

Cookie Policy

APP & SAAS TEMPLATE

Last updated: [EFFECTIVE DATE]

This Cookie Policy explains how [COMPANY NAME] uses cookies, software development kits, and similar technologies in [APP NAME] and the connected online service. It also sets out the controls you have over them.

Mobile apps do not use browser cookies the way a website does. They rely on stored files, device identifiers, and code supplied by other companies. This policy covers all of these and refers to them together as tracking technologies.

This version applies from [EFFECTIVE DATE] and covers [APP NAME] on every platform where we publish it, plus the account pages you reach from inside the app. Read it with our privacy policy.

Contents

1. Technologies We Use.....	2
2. Examples In Our App.....	2
3. Analytics And Crash Reporting.....	2
4. Advertising Identifiers.....	3
5. Tracking Permission Controls.....	3
6. In-App Consent Prompt.....	3
7. Device Level Controls.....	3
8. Web Views And Links.....	3
9. Changes And Contact.....	4

How to use this template

1. Replace every [PLACEHOLDER] with your own details. Use Find and Replace in Word to catch them all.
2. Delete any section that does not apply to your business, and renumber the headings that follow.
3. Have the finished document reviewed by a qualified lawyer in [COUNTRY/STATE] before you publish it.

1. Technologies We Use

Several kinds of technology run inside [APP NAME], and each does a different job. Some are needed for the app to function. Others run only if you allow them.

- Software development kits, or SDKs, are blocks of code from other companies that we build into the app for analytics, crash reporting, payments, or advertising.
- Local storage on the device holds settings, cached content, and a session token so you stay signed in between launches.
- Device and advertising identifiers, such as the Apple Identifier for Advertisers and the Google Advertising ID, are resettable codes that let partners recognise a device without using your name.
- Pixels and tags load in the in-app browser and on our web pages to measure whether a campaign led to an install or a purchase.
- Push tokens issued by Apple and Google let us deliver notifications to the correct device.

2. Examples In Our App

The table below lists representative technologies in [APP NAME]. The exact set changes as we add or remove features, so the privacy screen in the app settings is the accurate source for what is active on your device.

Technology	Provider	Purpose	Duration
Session token	[COMPANY NAME]	Keeps you signed in between launches	Until you sign out
Local settings store	[COMPANY NAME]	Saves preferences such as theme and language	Until app removal
Analytics SDK	Analytics provider	Measures feature use and performance	13 months
Crash reporting SDK	Crash reporting provider	Records diagnostics after a failure	90 days
Advertising identifier	Apple or Google	Attributes installs and limits repeat adverts	Until you reset it
Push token	Apple or Google	Delivers notifications to your device	Until notifications off

3. Analytics And Crash Reporting

Analytics shows us which screens people open, which features go unused, and where a flow is abandoned. We use it to decide what to build and fix in [APP NAME], not to identify you personally.

Crash reporting captures the state of the app when it fails. A report can include the device model, operating system version, the screen you were on, and a stack trace. It may carry a device identifier so repeated failures on one device can be grouped.

Where these tools are not required to run the app, we ask for consent before enabling them, and you can switch them off later in the app settings.

4. Advertising Identifiers

Advertising identifiers are codes held by the operating system rather than by us. Apple calls its version the Identifier for Advertisers, or IDFA. Google calls its version the Google Advertising ID, or AAID.

Advertising partners use these codes to tell whether an advert led to an install, to avoid showing the same advert repeatedly, and to build interest based audiences. We pass an identifier to a partner only where you have allowed tracking.

An advertising identifier does not contain your name or email address. It can still be matched to a profile held by an advertising partner, which is why the controls described below matter.

5. Tracking Permission Controls

On Apple devices, App Tracking Transparency requires us to ask before we track you across apps and websites owned by other companies. If you select Ask App Not to Track, we do not request the IDFA and our partners cannot use it for that purpose.

On Android, the Google advertising settings let you delete the advertising ID or opt out of personalised adverts. Once the identifier is deleted, apps receive a string of zeros in its place.

You can change either setting whenever you want. Turning tracking off does not limit your use of [APP NAME] and does not remove adverts. It makes them less specific to you.

6. In-App Consent Prompt

The first time you open [APP NAME] we show a consent screen covering analytics, crash reporting, and advertising technologies. Technologies needed to run the app, such as the session token and security checks, are described there but are not optional.

Your choices are stored on the device and linked to your account so they carry across sessions. You can reopen the screen at any time from the privacy section of the app settings.

Withdrawing consent stops further collection through the relevant SDK from that point onward. It does not delete data already sent. Write to [CONTACT EMAIL] to ask about data we already hold.

7. Device Level Controls

Both platforms offer controls that sit above anything inside [APP NAME]. You can reset the advertising identifier, which breaks the link to any profile built against the previous value, or switch off personalised advertising entirely.

You can also clear the app cache and stored data from the operating system settings, or delete the app. Removing the app clears its local storage, including saved preferences and the session token.

These controls apply to one device at a time. Repeat them on every device where you use [APP NAME].

8. Web Views And Links

Parts of [APP NAME] open web pages inside the app, for example help articles, billing pages, and checkout. These in-app browsers can set ordinary browser cookies, including analytics and payment cookies.

Cookies set in an in-app browser are governed by the cookie settings for that page rather than by the app consent prompt. Where the page is ours, the same consent tool appears. Where the page belongs to another company, their notice applies.

Links that open your normal browser take you out of [APP NAME] completely, and we have no control over what the destination site stores. Guidance on all of this is available at [SUPPORT URL].

9. Changes And Contact

We update this policy when we add or remove an SDK, change a provider, or change what is collected. The current version sits in the app settings and at [SUPPORT URL], and the date at the top shows when it last changed.

Where a change means we need fresh consent, the consent screen appears again the next time you open the app.

For questions about this policy, write to [COMPANY NAME] at [CONTACT EMAIL] or [POSTAL ADDRESS].

Before you publish

This template is a starting point only. Replace every placeholder in square brackets with your own details, confirm the technology table against the SDKs actually shipped in your build, and have a qualified lawyer in [COUNTRY/STATE] review the final document before you publish it.



Free template provided by PrivacyTerms.io. Drafting legal documents since 2013.

[Need a version written around your business? Build a tailored document in minutes at privacyterms.io](https://privacyterms.io)