Interface Divide privacy policy

This policy explains how we process personal data when you visit Interface Divide, contact us, use our tools, join a course waitlist or subscribe to the newsletter. Reading it does not subscribe you to emails.

Controller and contact

Matthias Dunker operates Interface Divide and is responsible for the processing described here. Email: matthias@interfacedivide.com. Postal address: Platanenstraße 25, 40233 Düsseldorf, Germany.

Visiting and protecting the website

When you access the website, technical request information may be processed, including your IP address, browser information, the page requested and the time of the request. Vercel hosts the website and processes this information to deliver and protect it. Vercel functions are configured for Frankfurt, Germany (fra1). Our application database uses Neon through Vercel and is configured in AWS Europe Central 1 (Frankfurt, Germany); it stores the information described in the sections below. The proposed legal basis is Article 6(1)(f) GDPR: our legitimate interest in operating a reliable and secure website.

[Confirm any international transfers (including Vercel and Neon network and support access) and log retention periods before publication.]

Enquiries, appointments and services

Hetzner provides our business email service, and the mailbox is hosted in Germany. We keep ordinary enquiry emails for one year after the enquiry is resolved, unless a legal retention obligation requires us to keep them longer.

When you contact us or request consulting, workshops or courses, we process the contact details, messages, scheduling information and relevant project information you provide to respond, arrange or deliver the service. Where necessary to take steps at your request before a contract or perform a contract, the legal basis is Article 6(1)(b) GDPR. For other enquiries, the proposed basis is Article 6(1)(f) GDPR: our legitimate interest in responding to correspondence. Where applicable, records required by tax or accounting law are retained under Article 6(1)(c) GDPR.

Our appointment links take you to zcal's website. If you choose to book there, zcal processes the booking information and we receive the appointment details you submit. We use Google Calendar through a personal Google account to manage our calendar, including appointment details. Google states that information may be processed on servers outside the country where you live; its privacy information and transfer frameworks are described at https://policies.google.com/privacy and https://policies.google.com/privacy/frameworks. Google’s role, the applicable terms and safeguards for this account require review before publication. We keep booking and calendar records for one year after the appointment, unless a legal retention obligation requires us to keep them longer. zcal states in its data processing addendum that processing occurs in the United States and potentially other jurisdictions, and that it incorporates the European Commission standard contractual clauses. See https://zcal.co/privacy and https://zcal.co/dpa for zcal's information. The applicability

of these terms and any additional safeguards to our account must be reviewed before publication. Opening our contact menu does not itself load an embedded booking service.

Paid course delivery and payment providers have not yet been selected. This policy must be updated before such services are introduced.

[Confirm retention periods for other business email and service records, the applicable zcal and Google Calendar provider arrangements, and any international transfers before publication.]

Diagnostic tools and accounts

If you use an interactive diagnostic tool, we store a session identifier, your selections, answers and resulting assessment. Depending on what you submit, this may include organisation details, names or notes. If you sign in, the session may be associated with your account. Account information may include your name, email address, verification records and technical session information.

We use this information to provide and protect the requested tool or account. The proposed basis is Article 6(1)(b) GDPR where processing is necessary for a requested contractual service; otherwise, Article 6(1)(f) GDPR for our legitimate interest in providing and protecting the requested functionality. The assessment supports your own evaluation; it is not an automated decision about your legal rights or access to essential services.

The diagnostic tool uses a session cookie lasting up to 30 days and stores a session reference in your browser's local storage so you can resume. That reference remains until the application removes it or you clear browser storage. Sign-in uses session cookies. If the account consent flow is used, pending choices are temporarily stored in session storage. These records support the functionality you request and are separate from newsletter consent.

The planned retention period for diagnostic answers and results is one year after your last use of the tool. This deletion rule has not yet been implemented. Accounts are intended to remain active until you request deletion; information may be retained longer where required by law. The account deletion process and any exceptions must be verified before publication.

[Confirm the legal basis and browser-storage requirements for each diagnostic and account feature available at launch, and implement the diagnostic retention rule.]

Course waitlist and newsletter

You can separately request course waitlist emails about the course launch, availability and related launch information, and newsletter emails about articles, experiments, tools and offers relating to AI interfaces and design systems. Newsletter emails may advertise Interface Divide's own products and services. Newsletter consent is optional when joining the course waitlist. Providing your email address is voluntary but necessary to receive the emails you request.

The legal basis for sending these emails is your consent under Article 6(1)(a) GDPR. We send a confirmation email and activate the selected subscription only after you confirm your email address. We record the selected purpose, document version and integrity reference, signup and confirmation times, and any withdrawal to administer and demonstrate your choices. The proposed basis for keeping this evidence is Article 6(1)(f) GDPR, our legitimate interest in documenting consent and responding to related claims, subject to review of the applicable requirements.

We also record the signup page, source, referring website origin and campaign parameters if provided. These remain in our application database and help us understand which pages and campaigns lead to signups. The proposed basis is Article 6(1)(f) GDPR, our legitimate interest in understanding and improving our campaigns. We temporarily use a hashed network identifier to limit repeated signup attempts, on the proposed basis of Article 6(1)(f) GDPR, our legitimate interest in preventing misuse.

Emailit is our intended provider for sending confirmation emails and managing confirmed contacts and audience memberships. Its consent records include project, document and version references and the confirmation time. Reoon is our intended provider for checking the email address before a confirmation email is sent. Both receive your email address for these purposes. Emailit states that workspace data is stored and processed in Prague, Czech Republic. Its published default message-content retention for the Pay as you go plan is seven days; the setting for our workspace must be confirmed. Reoon states that submitted addresses and verification results are stored and processed in the EU and automatically deleted after 15 days, including API checks. Reoon also states that authorised staff in Bangladesh may access the data when needed for support or verification, and checks may pass through other countries.

You can withdraw either email consent at any time with effect for the future using the relevant unsubscribe link or by emailing matthias@interfacedivide.com. Withdrawal does not affect the lawfulness of processing based on consent before withdrawal. You do not have to withdraw course consent to withdraw newsletter consent. Emailit's campaign unsubscribe applies across its shared workspace and may also stop emails from other projects using that workspace.

A request to remove Interface Divide subscription data removes the application's signup and consent records and Interface Divide audience memberships and consent records in Emailit, subject to applicable retention obligations and any lawful need to retain minimal evidence of consent or withdrawal. A shared Emailit contact may remain where another project still uses it. Requests covering all projects are assessed separately.

Website analytics

When configured, we use a self-hosted Umami instance running in a Docker container on Strato infrastructure in Germany to understand visits and events such as waitlist form views, submissions and confirmations. Information can include the page, referrer, campaign information, event time and browser or device information. Umami uses technical request information to derive visitor and session statistics. In this configuration it does not use tracking cookies. Analytics data currently has no automatic deletion period. The planned retention period for detailed analytics data is 24 months, to support year-on-year comparisons; deletion must be implemented before this period can be represented as operational. We do not deliberately include email addresses or confirmation tokens in custom analytics events.

The proposed legal basis is Article 6(1)(f) GDPR: our legitimate interest in understanding and improving the website. The absence of tracking cookies does not by itself settle whether consent is required.

[Implement the 24-month analytics retention period and confirm whether consent is required under applicable law before publication.]

Providers and transfers outside the EEA

Providers supporting hosting, storage, email, verification, analytics and scheduling receive information needed for their services. Providers identified are Vercel (hosting), Neon (database), Hetzner (business email), Emailit, Reoon, zcal, Google Calendar, and Strato (hosting for self-hosted Umami); other infrastructure and business communication providers may also be involved.

Reoon's published data processing agreement incorporates European Commission standard contractual clauses for transfers where required. Its agreement and transfer terms, including their applicability to our account and any additional safeguards, must be reviewed before publication.

[Identify the remaining providers, their roles and processing locations. Confirm all transfers outside the European Economic Area, applicable adequacy decisions or other transfer safeguards, and how to obtain information or a copy of those safeguards before publication.]

Retention

Unconfirmed signup requests are scheduled for removal seven days after their confirmation links expire; links expire after 24 hours. Unused contact records associated with those requests are also removed. Temporary signup rate-limit records expire after one hour, and processed webhook receipt records are removed after 30 days. Active subscription details are planned to be kept until you unsubscribe, subject to applicable law. Confirmed subscription and consent evidence currently has no automatic expiry. Unsubscribing does not automatically erase every record. The planned rule is to stop emails for the withdrawn purpose and retain minimal evidence, such as the email address, consent reference and withdrawal date, for three years after the end of the calendar year of withdrawal, to document the choice and help prevent unwanted resubscription. Other data would be deleted sooner when no longer needed, subject to applicable legal obligations. This retention and deletion workflow has not yet been implemented and requires legal review.

[Review and implement the proposed retention periods or clear criteria for confirmed subscriptions and consent evidence, business records, contracts, accounts, diagnostic data, hosting logs and analytics. Account for applicable legal obligations and claims before publication.]

Your rights

Subject to the applicable legal conditions, you may request access to your personal data, correction, erasure, restriction of processing and data portability. You may withdraw consent at any time with effect for the future. You may complain to a data protection supervisory authority, including one in the EU member state where you live or work or where you believe an infringement occurred. To exercise your rights, contact matthias@interfacedivide.com.

Right to object: You may object at any time, on grounds relating to your particular situation, to processing based on Article 6(1)(f) GDPR. You may object to processing for direct marketing at any time; this also applies to related profiling, if any. If you object to direct marketing, your data will no longer be processed for that purpose.