

Cookie Policy Template

A free, adaptable template for a SaaS cookie policy: ten clauses with filled sample wording, a cookie table with example rows to replace, a changes log, and a one-page audit and customization checklist. Shaped by the ePrivacy Directive Article 5(3), GDPR, the CCPA and UK PECR.

HOW TO USE THIS TEMPLATE

Run the audit on the last page first. Then replace every [bracketed value] with a fact about your own product, delete any clause that does not describe your practices, and have a lawyer read the final version before you publish. The sample wording only works if it matches what your pages actually load, so fill it from a scan of your marketing site and your logged-in app, 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 scan and 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. Keep the cookie table even if it is short.
- Do not publish the example cookie rows. Replace them with the cookies your own scan found, and take every duration from the provider's documentation.
- This template covers the external, customer-facing cookie notice. Your privacy policy and your internal information security policy are separate documents.

Where the cookie policy sits among your documents

Artefact	Its job	What a reviewer asks for
Cookie policy	Informs visitors what is set, why, by whom and for how long	The link, and the list of third-party scripts
Cookie banner	Collects the choice before non-essential scripts run	Proof that scripts do not load before consent, and that refusing is as easy as accepting
Consent record	Proves what each visitor chose, and when	A sample record with the policy version it applied to

The ten 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

Controller identity and a contact point.

[Company legal name] ("we", "us") runs [product name]. This policy explains how we use cookies and similar technologies on [website address] and in our product. You can reach us about this policy at [privacy email address].

2. What cookies and similar technologies are

Scope: local storage, pixels and SDK identifiers fall under the same rules.

Cookies are small text files that a website places on your device. We also use similar technologies, such as local storage, tracking pixels and software identifiers, that work in a comparable way. In this policy we call all of them "cookies."

3. Why we use cookies

Purposes must be specific enough for consent to be informed. Delete any purpose you do not have.

We use cookies to keep you signed in, to protect your account, to remember choices you make, to understand how our website and product are used so we can improve them, and, only if you agree, to measure and personalize our advertising.

4. Categories of cookies

Each category carries its own consent rule.

Category	What it does	Consent
Strictly necessary	Needed to deliver a service you asked for, such as signing in or keeping your account secure	Not required
Functional	Remembers choices you make, such as language or theme	[Depends on function and duration]
Analytics	Counts visits and feature use so we can improve the service	[Required in the EU unless a regulator's conditions are met; check the UK exception]

Marketing	Measures ads and builds audiences	Required in the EU and UK; opt-out in California
------------------	-----------------------------------	--

5. The cookie list

This is the clause reviewers read first. Replace every example row with a cookie your own scan found. Scan the marketing site and the logged-in product separately.

Cookie or tracker	Purpose	Set by	First or third party	Duration	Category
[Login session ID]	Keeps you signed in during a visit	[Us]	First	[Session]	Strictly necessary
[CSRF token]	Blocks forged requests to your account	[Us]	First	[Session]	Strictly necessary
[Interface preference]	Remembers the language or theme you chose	[Us]	First	[Duration]	Functional
[Product analytics ID]	Counts feature usage to improve the product	[Analytics provider]	Third	[Per provider documentation]	Analytics
[Support-chat visitor ID]	Recognizes a returning visitor in chat	[Chat provider]	Third	[Per provider documentation]	[Functional or analytics]
[Ad retargeting pixel]	Measures ads and builds audiences	[Ad platform]	Third	[Per provider documentation]	Marketing

DURATIONS

Take every duration from the provider's own documentation and re-check it at each scan. For example, Google documents the default expiry of its Google Analytics 4 cookie "_ga" as 2 years, and Intercom documents its session cookie at 1 week by default and its device identifier at 270 days. Lifetimes differ widely, so one blanket figure in the policy is almost always wrong.

6. First-party and third-party cookies

Users must be told whether third parties may access the cookies (CJEU, Planet49, C-673/17).

Some cookies are set by us. Others are set by providers that supply services to us, such as [analytics provider] and [support-chat provider]. Those providers may be able to read the cookies they set. The cookie list above names each provider and what its cookie does.

7. How long cookies last

Duration is part of the information users must receive.

Some cookies, called session cookies, expire when you close your browser. Others, called persistent cookies, stay on your device for a set period or until you delete them. The cookie list above shows how long each one lasts.

8. How to manage or withdraw consent

GDPR Article 7(3): withdrawing must be as easy as giving consent. Point to a control, not only an email address.

When you first visit, we ask for your choice before we set any cookie that is not strictly necessary. You can change or withdraw your choice at any time by selecting "Cookie settings" in the footer of any page. Withdrawing consent does not affect cookies already set for strictly necessary purposes. Most browsers also let you block or delete cookies, though some parts of our service may stop working if you block strictly necessary ones. [If you honor opt-out preference signals such as Global Privacy Control: We treat a Global Privacy Control signal from your browser as a request to opt out of the sale and sharing of your personal information.] [If you sell or share personal information in California: You can also use the "Do Not Sell or Share My Personal Information" link in our footer.]

9. Your rights

Link to the privacy policy for the full list of rights and the right to complain.

Depending on where you live, you may have rights over the personal data we collect through cookies, including the right to access it, correct it, delete it, object to certain uses and complain to your data protection authority. Our privacy policy at [privacy policy URL] explains these rights and how to use them.

10. Changes to this policy

Show the effective date, keep prior versions, and tie each consent record to the version the visitor saw.

We update this policy when we change the cookies we use, and we show the date of the latest version at the top. This version took effect on [date]. If a change requires new consent, we ask you again.

Changes log

Version	Date	Changed by	What changed and why
[1.0]	[Date]	[Role]	[Initial publication, based on scan of date]

One-page audit and customization checklist

Work down this list in order. The audit comes before the wording.

Done	#	Step
☐	1	Scan the marketing site and the logged-in app separately. Use a clean browser profile, load each surface before touching any consent control, then again after accepting everything, and record every cookie, local storage key and third-party request.
☐	2	Sort each item into a category and a consent rule. Ask what it does, who benefits, and whether the user asked for it.
☐	3	Fill the cookie list with the real names, providers, purposes and durations from provider documentation.
☐	4	Match the banner to the policy. Non-essential scripts load only after consent in the EU and UK, refusing is as easy as accepting, and nothing is pre-ticked.
☐	5	Add a persistent "Cookie settings" control so withdrawal stays as easy as giving consent.
☐	6	Store consent records with a timestamp and the policy version each choice applied to.
☐	7	Get counsel review of the finished policy and of the region sections you rely on.
☐	8	Publish with an effective date and link it from the footer, the banner, in-app settings and the signup form.
☐	9	Set the next scan and re-scan on every new script, tag-manager change, vendor swap and release that touches client-side code.

Four checks before you publish

Done	Check
☐	Every third-party domain on your network-request list appears in the cookie list
☐	No example or bracketed row is left in the published table
☐	Nothing non-essential sets a cookie before consent in the EU and UK
☐	The effective date and version are set

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