

PRIVACY POLICY SANDGRAIN – WEBSITE

1. INTRODUCTION

SandGrain B.V., having its corporate seat and office at High Tech Campus 9 Beta Building, 5656 AE Eindhoven, the Netherlands, and registered with the Dutch Chamber of Commerce under number 75990741 (**SandGrain, we, us or our**), respects the privacy of visitors and users of its website www.sandgrain.com and related webpages, forms and online resources (the **Website**).

In this privacy policy, we explain which personal data we collect when you visit or use the Website, contact us, request information, submit a vulnerability report, or otherwise interact with us through the Website. We also explain why we process such personal data, on which legal basis we do so, with whom we may share it, how long we retain it and which rights you have.

This privacy policy applies only to the processing of personal data through our public website. The processing of personal data in connection with the CyberRock platform is governed by the separate privacy information made available within the CyberRock platform.

Please read this privacy policy carefully before using the Website.

2. LEGAL BASES FOR PROCESSING

We process your personal data on the basis of one or more of the following legal bases under the General Data Protection Regulation (GDPR):

- I. your consent;
- II. the performance of a contract or steps prior to entering into a contract;
- III. compliance with a legal obligation; and/or
- IV. our legitimate interest.

Our legitimate interests include, among other things: responding to requests, business development, marketing, website security, fraud and misuse prevention, IT security, vulnerability handling, analytics, improvement of our Website and services, internal management, legal affairs and business operations. Below, we specify which legal basis applies to each category of processing.

3. PERSONAL DATA WE PROCESS AND PURPOSES OF PROCESSING

Access to the SandGrain portal: The Website provides access to the SandGrain portal (portal.sandgrain.eu), where you can register for an account, log in and access materials such as user documentation, knowledge base articles, whitepapers, product updates and other resources. If you register for or log in to the SandGrain portal, we may process the following personal data: first name and last name, email address, telephone number, company name email address (used as login credential); password (stored in encrypted form), access and usage logs, including pages visited, materials accessed and download activity. We process this data to create and

manage your portal account, authenticate your identity, provide access to the requested materials and resources, manage and secure access to the portal, understand interest in our products and services, follow up where appropriate and improve our content and communications. Depending on the circumstances, legal basis I., II. and/or IV. applies.

Website visits and technical data: When you visit the Website, we may process technical data relating to your visit, such as: IP address, browser type and version, device type, operating system, pages visited, date and time of visit, referring website, interaction data, such as clicks, scrolling behaviour and navigation patterns, session recordings reflecting your interactions with the Website (such as mouse movements, clicks and scrolling), demographic and interest data (such as age range and interests) derived from analytics tools, cookie identifiers and similar online identifiers. We process this data to operate and secure the Website, detect and prevent misuse, understand how the Website is used, improve the Website and our services, and maintain the performance and functionality of the Website. Depending on the circumstances, legal basis I. and/or IV. applies.

Contact forms and general enquiries: If you contact us through the Website, by email or otherwise, we may process the personal data you provide to us, including: first name and last name, email address, telephone number, company name, job title or role, country, message content, any other personal data included in your communication. We process this data to respond to your enquiry, communicate with you, provide information, manage our relationship with you, follow up on business opportunities and improve our communication processes. Depending on the circumstances, legal basis II. and/or IV. applies. Where you consent to being contacted for specific purposes, legal basis I. may also apply.

Demo, trial and product information requests: If you request a demo, trial, meeting, product information or commercial follow-up through the Website, we may process: first name and last name, email address, telephone number, company name, country, job title or role, areas of interest, trial or project description, correspondence with us, other information you choose to provide. We process this data to assess and respond to your request, arrange a demo or trial, provide relevant information, communicate with you, prepare for potential commercial cooperation and manage our business relationship with you. Depending on the circumstances, legal basis II. and/or IV. applies.

Vulnerability reports and security submissions: The Website allows you to submit information about vulnerabilities, security issues or related concerns, including by attaching files. If you submit a vulnerability report or security-related information, we may process: your name, email address, company or organization, role or job title, technical information about the reported vulnerability, files, screenshots, logs, code snippets or other attachments you submit, IP addresses, system identifiers, device identifiers, URLs, timestamps or other technical data included in your submission, correspondence and follow-up communications with you. You should avoid including unnecessary personal data or confidential third-party information in vulnerability reports or attachments. We process this data to receive, assess, validate, prioritize and remediate vulnerability reports, communicate with the reporter, protect the security of our systems, products and services, prevent misuse and maintain appropriate records of security issues. Depending on the circumstances, legal basis II., III. and/or IV. applies. If a vulnerability report contains personal data relating to third parties, we process such data only to the extent necessary for the handling, investigation, mitigation and documentation of the relevant security issue.

Marketing communications: To the extent permitted under applicable law, we may use your contact details to send you marketing communications, such as newsletters, product updates, event invitations or other business communications. If required by law, we will ask for your consent before sending such communications. You can unsubscribe at any time by using the unsubscribe link included in the communication or by contacting us. Depending on the circumstances, legal basis I. and/or IV. applies.

Compliance with legal obligations: We may process personal data where this is necessary to comply with applicable laws and regulations, lawful requests from authorities, court orders, tax obligations, accounting obligations, sanctions and export control requirements or other legal obligations. Legal basis III. applies.

Fraud detection, misuse prevention and legal protection: We may process personal data for the purpose of detecting, preventing and responding to fraud, misuse, unauthorized access, security threats, unlawful activities, violations of our terms or other harmful conduct, and to protect our rights, property, systems and legal position.

Depending on the circumstances, legal basis III. and/or IV. applies.

4. COOKIES

The Website may use cookies and similar technologies to operate the Website, improve functionality, analyze Website usage, enhance security and support marketing and business development activities.

Cookies may include:

- strictly necessary cookies, which are required for the Website to function properly;
- functional cookies, which remember preferences and improve usability;
- analytics cookies, which help us understand how visitors use the Website;
- marketing or tracking cookies, which may be used to measure engagement and improve communications;

Where required by law, we will ask for your consent before placing non-essential cookies or similar technologies. More information about the specific cookies used on the Website, their purposes and your choices can be found in our cookie policy, available at <https://sandgrain.com/cookie-policy/>.

5. SHARING PERSONAL DATA WITH THIRD PARTIES

We may share your personal data with third parties in the situations described below, to the extent permitted by applicable law.

External service providers

We may share your personal data with external service providers that perform services on our behalf, to the extent necessary for the purposes described in this privacy policy. This includes, among others, providers of hosting and cloud infrastructure, IT and security services, analytics and diagnostics, CRM and communications tools, billing and payment services, customer support tools, professional advisory services, and email delivery

and marketing services. We only share personal data with service providers that offer appropriate safeguards for the protection of your personal data. Where required, we enter into a data processing agreement with such providers, ensuring that personal data is processed only on our instructions and under our responsibility. Depending on the circumstances, legal basis II. and/or IV. applies.

In particular, we currently make use of the following third-party services in connection with the Website, subject to the actual configuration of the Website and the cookie choices made by the visitor:

- **Microsoft Clarity:** used for behavioural analytics, session recording and heatmap generation in connection with the Website. Microsoft Clarity is provided by Microsoft Ireland Operations Ltd., One Microsoft Place, Leopardstown, Dublin 18, Ireland, with processing taking place in the USA. Personal data processed includes (pseudonymised) IP address, mouse movements, scroll depth, clicks, session replay data, device/browser information and heatmap data. Personal data may be transferred outside the EEA on the basis of the EU-US Data Privacy Framework (Article 45 GDPR). Depending on the circumstances, legal basis I. and/or IV. applies.
- **Google Analytics 4:** used for website analytics, measurement of user behaviour and conversion tracking. Google Analytics 4 is provided by Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, with processing taking place primarily in the USA. Personal data processed includes IP address (anonymised by default), cookie identifiers (`_ga`, `_gid`), device/browser information, page URLs, events and approximate location, and may include demographic and interest data where enabled. Personal data may be transferred outside the EEA on the basis of the EU-US Data Privacy Framework (Article 45 GDPR), with EU Standard Contractual Clauses available as a supplementary safeguard. Depending on the circumstances, legal basis I. and/or IV. applies.
- **Leadinfo:** used for B2B lead identification and company-level website visitor enrichment. Leadinfo is provided by Leadinfo B.V. (Dutch Chamber of Commerce no. 78116643), the Netherlands, with processing taking place within the EU (Ireland and Germany). Personal data processed includes IP address (used to resolve company data and not stored), pseudonymous visitor data and publicly available company identifiers. No transfer outside the EU/EEA takes place.
- **Salesforce (CRM):** used for customer relationship management, data storage and management of our sales pipeline. Salesforce is provided by Salesforce, Inc., 415 Mission Street, San Francisco, CA 94105, USA, with processing taking place in the USA (EU data residency available via Hyperforce). Personal data processed includes name, email address, telephone number, company, job title, contact history and CRM records. Personal data may be transferred outside the EEA on the basis of the EU-US Data Privacy Framework (certified), EU Standard Contractual Clauses (2021) and Salesforce's Processor Binding Corporate Rules (Article 46 GDPR). Depending on the circumstances, legal basis II. and/or IV. applies.
- **Google Tag Manager:** used for tag management and deployment of third-party scripts; it does not independently collect data or set cookies itself. Google Tag Manager is provided by Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, with processing taking place in the USA. Personal data transmitted on script load may include IP address, device/browser information and referrer URL. Personal data may be transferred outside the EEA on the basis of the EU-US Data Privacy Framework (Article 45 GDPR) and EU Standard Contractual Clauses.

- **Cookiebot:** used for cookie consent management, consent logging and documentation. Cookiebot is provided by Usercentrics A/S (formerly Cybot A/S), Havnegade 39, 1058 Copenhagen, Denmark (CVR 34624607), with processing taking place within the EU/EEA. Personal data processed includes anonymised IP address (last three digits zeroed), cookie consent key, consent timestamp, banner version and user location (country). No transfer outside the EU/EEA takes place for the core service; any use of a content delivery network (Akamai) may involve EU Standard Contractual Clauses.
- **Combell** (hosting): used for web hosting, server log management and infrastructure provision. Combell is provided by Combell NV, Skaldenstraat 121, 9042 Ghent, Belgium (CBE 0541.977.701), with processing taking place in Belgium (EU). Personal data processed includes IP address and server log data (date, time, requested pages, browser information). No transfer outside the EU/EEA takes place.
- **Google reCAPTCHA:** used for bot detection, spam prevention and risk scoring (automated profiling). Google reCAPTCHA is provided by Google LLC, 1600 Amphitheatre Pkwy, Mountain View, CA 94043, USA, with processing taking place in the USA (from April 2026 Google acts as data processor and a data processing agreement is required). Personal data processed includes IP address, browser/device fingerprint, mouse movements, interaction patterns, the _greaptcha cookie and referrer URL. Personal data may be transferred outside the EEA on the basis of the EU-US Data Privacy Framework (Article 45 GDPR) and EU Standard Contractual Clauses.
- **Wordfence:** used for WordPress security, malware detection, brute-force protection and threat intelligence. Wordfence is provided by Defiant, Inc., 800 5th Ave Ste 4100, Seattle, WA 98104, USA, with processing taking place in the USA. Personal data processed includes IP addresses of website visitors, login attempts, blocked requests and firewall event data. Personal data may be transferred outside the EEA on the basis of EU Standard Contractual Clauses (2021 EU Commission clauses, Article 46 GDPR), which Defiant has opted for instead of the Data Privacy Framework.
- **Salesforce** (web-to-lead): used for lead capture, CRM form submission and contact creation. Salesforce is provided by Salesforce, Inc., 415 Mission Street, San Francisco, CA 94105, USA, with processing taking place in the USA (EU data residency available via Hyperforce). Personal data processed includes name, email address, telephone number, company, job title and form submission data. Personal data may be transferred outside the EEA on the basis of the EU-US Data Privacy Framework (certified), EU Standard Contractual Clauses (2021) and Salesforce's Processor Binding Corporate Rules (Article 46 GDPR).
- **YouTube** (embedded): used for video hosting and playback, user preference tracking and, where enabled, ad personalisation. YouTube is provided by Google LLC, 1600 Amphitheatre Pkwy, Mountain View, CA 94043, USA (YouTube LLC is a Google subsidiary), with processing taking place in the USA. Where consent is given, personal data processed includes IP address, device/browser information, viewing behaviour and the VISITOR_INFO, YSC and yt-remote-* cookies. Personal data may be transferred outside the EEA on the basis of the EU-US Data Privacy Framework (Article 45 GDPR) and EU Standard Contractual Clauses; the youtube-nocookie.com embed is used to minimise data before consent. Depending on the circumstances, legal basis I. and/or IV. applies.

Competent authorities

We may disclose personal data to law enforcement authorities, supervisory authorities, courts, regulators or other government bodies where we are legally required to do so or where such disclosure is strictly necessary for the prevention, detection or prosecution of criminal offences, fraud or other unlawful conduct. Legal basis III. and/or IV. applies.

Corporate transactions

We may transfer your personal data to third parties in the event of a merger, acquisition, reorganization, financing transaction, sale of assets or insolvency. Where required by applicable law, we will take the necessary steps to protect your rights, including requesting your prior consent where required. Legal basis IV. applies.

6. INTERNATIONAL TRANSFER OF PERSONAL DATA

The Website is managed and operated primarily from within the European Economic Area (EEA). If personal data are transferred to a third party outside the EEA, this will only take place where such transfer is permitted under applicable law, and only to a country that the European Commission has determined provides an adequate level of protection for personal data. Where the country concerned does not provide an adequate level of protection, we will ensure that the legally required safeguards are in place, such as the execution of standard contractual clauses approved by the European Commission.

At the time of drafting this privacy policy, several services used in connection with the Website process personal data outside the EEA, in particular in the United States (including Microsoft Clarity, Google Analytics 4, Salesforce, Google Tag Manager, Google reCAPTCHA, Wordfence and YouTube). Other services process personal data exclusively within the EU/EEA (including Leadinfo, Cookiebot and Combell). These transfers take place on the basis of the EU-US Data Privacy Framework and/or EU Standard Contractual Clauses, as further specified in paragraph 5 of this privacy policy and, where relevant, in our cookie policy.

7. RETENTION PERIODS

We do not retain personal data longer than permitted under applicable law or longer than necessary for the purposes for which the data was collected and processed.

In general:

- i. contact and enquiry data are retained for as long as necessary to handle and follow up on the relevant request;
- ii. portal account data are retained for as long as your account remains active and, following deactivation or deletion of your account, for a period of 1 year, or for such longer period as may be necessary for the purposes for which the data was collected, including the resolution of any outstanding matters;
- iii. demo, trial and commercial communication data are retained for as long as necessary for the relevant relationship, opportunity or communication;

- iv. marketing data are retained until you unsubscribe or object, unless we are legally permitted or required to retain certain data for a longer period;
- v. vulnerability reports and related security communications are retained for as long as necessary to investigate, remediate and document the relevant security issue and protect our systems and legal position;
- vi. website analytics data are retained in accordance with the settings of the relevant analytics tools and applicable cookie choices;
- vii. business, accounting and legal records are retained for as long as required under applicable statutory retention periods.

We may retain anonymized or aggregated data for a longer period for analytics, research, security improvement and service development purposes, provided such data can no longer be traced back to an individual. If you have questions about the retention period of specific personal data, please contact us using the details below.

8. SECURITY

We employ appropriate technical and organizational measures to protect personal data against unauthorized access, loss, alteration, destruction or disclosure. These measures include safeguards designed to secure our systems, Website, communications and data storage. Personal data is processed by authorized persons who are bound by confidentiality obligations and who require access for the performance of their tasks. Although we take security seriously, no website, transmission or storage system can be guaranteed to be fully secure. If you believe that you have identified a security issue, please report it to us responsibly and avoid including unnecessary personal data in your report.

9. YOUR RIGHTS

Subject to the conditions and limitations laid down in the GDPR, you have the right to:

- i. obtain information about the personal data we process about you and what we do with it;
- ii. access the personal data we hold about you;
- iii. have inaccurate or incomplete personal data corrected;
- iv. have your personal data deleted;
- v. restrict the processing of your personal data;
- vi. withdraw your consent, where processing is based on consent;
- vii. object to certain processing activities;
- viii. receive your personal data in a structured, commonly used and machine-readable format and, where applicable, have it transferred to another controller.

If you wish to exercise one or more of these rights, please contact us using the contact details below. We may ask you for additional information to verify your identity before responding to your request. We will respond to your request within one month of receipt. Depending on the complexity and number of requests, this period may be extended by up to two additional months, in which case we will inform you accordingly.

10. MINORS

The Website and our products and services are intended for business users and organizations. We do not target minors with the Website. If it appears that we have unlawfully collected personal data from a minor, we will take steps to delete such data as soon as reasonably possible. Legal representatives of minors have the same rights as described in section 9 of this privacy policy.

11. COMPLAINTS

If you have a complaint about the way we process your personal data, we would appreciate the opportunity to address it first. Please contact us using the contact details below. Under the GDPR, you also have the right to file a complaint directly with the Dutch Data Protection Authority regarding the way we process personal data via <https://klachten.autoriteitpersoonsgegevens.nl/>

12. CHANGES TO THIS PRIVACY POLICY

We reserve the right to amend this privacy policy from time to time. The most current version of this privacy policy will be made available on the Website. We recommend checking this privacy policy regularly to stay informed of any changes.

13. CONTACT DETAILS

If you have any questions about this privacy policy or about the way we process your personal data, please contact us using the following details:

SandGrain B.V.
High Tech Campus 9 Beta Building
5656 AE Eindhoven
The Netherlands
Chamber of Commerce: 75990741
Email: privacy@sandgrain.com

This privacy policy was last updated on: 23 June 2026