

Privacy Notice – Template

GDPR-compliant template (Art. 13–14 GDPR) for SME websites · EN

Legally reviewed by a certified Data Protection Officer (CIPP/E) · Provided by ETHYX · Version 1.1 · July 2026

► **HOW TO USE THIS SECTION** This is a modular template. The CORE sections below are required for almost every business – keep them. Each OPTIONAL MODULE is marked with a blue box; keep only the ones that apply to you and delete the rest. Replace every [orange placeholder] with your own details, then delete this guidance box and all remaining guidance boxes before publishing. A simple website ends up around 4 pages; a complex one around 9. This template does not replace legal review – have your final notice checked by a qualified Data Protection Officer.

Before you publish – quick checklist

- Replaced every [placeholder] with your real details (company, address, email, authority).
- Kept only the optional modules that match the tools and processes you actually use.
- Listed your real processors (hosting, email, analytics, newsletter, CRM, etc.).
- Named the correct supervisory authority for your federal state (Bundesland).
- Deleted all guidance boxes and the optional-module markers themselves.
- Had the final version reviewed by a DPO or qualified counsel.

Privacy Notice

Last updated: [Month Year]

This privacy notice explains how [COMPANY NAME] ("we", "us") collects, uses and protects personal data when you visit our website [www.example.com] or otherwise interact with us. We process personal data in accordance with the EU General Data Protection Regulation (GDPR) and applicable national data protection law.

1. Who is responsible (Data Controller)

The controller responsible for data processing on this website is:

[COMPANY NAME]

[Legal form, e.g. GmbH]

[Street and number]

[Postal code, City]

[Country]

Email: [contact@example.com]

Phone: [+49 ...]

Represented by: [Managing Director / Geschäftsführer name]

► **HOW TO USE THIS SECTION** This is the legally required identity of the controller (Art. 13(1)(a) GDPR). Use the full legal entity, not a brand name. Include the Geschäftsführer / Managing Director.

2. Data Protection Officer

Our Data Protection Officer can be contacted at:

[DPO name or company]
[Address, if different]
Email: [dpo@example.com]

► **HOW TO USE THIS SECTION** A DPO is mandatory under Art. 37 GDPR (and § 38 BDSG) when, broadly, 20+ people are constantly engaged in automated processing, or your core activity involves large-scale or special-category processing. If you have not appointed a DPO and are not required to, delete this whole section. If ETHYX provides your external DPO, name them here.

3. Your rights as a data subject

Under the GDPR you have the following rights regarding your personal data. To exercise any of them, contact us at **[contact@example.com]**.

- Right of access (Art. 15) – to know what data we hold about you and to receive a copy.
- Right to rectification (Art. 16) – to have inaccurate data corrected.
- Right to erasure / “right to be forgotten” (Art. 17) – to have your data deleted where the legal conditions are met.
- Right to restriction of processing (Art. 18).
- Right to data portability (Art. 20) – to receive your data in a structured, machine-readable format.
- Right to object (Art. 21) – to object to processing based on legitimate interests, and to direct marketing at any time.
- Right to withdraw consent (Art. 7(3)) – where processing is based on consent, you can withdraw it at any time, without affecting the lawfulness of processing before withdrawal.

We will respond to any request within one month (Art. 12(3)).

4. Right to lodge a complaint

If you believe our processing of your personal data infringes the GDPR, you have the right to lodge a complaint with a supervisory authority (Art. 77). The authority responsible for us is:

[Name of the supervisory authority of your federal state]
[Address]
[Website]

► **HOW TO USE THIS SECTION** In Germany each Bundesland has its own authority (e.g. Berlin: Berliner Beauftragte für Datenschutz und Informationsfreiheit; Bavaria: BayLDA). Name the one for the state where your company is based. You can also reference the data subject's own local authority.

5. Visiting our website (server log files)

What we process

When you visit our website, our hosting provider automatically collects and stores information in server log files that your browser transmits. This includes: browser type and version, operating system, referrer URL, host name of the accessing device, time of the server request, and IP address.

Legal basis and purpose

This data is processed on the basis of our legitimate interest (Art. 6(1)(f) GDPR) in the secure, stable and correct operation of our website. The data is not merged with other data sources.

Hosting

Our website is hosted by **[hosting provider name, address]**. The provider processes the data described above on our behalf as a processor under a data processing agreement (Art. 28 GDPR). Server logs are deleted after **[e.g. 7 / 30]** days.

► **HOW TO USE THIS SECTION** Name your real hosting provider. If they are outside the EU, see the Third-Country Transfers module below and add the safeguard. Adjust the log retention period to your provider's actual setting.

6. Contacting us (contact form & email)

If you contact us via our contact form or by email, the data you provide (e.g. name, email address, your message) is processed to handle your enquiry. The legal basis is Art. 6(1)(b) GDPR where your request relates to a contract, otherwise our legitimate interest in responding to enquiries (Art. 6(1)(f) GDPR). We retain this data until your enquiry is resolved and any applicable statutory retention periods have expired, after which it is deleted.

7. How long we keep your data

We process and store personal data only for as long as necessary for the purpose it was collected, or as required by statutory retention obligations. Under German commercial and tax law (§ 257 HGB, § 147 AO), business and accounting records must be retained for up to 10 years. Once a retention period expires, the corresponding data is routinely deleted.

8. Data security

We use appropriate technical and organisational measures (Art. 32 GDPR) to protect your data against unauthorised access, loss or manipulation. Our website uses SSL/TLS encryption, recognisable by the "https://" in the address bar. We review and update our security measures in line with technological developments.

9. Changes to this privacy notice

We may update this privacy notice to reflect changes in our processing or in legal requirements. The current version always applies and is available on this page. Last updated: **[Month Year]**.

Optional modules

► **HOW TO USE THIS SECTION** Everything below is OPTIONAL. Keep a module only if you actually use that tool or process. Move kept modules up into the numbered sequence above (and renumber), then delete this page heading, all module markers, and all guidance boxes.

◆ **OPTIONAL MODULE** NEWSLETTER – keep only if you send a marketing newsletter.

Newsletter

If you subscribe to our newsletter, we use the email address you provide to send you information about our products, services and offers. Subscription uses the double opt-in procedure: you receive a confirmation email and your subscription is only activated once you confirm. The legal basis is your consent (Art. 6(1)(a) GDPR). You can unsubscribe and withdraw your consent at any time via the link in every newsletter or by emailing [\[contact@example.com\]](mailto:contact@example.com). We store your consent record (timestamp) as evidence. Our newsletter is sent via [\[newsletter provider, e.g. HubSpot / Brevo\]](#), who acts as our processor under a data processing agreement.

► **HOW TO USE THIS SECTION** Name your real newsletter tool. If it is US-based (e.g. HubSpot, Mailchimp), also keep the Third-Country Transfers module.

◆ **OPTIONAL MODULE** COOKIES & WEB ANALYTICS – keep if you use analytics. Preset below = Matomo, cookieless.

Cookies and web analytics

Cookies

Our website uses only technically necessary cookies required for basic operation. These do not require consent (§ 25(2) TDDDG). [\[If you set non-essential cookies, you must obtain consent via a consent banner and describe them here.\]](#)

Web analytics (Matomo)

We use Matomo, an open-source web analytics tool, hosted on our own servers within the EU. Matomo is configured to run without cookies and anonymises your IP address (the last octet is removed) before storage. No data is transmitted to third parties. We use this data to understand how our website is used and to improve it. The legal basis is our legitimate interest (Art. 6(1)(f) GDPR) in a needs-based, optimised website. Because the configuration is cookieless and IP-anonymised, no consent is required.

► **HOW TO USE THIS SECTION** This preset matches a self-hosted, cookieless Matomo setup. If you use Google Analytics or any tool that sets cookies or transfers data to a third country, this section must be rewritten: you then need a consent banner, consent as the legal basis (Art. 6(1)(a)), and the Third-Country Transfers module.

◆ **OPTIONAL MODULE** SOCIAL MEDIA – keep if you run social media profiles or embed social content.

Social media presence

We maintain profiles on **[LinkedIn / Instagram / ...]**. When you interact with our profiles, the respective platform processes your personal data under its own privacy policy and as a controller (or joint controller) in its own right. We process the data you share with us on these platforms to communicate with you (Art. 6(1)(f) GDPR). For details of the platforms' processing, please see their privacy policies: **[link to each platform's policy]**.

◆ **OPTIONAL MODULE** JOB APPLICATIONS – keep if you receive applications via the website or email.

Job applications

If you apply for a position with us, we process the personal data in your application (CV, cover letter, references and related correspondence) to assess your suitability and conduct the recruitment process. The legal basis is Art. 6(1)(b) GDPR and § 26 BDSG (employment context). If your application is unsuccessful, we delete your data within **[6]** months, unless you have consented to inclusion in our talent pool or longer retention is legally required. Special-category data (Art. 9 GDPR), if voluntarily provided, is processed only where permitted under Art. 9(2)(b) GDPR.

◆ **OPTIONAL MODULE** PAYMENT PROVIDERS – keep if you sell online / take payments.

Payment processing

For purchases and paid services we use the following payment service providers: **[Stripe / PayPal / ...]**. When you choose a payment method, the data required to process the payment (e.g. name, payment details, amount) is transmitted to the relevant provider, who processes it under its own responsibility and privacy policy. The legal basis is contract performance (Art. 6(1)(b) GDPR).

◆ **OPTIONAL MODULE** AUTOMATED DECISIONS & PROFILING – keep if any tool scores, ranks or filters people (e.g. lead scoring, CV screening).

Automated decision-making and profiling

We use **[tool, e.g. our CRM's lead scoring / our applicant screening software]** to **[what it does, e.g. score sales leads / pre-sort incoming applications]**. The logic involved: **[main criteria in plain language]**. The significance and consequences for you: **[e.g. it influences the order in which applications are reviewed]**. We do not make decisions based solely on automated processing that produce legal or similarly significant effects for you; a member of our team reviews the outcome before any such decision is taken. Under Art. 22 GDPR you have the right not to be subject to a decision based solely on automated processing, and you can request human intervention, express your point of view and contest a decision via **[contact email]**.

► **HOW TO USE THIS SECTION** Keep this module if you use AI-assisted or rule-based tools that score, rank or filter people (lead scoring, CV screening, credit checks, chatbot triage) - Art. 13(2)(f) GDPR requires disclosing the existence of such processing, meaningful information about the logic, and the consequences. If a tool decides WITHOUT human review, seek advice before relying on this wording: Art. 22 permits that only under narrow conditions.

◆ **OPTIONAL MODULE** THIRD-COUNTRY TRANSFERS – keep if ANY processor is outside the EU/EEA (e.g. US tools).

Transfers to third countries

Some of the providers we use process data outside the European Economic Area (e.g. in the USA: **[list providers]**). Where this is the case, we ensure an adequate level of protection through one of the following safeguards: an EU Commission adequacy decision, or the EU Standard Contractual Clauses (Art. 46(2)(c) GDPR), supplemented where necessary by additional technical and organisational measures. You can request a copy of the relevant safeguards from us at **[contact@example.com]**.

► **HOW TO USE THIS SECTION** List the real providers that transfer data outside the EU (Google, Microsoft, Salesforce, HubSpot, Zoom, LinkedIn, Stripe, etc.) and the safeguard each relies on. This must match your ROPA.