Cookie Policy

Version 0.1 · November 5, 2026
https://recurrentaero.com/legal/en/WORLD/cookies

Pre-launch version
Pre-launch version 0.1. These terms take effect for a training centre on the date it signs or accepts them, and for all other users on the date the service opens. No payments are taken under this version yet.

This policy describes the cookies and similar technologies the Recurrent web applications (Book and Manager) use. Data controller: Nivorbit Teknoloji Limited Şirketi. Questions: contact@nivorbit.com.

1. In short

The Platform uses **strictly necessary** cookies only: to keep you signed in, to remember your language and organization, and to take card payments safely. **We use no advertising, analytics or tracking cookies** and share no data with advertising networks. Strictly necessary cookies are needed for the service to work and so do not depend on your consent (the Turkish Data Protection Authority's Guide on Cookies; ePrivacy Directive Art. 5(3)).

2. The cookies we use

Session and security (first party)

- **pz_book_session, pz_manager_session**: your signed-in session; encrypted and readable only by the server (HttpOnly, Secure). Lifetime: the session's maximum lifetime (10 hours by default) or until you sign out.
- **pz_book_idt, pz_manager_idt**: the identity token sent to the sign-in server when you sign out; encrypted. Lifetime: as the session.
- **pz_book_tx, pz_manager_tx**: a one-time value that secures the redirect while you sign in. Lifetime: 10 minutes.

Preferences (first party)

- **NEXT_LOCALE**: the language you chose. Lifetime: the browser session.
- **pz_book_org, pz_manager_org**: the organization you last chose, if you work in several. Lifetime: 1 year.
- **pz_consent**: your cookie choice from the banner or "Cookie settings", so we do not ask again. Lifetime: 1 year.

Sign-in server

You sign in on our identity server (Keycloak). It uses strictly necessary cookies on its own domain to manage the sign-in session (for example **AUTH_SESSION_ID**, **KEYCLOAK_IDENTITY**, **KEYCLOAK_SESSION**, **KC_RESTART**). Lifetime: the sign-in session.

Payment (third party: Stripe)

Only on the payment page, while you enter card details into Stripe's secure field, Stripe sets cookies to prevent fraud (for example __**stripe_mid**, 1 year, and __**stripe_sid**, 30 minutes). See Stripe's cookie policy for details.

3. Local storage

The session-day check-in desk in Manager keeps which device the desk is for in the browser's local storage (**pilotzo.checkIn.device**). It holds no personal data and stays in that browser.

4. The mobile app

The mobile app uses no cookies. Its sign-in keys are kept in the device's secure store (iOS Keychain, Android Keystore); for notifications, the device's push token is registered with our server and removed when you sign out.

5. Managing cookies

You can delete or block cookies in your browser's settings. If you block the strictly necessary ones, you cannot sign in or pay. If we ever add a cookie that is not strictly necessary, we will ask for your consent before using it.