

PRIVACY NOTICE

Fighter Application

Effective from 7 September 2026 until withdrawn

Version: v1.0 | Date: 27 August 2026

1. Details of the Controller

The controller is NestKerCom Korlátolt Felelősségű Társaság (registered office: 6300 Kalocsa, Majoranna utca 3.; company registration number: 03-09-133275; tax number: 27279171-1-03; represented by: Kerpács Rezső, Managing Director; e-mail: info@nestker.com; hereinafter: the “Service Provider” or the “Controller”), which operates the Fighter mobile application (hereinafter: the “Application” or the “Platform”).

Enquiries relating to data processing may be submitted using the following contact details:

- E-mail: info@nestker.com
- Postal address: 6300 Kalocsa, Majoranna utca 3.
- The Controller informs data subjects that it is not required to designate a data protection officer pursuant to Article 37 GDPR, as its core activities do not include processing operations which, by virtue of their nature, scope and/or purposes, require regular and systematic monitoring of data subjects on a large scale, nor do they involve large-scale processing of special categories of personal data. Enquiries relating to data processing may be submitted using the contact details specified in Section 1 of this Notice.
- The Controller is established within the territory of the European Union and is therefore not required to designate a representative under Article 27 GDPR.

2. Material and Personal Scope of this Notice

This Privacy Notice applies to the processing of personal data of all data subjects using the Application, including both natural persons acting as consumers (hereinafter: “Users”) and natural or legal persons, or organisations without legal personality, advertising and selling products or services on the Platform (hereinafter: “Advertisers”).

This Notice sets out detailed rules concerning the legal basis, purposes and duration of processing and the rights of data subjects, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter: the “GDPR”), Act CXII of 2011 on Informational Self-Determination and Freedom of Information (the “Hungarian Privacy Act”), Act V of 2013 on the Civil Code (the “Hungarian Civil Code”), in particular its provisions on the protection of personality rights and contractual legal relationships, Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services (the “E-Commerce Act”), and Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities (the “Advertising Act”).

3. Categories of Data Subjects

3.1. Users

A User is exclusively a natural person who has reached the age of 16 and uses the Application outside his or her trade, independent occupation or business activity, i.e. acts as a consumer.

A Minor User is a User who has reached the age of 16 but has not yet reached the age of 18. A Minor User may independently consent to processing activities based on consent; however, the purchasing functions of the Marketplace and Advertiser registration may be used only after reaching the age of 18. Persons under the age of 16 may not register for or use the Application.

3.2. Advertisers

An Advertiser is a natural person acting in the course of his or her trade, independent occupation or business activity, a legal person, or an organisation without legal personality, who/which advertises and sells a product or service on the Platform and who/which accepted the Advertiser Terms during Advertiser registration. An Advertiser is not considered a User within the meaning of the General Terms and Conditions (hereinafter: the "GTC").

4. Categories of Personal Data Processed and Detailed Rules of Processing

4.1. Processing Relating to Users

4.1.1. Processing of Registration Data

Data processed: Registration is required for full use of the Application. During registration, the User must provide true and accurate data, set a valid e-mail address and password, declare that he or she has reached the age of 16, and, in the case of a Minor User, provide the e-mail address of a legal representative, and accept the GTC and the Privacy Notice.

Purpose of processing: Creation of a User account, enabling personal-access use of the Application, and identification and maintenance of the account.

Legal basis: The legal basis for processing data necessary for the creation and maintenance of the User account (e-mail address, password, age declaration) is performance of the contract with the User (Article 6(1)(b) GDPR). With regard to the e-mail address of the legal representative of a Minor User, the legal basis is compliance with a legal obligation applicable to the Service Provider (Article 6(1)(c) GDPR), taking into account the provisions of the Hungarian Civil Code concerning the protection of minors and the requirements of the Hungarian Privacy Act.

Retention period: For the duration of the account; where deletion is requested, the Service Provider completes deletion of the account within no more than 30 days from submission of the request.

4.1.2. Community Functions and User Content

Data processed: The Application enables Users to register for and organise sporting events, search for training partners, teams and groups, share sporting results, achievements and experiences, publish community content (posts, images, videos and comments), search for and review locations and facilities, and view messages, advertisements and notices within the community. Data recorded and shared through the use of these functions may constitute personal data.

Purpose of processing: Provision of the sports-community functions and display of content on the Platform.

Legal basis: Processing necessary to provide the community functions, including displaying content published by the User on the Platform, is based on performance of the contract with the User (Article 6(1)(b) GDPR).

The User must ensure that content published by him or her on the Platform, including in particular images, videos and other content making third-party natural persons identifiable, contains personal data of those third parties only where an appropriate legal basis is available, in particular their consent. Content containing personal data of a third-party minor may be published only with the prior consent of the minor's legal representative. The User acknowledges that the User is solely responsible for the lawful processing of personal data of third parties appearing in content published by the User, including ensuring an appropriate legal basis; the Service Provider is not the controller in this respect. The Service Provider is entitled, upon notification by the affected third party or upon otherwise becoming aware of the matter, to remove unlawful content without delay.

Retention period: Personal data processed within the community functions are retained for the duration of the User's account and, following deletion of the content by the User or withdrawal of consent, are deleted without undue delay but no later than within 30 days. Data necessary for performance of the contract are retained for the duration of the account.

4.1.3. Processing of Marketplace Purchaser Data

Data processed: In connection with transactions concluded on the Marketplace, the User's identification data, payment data and order details.

Purpose of processing: Through the Marketplace, Users may browse sports equipment, sports-related products and services and purchase them from Advertisers. The purpose of processing is to facilitate the technical execution of transactions.

Legal basis: A transaction concluded on the Marketplace is entered into between the User and the Advertiser; the Service Provider is not a contracting party to the transaction and merely provides the technical operation of the Platform. Processing of the User's identification, payment and order data in connection with the technical operation of the Marketplace and facilitation of the technical execution of the transaction (hereinafter: the "Transaction") takes place for the performance of the contract between the Service Provider and the User (Article 6(1)(b) GDPR).

Retention period: The Service Provider retains Marketplace purchaser data for the duration of the User's account and, following completion of the Transaction, for the retention period prescribed by law. Accounting documents are retained by the Service Provider, as a general rule, for 8 years in accordance with applicable legislation.

The Service Provider informs data subjects that, in relation to transactions concluded on the Marketplace, the Service Provider and the Advertiser are not joint controllers within the meaning of Article 26 GDPR. The Service Provider acts solely as the technical operator of the Platform; with respect to processing relating to products and services sold by it, the Advertiser acts as an independent controller and processes personal data in accordance with its own privacy notice.

4.1.4. Special Processing Rules Applicable to Minor Users

Persons who have reached the age of 16 but have not yet reached the age of 18 may independently consent to processing activities based on consent. Registration of a Minor User becomes complete only if the legal representative (parent or guardian) specified during registration confirms the registration through the validation e-mail sent by the Service Provider to the legal representative's e-mail address.

Until the validation e-mail has been confirmed, the Minor User may not use the functions of the Application.

Users aged 16 to 18 may upload video and image content; by uploading, they warrant that they have the consent of the persons appearing in the video or image and, in the case of a minor, the consent of that minor's legal representative. The Service Provider does not subject uploaded image or video content to facial-recognition or other biometric-identification procedures and does not process special categories of data under Article 9 GDPR on the Platform. The User is responsible for ensuring that content uploaded by the User does not contain special-category personal data whose publication has not been consented to by the data subject.

The legal representative may withdraw at any time any consent given on behalf of the Minor User and may exercise all data-subject rights under the GDPR on behalf of the minor concerned. Where consent is withdrawn, the Service Provider processes the Minor User's account and associated data in accordance with this Privacy Notice.

With regard to age verification, the Service Provider endeavours to apply proportionate technical and procedural measures to identify and protect minors, including continuous review of available technological solutions and their development where necessary; however, the Service Provider cannot be required to conduct comprehensive technical verification of age. The Service Provider develops and maintains its measures for the protection of minors in accordance with Regulation (EU) 2022/2065 (Digital Services Act, DSA).

4.2. Processing Relating to Advertisers

4.2.1. Processing of Advertiser Registration Data

Data processed: During registration, the Advertiser must provide true, accurate and complete data, including, for individual Advertisers, full name and contact details and, where an economic activity is carried out, tax number; and, for legal persons, company name, registered office, company registration number and tax number. At least one valid contact e-mail address and telephone number must also be provided, and the Advertiser Terms and the Privacy Notice must be accepted.

Purpose of processing: Creation and maintenance of the Advertiser account, enabling commencement and continuation of Advertiser activity, and administration of the contractual legal relationship with the Advertiser.

Legal basis: Performance of a contract (Article 6(1)(b) GDPR).

Only natural persons who have reached the age of 18, legal persons and organisations without legal personality may register as Advertisers. If the Service Provider becomes aware that an Advertiser Account was created by a person under 18, it will delete the account without delay.

Retention period: For the duration of the legal relationship with the Advertiser and, following termination of the legal relationship, for the retention period prescribed by law.

4.2.2. Processing of Transaction and Billing Data

Data processed: Data relating to Transactions conducted on the Marketplace, data serving as the basis for commission calculation and settlement, and billing data.

Purpose of processing: The Service Provider charges the Advertiser a commission for each Transaction concluded and completed through the Marketplace. The purpose of processing is to calculate, invoice and record the commission.

Legal basis: Compliance with a legal obligation (Article 6(1)(c) GDPR).

Retention period: The Service Provider retains data relating to Transactions for the retention period prescribed by law, including billing and settlement data. Accounting documents are retained by the Controller, as a general rule, for 8 years in accordance with applicable legislation.

4.2.3. Processing for Verification and Authentication Purposes

Data processed: Identification data provided by the Advertiser.

Purpose of processing: The Service Provider is entitled, but not obliged, to verify the data provided by the Advertiser and to reject the registration if, in its assessment, it does not comply with the requirements of the Advertiser Terms.

Legal basis: Legitimate interest (Article 6(1)(f) GDPR), based on the interest in the secure and lawful operation of the Application.

Retention period: The Service Provider retains data processed for verification and authentication purposes for the duration of the legal relationship with the Advertiser and, following termination of that relationship, for as long as the legitimate interest exists, but in any event for no longer than 5 years after termination of the legal relationship.

5. Common Processing Purposes and Legal Bases

5.1. Content Moderation

When moderating content published on the Application, the Service Provider acts in accordance with Regulation (EU) 2022/2065 (DSA). Content moderation extends to content published by Users and Advertisers and includes removal or disabling of access to illegal content and handling of content that violates the GTC or applicable law. The Service Provider takes content-moderation decisions in a transparent, non-discriminatory and proportionate manner and informs the affected content provider of the decision, the reasons for it and the available remedies.

Data processed: During the content-moderation procedure, the Service Provider processes the identifier of the contested content, identification data of the User or Advertiser who published the content, the content of the notice, the reasoning for the moderation decision, and the date of the decision.

Legal basis: Compliance with a legal obligation (Article 6(1)(c) GDPR).

Retention period: The Service Provider retains content-moderation decisions and the reasons for them for at least 6 months from the date of the decision, in accordance with the DSA. Retention for legal-enforcement purposes is governed by Section 5.4.

5.2. Contact and Notifications

Data processed: E-mail address and telephone number.

Purpose of processing: Communicating information, notifications and amendments necessary for Users and Advertisers. The Service Provider informs Users of material amendments by in-app notification or e-mail at least 30 days before they enter into force. In the case of Advertisers, the Service Provider informs the Advertiser of amendments by e-mail at least 15 days before they enter into force.

Legal basis: Performance of a contract (Article 6(1)(b) GDPR).

Retention period: Personal data processed for contact purposes are processed for the duration of the User's or Advertiser's account and, after termination of the legal relationship, for the retention period prescribed by law.

5.3. Push Notifications and Marketing Communications

Data processed: Device identifier (push token), e-mail address, and notification preferences provided by the User or Advertiser.

Purpose of processing: Sending in-app push notifications to Users and Advertisers regarding the Platform's services, new features, offers and promotions, and sending electronic communications for direct-marketing purposes.

Legal basis: Push notifications and electronic communications for direct-marketing purposes are sent only on the basis of the data subject's prior, freely given, specific and informed consent (Article 6(1)(a) GDPR). The data subject may withdraw consent at any time, without restriction and without giving reasons, in the Application settings or via the unsubscribe link contained in the communication. Withdrawal of consent does not affect the lawfulness of processing carried out before withdrawal. The legal basis for sending non-marketing notifications directly related to the provision of the Service (e.g. transaction notifications, security alerts) is performance of the contract (Article 6(1)(b) GDPR).

Retention period: The Service Provider processes personal data relating to marketing processing until consent is withdrawn or until the User's or Advertiser's account is terminated.

5.4. Enforcement of Legal Claims and Management of Legal Disputes

Data processed: All relevant data relating to the legal relationship with the data subjects.

Purpose of processing: Establishment, exercise, defence and adjudication of legal claims.

Legal basis: Legitimate interest (Article 6(1)(f) GDPR).

Retention period: The Service Provider retains personal data processed for the purposes of legal enforcement and dispute management until the expiry of the general limitation period calculated from termination of the relevant legal relationship – as a general rule, 5 years pursuant to Section 6:22(1) of the Hungarian Civil Code – unless a longer retention period is prescribed by law.

5.5. Automated Decision-Making and Profiling

The Service Provider does not use automated decision-making within the meaning of Article 22 GDPR, including profiling, in the operation of the Application. If automated decision-making is introduced in the future, the Service Provider will inform data subjects in advance by amending this Privacy Notice.

5.6. Legitimate Interest Assessment

Where processing is based on legitimate interests (Article 6(1)(f) GDPR), the Service Provider carries out and documents a legitimate interest assessment. The data subject may request information on the outcome of that assessment using the Controller's contact details specified in Section 1.

5.7. Data Protection Impact Assessment

The Controller carries out a data protection impact assessment pursuant to Article 35 GDPR where processing is likely to result in a high risk to the rights and freedoms of data subjects and, where necessary, conducts prior consultation with the supervisory authority (Article 36 GDPR).

5.8. Records of Processing Activities

The Controller maintains records of its processing activities pursuant to Article 30 GDPR and makes such records available to the supervisory authority upon request.

6. Data Transfers and Processors

The Controller has entered into data-processing agreements pursuant to Article 28 GDPR with the processors it uses. Such agreements specify the subject matter, duration, nature and purpose of processing, the types of personal data, categories of data subjects, and the obligations and rights of the Controller and the processor. Processors may process personal data only on the documented instructions of the Controller.

6.1. Payment Service Provider

The Service Provider provides a technical payment interface within the Application for payment of the purchase price; however, it is not a payment service provider, and responsibility for executing the payment transaction rests solely with the payment service provider used. For the purpose of executing payment transactions, the Service Provider uses a third-party payment service provider (name: Stripe Payments Europe, Ltd.; registered office: One Wilton Park, Wilton Place Dublin 2, D02 FX04, Ireland; hereinafter: the "Payment Service Provider") and transfers the relevant data to the Payment Service Provider to the extent necessary. The Payment Service Provider processes personal data provided during payment transactions as a processor in accordance with its privacy notice available at <https://stripe.com/en-hu/privacy>.

6.2. Processors

In operating the Application, the Service Provider uses, in particular, the following administrative, IT, payment, hosting, notification, analytics and platform service providers as processors, depending on the nature of the relevant service:

- Google Ireland Limited (registered office: Google Building Gordon House, Barrow St, Dublin, D04 E5W5, Ireland) – Firebase and Google Cloud services, including in particular authentication, database services, file storage, cloud functions, hosting, push notifications, App Check, Crashlytics, Analytics, Secret Manager, Google Maps Platform, and e-mail sending infrastructure;
- Stripe Payments Europe, Ltd. (registered office: One Wilton Park, Wilton Place Dublin 2, D02 FX04, Ireland);
- IRATKUPAC Bt. (registered office: 6300 Kalocsa, Obermayer tér 7. II. em. 1. ajtó) – accounting services.

6.3. Categories of Recipients of Personal Data

In accordance with Article 13(1)(d) GDPR, the Service Provider informs data subjects that the recipients or categories of recipients of their personal data may include: (i) cloud / hosting service providers; (ii) database and backend service providers; (iii) authentication service providers; (iv) the Payment Service Provider; (v) e-mail delivery service providers; (vi) push-notification service providers; (vii) analytics and crash-reporting service providers; (viii) app-store / platform service providers; (ix) mapping service providers; (x) accounting and tax-advisory service providers; (xi) legal advisers; (xii) IT support service providers; (xiii) authorities acting upon request on the basis of a statutory obligation; and (xiv) courts in the event of a legal dispute. The Service Provider transfers personal data to the above recipients only for the purposes and on the legal bases specified in this Notice and only to the extent necessary.

6.4. Authorities

For the purpose of complying with a statutory obligation, or in response to a request from an authority, the Service Provider may transfer data to competent authorities to the extent necessary. In the event of a serious infringement, the Service Provider may also notify the authorities.

6.5. DSA Point of Contact

Pursuant to Articles 11 and 12 of Regulation (EU) 2022/2065, the Service Provider designates the following point of contact for direct electronic communication with Member State authorities, the European Commission, the European Board for Digital Services and recipients of the service: e-mail: info@nestker.com. Languages of communication: Hungarian and English.

6.6. Transfers to Third Countries

Based on the territorial scope of the GDPR (Article 3), the Regulation applies to all processing activities involving personal data of persons located within the EU/EEA. Accordingly, the Service Provider processes personal data of data subjects within the EU/EEA in all cases in accordance with the GDPR; data of data subjects located in third countries are processed by the Service Provider applying the GDPR as the governing standard. Where personal data are transferred to a third country outside the EU/EEA, the Service Provider ensures that the transfer takes place only where the conditions set out in Chapter V GDPR are met, in particular on the basis of an adequacy decision of the European Commission (Article 45 GDPR) or appropriate safeguards, including in particular the standard contractual clauses adopted by the European Commission.

7. Rights of Data Subjects

Under the GDPR, data subjects, including both Users and Advertisers, have the following rights:

Right of access (Article 15 GDPR): The data subject has the right to obtain information as to whether personal data concerning him or her are being processed and, where that is the case, to access the personal data and information concerning the circumstances of the processing.

Right to rectification (Article 16 GDPR): The data subject has the right to request rectification of inaccurate or incomplete personal data.

Right to erasure (Article 17 GDPR): The data subject has the right to request erasure of his or her personal data where the legal basis for processing has ceased to exist or the processing is unlawful.

Right to restriction of processing (Article 18 GDPR): The data subject has the right to request restriction of processing where the relevant statutory conditions are met.

Right to data portability (Article 20 GDPR): Where processing is based on consent or a contract and is carried out by automated means, the data subject has the right to receive the personal data he or she has provided to the Controller in a structured, commonly used and machine-readable format (including, but not limited to, CSV, JSON or XML) and has the right to transmit those data to another controller. The right to data portability is an independent data-subject right which may be exercised at any time, irrespective of any request for erasure.

Right to object (Article 21 GDPR): The data subject has the right to object to the processing of his or her personal data where the processing is based on legitimate interests.

Right to withdraw consent: Where processing is based on consent, the data subject has the right to withdraw consent at any time. Withdrawal does not affect the lawfulness of processing carried out before withdrawal. For the purposes of this Notice, processing based on consent includes in particular:

(i) the use of statistical, analytics and marketing cookies; (ii) the sending of push notifications and electronic communications for direct-marketing purposes; (iii) confirmation by the legal representative of the registration of a Minor User; and (iv) any other processing activities based on consent introduced by the Controller in the future.

How to exercise data-subject rights: by sending a clear request to info@nestker.com. The Service Provider may request proof of the data subject's identity in order to prevent abuse; where reasonable doubts arise concerning the identity of the data subject, the Service Provider may suspend fulfilment of the request until identity has been appropriately verified. The Service Provider handles data-subject requests in accordance with the GDPR without undue delay and in any event within one month. Taking into account the complexity and number of requests, this period may be extended by a further two months; the Service Provider informs the data subject of any such extension, together with the reasons for the delay, within one month of receipt of the request. Where the Service Provider does not act on the data subject's request, it informs the data subject within one month of receipt of the request of the reasons for not taking action and of the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

8. Termination of User and Advertiser Accounts and the Fate of Data

8.1. Deletion of a User Account

The User may delete his or her account at any time, without giving reasons and without any consequence or payment obligation, in the Application settings. Deletion is irreversible; the Service Provider completes deletion of the account within no more than 30 days from submission of the request. If, at the time of deletion, the User has outstanding obligations arising from ongoing transactions concluded on the Marketplace, deletion of the account does not release the User from those obligations.

8.2. Termination of an Advertiser Account

The Advertiser may terminate the legal relationship at any time, without giving reasons, by deleting the Advertiser Account. Termination does not affect ongoing Transactions; the Advertiser must complete them and pay any commission due.

At the same time as the account is terminated, the Service Provider deletes the data, except for data that must be retained pursuant to a statutory obligation, for example for accounting or tax purposes.

9. Complaints and Remedies

9.1. Complaint to the Controller

The data subject may submit a complaint relating to processing using the following contact details:

- E-mail: info@nestker.com
- Postal address: 6300 Kalocsa, Majoranna utca 3.

The Service Provider investigates complaints received within 30 days and responds in writing.

9.2. Complaint to the Supervisory Authority

The data subject has the right to lodge a complaint with the Hungarian National Authority for Data Protection and Freedom of Information (NAIH):

- Address: 1055 Budapest, Falk Miksa utca 9-11.
- E-mail: ugyfelszolgalat@naih.hu

- Website: www.naih.hu

9.3. Judicial Remedy

Where the data subject's rights relating to the processing of personal data are infringed, the data subject may bring proceedings before a court. Jurisdiction lies with the competent regional court determined by the registered office of the Controller or by the domicile or place of residence of the data subject.

A data subject whose habitual residence is in an EU/EEA Member State may, pursuant to Article 79(2) GDPR, also bring proceedings against the Controller before the courts of the Member State in which the data subject has his or her habitual residence.

A data subject located in a third country outside the EU/EEA may, under the GDPR, enforce his or her rights relating to the protection of personal data before the competent Hungarian court determined by the registered office of the Controller.

10. Notice-and-Action Mechanism under the DSA

Users may submit a notice under Article 16 of Regulation (EU) 2022/2065 (DSA) concerning advertisements or other content they consider to be illegal at the following contact address: info@nestker.com. The notice must contain: (i) precise identification of the content concerned, including a link or other identifier; (ii) a sufficiently substantiated explanation of the reasons why the content is alleged to be illegal; (iii) the name and contact details of the person submitting the notice; and (iv) a statement by the notifier made in good faith that the information contained in the notice is accurate and complete. The Service Provider examines the notice without undue delay, diligently and objectively, and informs the notifier electronically of its decision and the reasons for it.

11. Data-Security Measures

In processing personal data, the Controller applies appropriate technical and organisational measures in accordance with Article 32 GDPR to ensure the security of personal data. The User is responsible for keeping the login credentials provided by the User confidential and for all activity associated with the User's account. In the event of unauthorised access, the User must notify the Service Provider without delay at info@nestker.com.

12. Cookies, SDKs and Tracking Technologies

On the website and in the Application, the Service Provider may use cookies, mobile SDKs, local-storage solutions, device identifiers and other technical technologies and, where consent has been given, tracking technologies for the operation and security of the Application, maintenance of user sessions, processing of payments, delivery of notifications, error reporting, performance measurement and, where applicable and where an appropriate legal basis is available, analytics purposes.

Data processed include, in particular, cookie identifiers, device identifiers, application-installation identifiers, push tokens, IDFV/GAID-type identifiers, IP address, browser and operating-system type, device and application version, screen resolution, session identifiers, application-usage data, crash-reporting data (crash logs), and notification and analytics preferences provided by the data subject.

Technologies necessary for the operation of the Application may be used, in particular, for login, identification, data security, fraud prevention, App Check / integrity protection, payment redirects, service-related notifications, troubleshooting and service security. The legal basis for the use of these technologies is performance of the contract with the User (Article 6(1)(b) GDPR) and/or the legitimate interest in the secure operation of the Application (Article 6(1)(f) GDPR).

Third-party SDKs and technologies used in the Application may in particular relate to Google / Firebase, Google Maps, Stripe, Apple and Google Play services. These providers may also process personal data in accordance with their own privacy notices, data-processing terms and platform rules.

Where analytics, marketing or other non-essential tracking technologies are used, the Service Provider requests the data subject's prior, freely given, specific and properly informed consent (Article 6(1)(a) GDPR), in accordance with Section 155/A of the Hungarian Privacy Act, Directive 2002/58/EC (ePrivacy Directive), and the GDPR rules on consent, and provides the possibility to manage the related settings. Consent may be withdrawn at any time, without restriction and without giving reasons; withdrawal does not affect the lawfulness of processing carried out before withdrawal.

Retention period: Session cookies and session-type identifiers are automatically deleted or expire at the end of the session. Data collected by analytics and other non-essential technologies are retained by the Service Provider 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. After expiry of the retention period, the data must be deleted or anonymised.

Further detailed information relating to this Section 12 is available in the Cookie Notice on the website and through the privacy or settings interface available within the Application.

13. Personal Data Breach Management

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (Article 4(12) GDPR).

The Controller notifies the NAIH of a personal data breach within 72 hours after becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of data subjects (Article 33 GDPR). If the 72-hour deadline is exceeded, the reasons for the delay must accompany the notification.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Controller informs the affected data subject without undue delay and in clear and plain language of the nature of the breach, its likely consequences, and the measures taken or proposed to address it (Article 34 GDPR).

The Controller documents all personal data breaches in an internal register, including the facts relating to the breach, its effects and the remedial action taken, irrespective of whether a notification obligation applies (Article 33(5) GDPR).

14. Availability and Amendment of the Privacy Notice

The Privacy Notice in force is continuously available on the Service Provider's website (nestker.com); the link provided within the Application directs users to the notice published on the website. The Service Provider reserves the right to amend the Privacy Notice unilaterally.

The Controller informs data subjects of amendments to the Privacy Notice before such amendments enter into force, in accordance with the notice periods applicable to amendments of the GTC and the Advertiser Terms.

The Service Provider retains previous versions of the Privacy Notice in archived form and makes them available to the data subject upon request.