COOKIE AND SDK NOTICE

Controller	NestKerCom Korlátolt Felelősségű Társaság
Contact	info@nestker.com
Purpose of document	Presentation of the cookies, mobile SDKs, local-storage solutions and technical identifiers used on Fighter's website and in its mobile applications.
Version	v1.0
Date	27 August 2026
Effective	7 September 2026 until withdrawn

1. Purpose of this Notice

This Cookie and SDK Notice describes the cookies, mobile SDKs, local-storage solutions, device identifiers and other technical or tracking technologies that may be used by the Fighter Application and its related web interfaces.

Fighter operates primarily as a mobile application; accordingly, this Notice covers not only browser cookies but also mobile SDKs, in-app local storage, push tokens, integrity-protection tokens and payment/map technologies.

2. Definitions

- Cookie: a small data file placed in the browser, or an equivalent web technology.
- Web cookies may be session (temporary) cookies or persistent cookies. Session cookies expire when the browser is closed, while persistent cookies may remain on the device until the end of the specified retention period.
- Mobile SDK: a software development kit integrated into the application to provide an external service, such as login, crash reporting, maps or payments.
- Local storage: technical data, settings or temporary cache stored on the device or within the application.
- Device identifier: an identifier associated with the operation of the application, device or service, such as a push token, application-instance identifier or integrity-protection token.
- Non-essential technology: an analytics, marketing or similar tracking solution that is not indispensable for operation of the requested service.

3. Technology Categories

3.1. Technologies Necessary for Operation

These technologies provide the core operation of the application, including login, account management, secure data connections, payment redirects, content uploads and essential service notifications. Without them, Fighter services would either not be available or would not be available securely.

3.2. Security and Fraud-Prevention Technologies

These include, in particular, App Check, Apple App Attest / DeviceCheck, Google Play Integrity, logging, rate limiting, authorisation checks and other technical safeguards. Their purpose is to prevent attacks on the backend from counterfeit applications, automated tools or by unauthorised means.

3.3. Performance and Error-Reporting Technologies

The Service Provider may use crash-reporting and stability tools to identify, investigate and remedy application crashes, slowdowns and operational errors.

3.4. Analytics and Marketing Technologies

Non-essential tracking technologies used for analytics or marketing purposes may be applied only where there is an appropriate legal basis, in particular prior consent. Consent may be withdrawn at any time.

Cookies used on web interfaces may originate from the Service Provider (first-party cookies) or from third-party service providers. In the case of third-party technologies, the relevant service provider's own privacy terms also apply.

4. Consent and Management of Settings

Technologies necessary for operation are connected to the provision of the service or the secure operation of the application; disabling them may therefore impair the application's essential operation. For non-essential analytics or marketing technologies, the Service Provider requests consent in accordance with applicable law.

The User may manage the relevant preferences in the device operating-system settings, in the application's privacy or notification settings, or through the cookie-settings interface available on the website. Browser cookies may also be deleted or restricted in the browser settings.

5. Retention Period

- Session-type cookies and identifiers are automatically deleted or expire at the end of the session.
- Technical data necessary for operation and security may be processed for as long as required to achieve the relevant purpose.

- Data collected by analytics or other non-essential technologies may be retained until consent is withdrawn or for no more than 13 months, unless the detailed notice applicable to the technology, applicable law or a legitimate security interest justifies a shorter or different retention period.
- In the event of a legal dispute, security incident or statutory obligation, certain technical logs may be retained for a further period that is necessary and proportionate.

6. Notices of Third-Party Service Providers

Third-party technologies used by Fighter are subject to the providers' own privacy terms. The most important related notices are:

- Google / Firebase: https://firebase.google.com/support/privacy
- Google Cloud: https://cloud.google.com/terms/data-processing-addendum
- Stripe: https://stripe.com/privacy and https://stripe.com/legal/dpa
- Apple: https://www.apple.com/legal/privacy/
- Google Play / Google: https://policies.google.com/privacy

7. Amendment of this Notice

The Service Provider is entitled to amend this Cookie and SDK Notice, in particular in the event of a new feature, a new SDK, a new processor, a new analytics or marketing technology, or a change in applicable law. The Service Provider will provide information about material changes within the application or on the website.