ComplyJet

Privacy Policy Template

A free, adaptable template for a SaaS privacy policy: twelve clauses with filled sample wording, a retention table, a sub-processor table, a changes log, and a customization checklist. Shaped by GDPR Articles 12 to 14, the CCPA, and CalOPPA.

HOW TO USE THIS TEMPLATE

Replace every [bracketed value] with a fact about your own product. Delete any clause that does not describe your practices, keep the numbering, and have a lawyer read the final version before you publish it. The sample wording is a starting point: it only works if it matches what your product actually does, so fill it from a data inventory, not from memory.

Company: [Company legal name]

Product: [Product name]

Policy owner: [Role]

Privacy contact: [Privacy email address]

Version: [1.0]

Effective date: [Date]

Reviewed by counsel: [Name, date]

Next review: [Date, e.g. every six months]

Before you start: delete-before-publishing guide

- Remove this page, the italic notes under each heading, and every instruction in square brackets.
- Keep the clause numbers in your internal copy so the changes log can refer to them.
- Delete a clause only if it truly does not apply. A children's clause still needs a position even with no child users.
- Do not list sensitive categories (health, biometric, precise location) just because a generator did. If you do not collect them, say so.
- This template covers the external, customer-facing policy. Your internal information security policy is a separate document for your own staff.

Where the privacy policy sits among your documents

Document	Who reads it	What it covers
Privacy policy	Users, visitors, regulators, buyers	What personal data you collect, why, who gets it, how long you keep it, and user rights
Terms of service	Users and customers	Rules of using the product, payment, liability, termination
Cookie policy	Visitors	Which cookies and trackers run, and the choices people have

Data processing agreement	Customers' legal and security teams	How you process the personal data customers load into your product

The twelve clauses

Square brackets mark the facts only you can supply. Everything else is written to be used as it stands once it matches your practices.

1. Who we are and how to contact us

GDPR requires controller identity and contact details.

> [Company legal name] ("we", "us") runs [product name]. We are the controller of the personal data described in this policy. You can reach us at [privacy email address] or at [postal address]. [If you have appointed a data protection officer: Our data protection officer can be contacted at [address].]

2. Data we collect

Every law asks for categories of data. Sort what you collect into three buckets: given by users, collected automatically, received from others.

> We collect data you give us, such as your name, work email address, password and billing details, and the messages you send our support team. We collect some data automatically when you use the service, such as your IP address, browser and device type, and the pages and features you use. We may receive data from others, for example when you sign in through a single sign-on provider or when a colleague invites you to an account. We do not knowingly collect [health, biometric or precise location] data.

3. How we use data and why

GDPR requires a purpose and a legal basis for each. Treat the pairings as a starting position to test against your own processing.

> We use your data to provide the service and manage your account (to perform our contract with you), to bill you and keep records (contract and legal obligation), to secure the service and understand how it is used (our legitimate interests in keeping it safe and improving it), and to send product updates and marketing emails (your consent, or our legitimate interests where the law allows). You can withdraw consent at any time.

Purpose	Typical legal basis	What to say in plain words
Creating and running the account	Contract	We use your details to provide the service you signed up for
Billing and tax records	Contract and legal obligation	We keep records to charge you and meet accounting rules

Product analytics and security monitoring	Legitimate interests	We look at usage to fix bugs, prevent abuse and improve the product
Marketing emails	Consent, or legitimate interests where the local law allows it	We email you about updates, and you can opt out at any time
Advertising and retargeting tags	Consent	We run these only if you accept them

Where you rely on legitimate interests, say in one sentence what the interest is. Where you rely on consent, say the person can withdraw it.

4. Who we share data with

Recipients or categories of recipients must be named. Naming the vendors is better, and buyers often ask for it.

> We share data with service providers that help us run the service: [hosting, analytics, email delivery, payments, customer support, error monitoring]. They may use it only on our instructions. The current list is at [sub-processor page link]. We do not sell your personal data, and we [do / do not] share it for cross-context behavioral advertising. We may disclose data where the law requires it.

Sub-processor table

Either keep this list on a separate page that you update, or list vendors in the policy and treat each change as a policy update. The first is easier to keep current.

Vendor	Category	What it does for us	Where it processes data
[Vendor name]	Hosting	[Purpose]	[Countries]
[Vendor name]	Analytics	[Purpose]	[Countries]
[Vendor name]	Email delivery	[Purpose]	[Countries]
[Vendor name]	Payments	[Purpose]	[Countries]
[Vendor name]	Customer support tooling	[Purpose]	[Countries]
[Vendor name]	Error monitoring	[Purpose]	[Countries]

CHECK YOUR OWN PAGES
Open your signup page, go to the browser's Network tab, reload, and list every third-party request. Every domain on that list is either a recipient the policy must cover or a tag you did not know you were running.

5. International transfers

Required if data leaves the EU, with the safeguard stated. Name the transfer mechanism you actually rely on and check it periodically.

We are based in [country] and our providers may process data in [countries]. Where data leaves the European Economic Area or the United Kingdom, we rely on [an adequacy decision / standard contractual clauses] and additional safeguards where needed. You can ask us for a copy of the safeguards at [privacy email address].

6. How long we keep data

State a period where you have one, and the criteria where you do not. Do not leave it as "as long as necessary".

We keep account data while your account is active and delete it within [90 days] after you close it. We keep billing records for [7 years] to meet tax and accounting rules, and server logs for [12 months]. Where we cannot give a fixed period, we keep data only as long as needed for the purpose it was collected for, or as the law requires.

Retention table

The rows are adjustable defaults, not legal periods. Your own tax, contract and regulatory obligations decide what is right for you. The public statement should never promise more than your internal retention schedule delivers.

Data	Example retention statement	Adjust for
Account data	While the account is active, then deleted within [90 days] of closure	Your deletion process and backup cycle
Billing records	[7 years] after the transaction	Tax and accounting rules where you operate
Server and access logs	[12 months]	Your security monitoring needs
Marketing contacts	Until unsubscribe, or after [24 months] of no engagement	Local marketing and consent rules

7. Security

Describe what you actually do in terms a customer can check, such as encryption in transit and at rest, access controls, and independent audits if you hold them. Avoid "industry-leading security" and "your data is 100% safe": neither is verifiable.

We protect personal data with [encryption in transit and at rest, access controls, and independent audits if you hold them]. [Describe only the measures you can show evidence for.]

8. Your rights and how to use them

GDPR and CCPA both require the rights list and a way to use it. Give a channel, say how you confirm identity, and state a response time you can keep.

> Depending on where you live, you may have the right to access, correct, delete, restrict or object to our use of your data, to receive it in a portable format, and to opt out of its sale or sharing. To use these rights, email [privacy email address]. We will confirm your identity and respond within [30 days]. If you are in the EU or UK, you may also complain to your local data protection authority. We do not penalize you for using your rights.

GDPR Article 12(3) requires action without undue delay and within one month of receipt, extendable by two further months for complex or numerous requests, with notice to the person. A promise tighter than the law is fine only if you can keep it.

9. Cookies and tracking

CalOPPA asks for the do-not-track disclosure and whether third parties collect information across sites through your service. A separate cookie policy can carry the detailed cookie table.

> We use cookies and similar technologies for [essential functions, analytics and, with your consent, advertising]. Third parties such as [analytics provider] may collect data about your activity on our site through these technologies. [Our site does not respond to browser "do not track" signals / We respond to browser "do not track" signals by ...]. You can manage cookies through [cookie settings link] and your browser.

10. Children

Sets your position on minors' data.

> Our service is not directed to children under [16], and we do not knowingly collect their data.

11. Changes to this policy

CalOPPA asks how users learn of material changes. What you write here becomes a promise you have to keep.

> If we make material changes to this policy, we will tell you by [email or in-app notice] before they take effect and update the date below. Earlier versions are available at [link].

12. Effective date

The date proves which version applied when.

> Effective date: [date].

Customer data we process for others

For your own website visitors, trial users and account holders, you decide why and how data is used, so you are the **controller**. For data your customers load into your product, the customer decides the purpose and you act on their instructions, so you are usually the **processor**. That processing is governed by the customer data processing agreement, not your public privacy policy.

Data type	Your role	Document that covers it	Who answers a rights request
Website visitors and cookie data	Controller	Privacy policy and cookie policy	You
Trial sign-ups and account holders	Controller	Privacy policy	You
Billing contacts	Controller	Privacy policy	You
Data your customers upload or generate	Usually processor	Customer DPA and your terms	The customer, with your help
Data of your customer's end users	Usually processor	Customer DPA	The customer, with your help

OPTIONAL PARAGRAPH FOR THE POLICY

We process the data our customers submit to the service on their instructions. If you are one of our customers' users, contact the customer first, and we will assist them with your request.

Optional summary layer

A long policy is hard to read, and GDPR asks for concise, easily accessible information. Put a short summary at the top and the full text below it.

SAMPLE SUMMARY LAYER

The short version: we collect your account details and usage data to run [product name]. We share data only with the service providers that help us operate it. We do not sell your data. You can ask to see, correct or delete your data at any time at [privacy email address]. The full policy follows.

Link the policy where people make decisions, not only in the footer: the footer of every page, the signup form next to the button, in-app settings, app store listings where the store requires a policy link, and checkout where billing details are collected.

Changes log

Keep a short version log with each change, its date, and a one-line summary. Show the effective date at the top of the policy, announce material changes the way clause 11 says you will, and keep prior versions available.

Version	Date	One-line summary of the change	Clauses changed	Approved by
[1.0]	[Date]	[Initial publication]	[All]	[Name]

When the policy must change

Change	Why the policy must change
New analytics, advertising or tracking tool	It creates a new recipient and often new cookies
New sub-processor	The sharing clause and the sub-processor list change
New data category	The data clause and the legal basis table change
New product feature, including AI features	A new purpose, and possibly a new recipient
New market or user region	New laws, rights and transfer rules may apply
Change in retention	The retention clause must match what you now do
Security incident	Security statements and any notices may need revisiting

Review the policy on a fixed cadence even when nothing seems to have changed, for example every six months, and record the review. Some laws may set a minimum review frequency of their own, so ask your counsel whether one applies to you.

One-page customization checklist

Do these in order, because each step feeds the next.

Done	#	Step
☐	1	**Inventory the data and tools.** List what you collect, where it is stored, and which vendors touch it.
☐	2	**Map each item to a purpose and a legal basis.** If you cannot name a purpose, stop collecting it.
☐	3	**Fill the clauses** from the inventory, not from memory.
☐	4	**Delete what does not apply.** A children's clause still needs a position, but a section for a country with no users does not.
☐	5	**Get counsel review** of the finished draft.
☐	6	**Publish with an effective date** and keep the old version.
☐	7	**Link it** from the footer, the signup form and your app listings.
☐	8	**Brief the team**, so support, sales and engineering know what the policy promises.

Four checks before you publish

Done	Check
☐	Every tool on your network-request list appears in the sharing clause
☐	Every retention period matches what your systems do
☐	The rights email address is monitored
☐	The effective date is set

Mistakes to avoid

- Copying a competitor's policy. It describes their tools, regions and promises, not yours.
- Listing tools you no longer use, or omitting ones you do.
- Promising "we never share your data" while running ad pixels.
- Stale transfer language. Name the transfer mechanism you actually rely on and check it periodically.
- Leaving retention as "as long as necessary".
- Publishing with no effective date or version history.

Not legal advice. This template is a starting point and general information, not legal advice. Privacy statutes change, and which ones apply to you depends on your users and your data. Have counsel review your final policy before you publish it. Free from ComplyJet. Read the full guide at complyjet.com/blog/privacy-policy-template.