



AppXite Platform Cookie Policy

Last Updated: 16.02.2024

1. Introduction

This Cookie Policy explains how AppXite ("we", "us", or "our") uses cookies and similar technologies on the AppXite Platform (the "Platform"). This policy is designed to provide you with clear and comprehensive information about the cookies we use, the purposes for which we use them, and your choices regarding their use, in compliance with the General Data Protection Regulation (GDPR) and the ePrivacy Directive.

The AppXite Platform is provided on a white-label basis to our partners ("Partners"). This means that our Partners may customize the Platform and may integrate their own services and cookie solutions. This policy primarily covers the cookies that are set by the core AppXite Platform. Our Partners are responsible for their own cookie practices and for providing their own cookie policies to end-users.

2. What are Cookies?

Cookies are small text files that are placed on your device (computer, smartphone, or tablet) when you visit a website. They are widely used to make websites work, or work more efficiently, as well as to provide information to the owners of the site.

Cookies can be classified by their duration, provenance, and purpose:

- Session cookies: These are temporary and expire once you close your browser.
- Persistent cookies: These remain on your device for a set period or until you delete them.
- First-party cookies: These are set by the website you are visiting.
- Third-party cookies: These are set by a domain other than the one you are visiting, such as by our service providers for analytics or advertising.

3. How We Use Cookies

We use cookies for several purposes on the AppXite Platform. These cookies are essential for you to browse the Platform and use its features, such as accessing secure areas. The Platform cannot function properly without these cookies.

Cookie Name	Provider	Duration	Purpose
AppContext	AppXite	24h	Used to enable core web application functionality.
Ai_session	Microsoft	Session	Application Insights to collect page telemetry and usage



			information (i.e. availability & performance).
Ai_User	Microsoft	Session	Application Insights to collect page telemetry and usage information (i.e. number of users accessing the application over time).
a0.spajs.txs.	Auth0	Immediately expired upon logging in.	Auth0 security token mechanism. Used to validate user redirection requests.
__stripe_mid	Stripe	1 year	Necessary for making credit card transactions on the website.
__stripe_sid	Stripe	Session	Necessary for making credit card transactions on the website.
ai_session	Microsoft	Session	Preserves user states across page requests.
auth0.is.authenticated	Auth0	Session	Keeps the user logged in by indicating an authenticated state.
AuthToken	AppXite	Session	Stores the authentication token required to access secure parts of the user session
cf_clearance	Cloudflare	1 year	Helps improve website performance and provides security against malicious traffic.