz-berlin.de

www.datenschutz-berlin.de

19 Änderungen

Wir aktualisieren diese Datenschutzerklärung, wenn sich unsere Verarbeitung, unsere Dienste oder die rechtlichen Anforderungen ändern. Die jeweils aktuelle Fassung ist unter dieser Adresse verfügbar. Über wesentliche Änderungen informieren wir zusätzlich, soweit dies gesetzlich erforderlich oder nach Art der Änderung angemessen ist.