

Privacy Notice Starter

A GDPR-shaped privacy notice for data-heavy products - written in plain language with bracketed placeholders and margin guidance, so you start from a real draft.

FRAMEWORK	TIME TO COMPLETE	VERSION
GDPR ART. 13-14	60 MINUTES	JULY 2026

How to use this

Replace every **[BRACKETED]** placeholder with your specifics and delete what doesn't apply. The grey guidance notes are for you - remove them before publishing. This is a starting point, not a finished, jurisdiction-checked notice: have it reviewed before you rely on it.

1 Who we are

[COMPANY LEGAL NAME] is the data controller for the personal data described in this notice. You can contact us at [PRIVACY EMAIL / ADDRESS]. [Our Data Protection Officer / privacy contact is [NAME / EMAIL].] [If required, our EU/UK representative is [NAME / CONTACT].]

Guidance

Give a real, monitored contact. If you're established outside the EU but offer goods/services to people in it, you may also need an EU representative.

2 What we collect & why

List each purpose with the data used and your lawful basis. Be specific.

Purpose	Data used	Lawful basis (GDPR Art. 6)
Provide the service & account	name, email, usage	Contract
Security & fraud prevention	device, logs, IP	Legitimate interests
Marketing (if opted in)	email, preferences	Consent
[ADD ROW]		

Guidance

Special-category data (health, biometrics, etc.) also needs an Art. 9 condition. Purpose limitation: don't reuse data for new, incompatible purposes without a fresh basis. If relying on legitimate interests, name the interest and keep a balancing test.

3 Where data comes from

If we did not collect personal data directly from you, we received it from [SOURCE] and the categories of data are [CATEGORIES]. We provide this information within the timeframe required by law.

Guidance

Keep this section if you import leads, enrich profiles, receive referrals, or obtain data from partners. Delete it only if every item is collected directly from the person.

4 Who we share it with

We share personal data with service providers who process it on our behalf under a data processing agreement, including [HOSTING], [PAYMENTS], [ANALYTICS], [EMAIL]. We do not sell your personal data. We may disclose data where legally required, or to protect our rights and users.

5 International transfers

Where we transfer personal data outside the [EEA/UK], we rely on an appropriate safeguard - typically the European Commission's **Standard Contractual Clauses** [and/or an adequacy decision], together with any additional measures needed to protect your data. You can request details of these safeguards using the contact above.

6 How long we keep it

We keep personal data only as long as needed for the purposes above, then delete or anonymise it. Our retention periods are: [e.g. account data - [X] months after closure; support tickets - [X] months; billing records - [X] years for tax/legal reasons]. See our Data Management Plan for detail.

7 Your rights

- Access a copy of your personal data
- Correct inaccurate or incomplete data
- Erase data, sometimes called the right to be forgotten, where applicable
- Restrict or object to certain processing, including direct marketing
- Data portability - receive your data in a portable format
- Withdraw consent at any time, without affecting prior processing

To exercise any right, contact [PRIVACY EMAIL]. We respond within one month. You also have the right to complain to your data protection supervisory authority - in [COUNTRY], the [SUPERVISORY AUTHORITY].

8 Automated decisions & required data

[We do / do not] use automated decision-making, including profiling, that produces legal or similarly significant effects. If we do, we explain the logic involved, the significance, and the expected consequences here: [EXPLAIN].

Where providing personal data is a statutory or contractual requirement, or needed to enter a contract, we explain whether you must provide it and what happens if you do not: [EXPLAIN].

9 Security & breach handling

We use appropriate technical and organisational measures - including [encryption in transit and at rest], [access controls], and [monitoring] - to protect your data.

Internal procedure (remove before publishing)

On becoming aware of a personal-data breach: contain it; assess the risk to individuals; notify your supervisory authority **within 72 hours** if the breach is likely to result in a risk to people's rights; notify affected individuals without undue delay if the risk is high; and record every breach in a breach log regardless of whether it's notified.

10 Changes to this notice

We may update this notice from time to time. We'll post the updated version here and, for significant changes, notify you directly. **Last updated: [DATE].**

Need a practical compliance review?

This template gets you started. If you'd like an engineer who does compliance to pressure-test your answers - or turn them into working controls, documentation, and audit-ready evidence - book a free 30-minute discovery call.

Book a free discovery call

or visit rdelune.dev

This template is provided by rdelune LLC for general informational purposes only and does not constitute legal, regulatory, or professional advice, nor create a consultant-client relationship. Regulatory obligations depend on your specific facts and jurisdiction. Validate your completed document against the applicable law (e.g. the EU GDPR, the ePrivacy Directive, and the EU AI Act) and, where appropriate, with a qualified professional. © 2026 rdelune LLC. You may use and adapt this template freely within your organisation; please retain this attribution.