Privacy Notice

View Privacy Notice in :
[Czech] | [Austrian German] | [German] | [Croatian] |
[Hungarian] | [Polish] | [Slovak]

Version: 1.0
Last Updated: October 19, 2026

Introduction - 01

Nuclei Technologies, Unipessoal Lda (Portugal) ("**Nuclei**", "we", "us", "our") is committed to protecting the privacy and security of personal data. This Privacy Notice explains how we collect, use, disclose, and protect personal data when you interact with our SDKs, websites, chat and voice services, and other platforms.

Who We Are

EU Controller Information

- **Core platform operation:** CDNA Technologies Pvt Ltd (India) F1-4141, Sobha Arena The Park Thalaghattapura PO, Kanakapura, Main Road, Uttarahal, Bangalore, 560062, India (info@gonuclei.com)
- **EU-facing commercial services:** CDNA Technologies Pvt Ltd (India) and Nuclei Technologies Unipessoal Lda (Portugal) (Joint Controllers) Rua Quinta da Lobita N° 65, 3° A 2775-621 Carcavelos, Portugal (info@gonuclei.com)
- **EU statutory compliance:** Nuclei Technologies Unipessoal Lda (Portugal) Rua Quinta da Lobita N° 65, 3° A 2775-621 Carcavelos,

Portugal (info@gonuclei.com)

You may contact either entity regarding your data protection rights.

What Data We Collect

Depending on the service and the use-cases we *may* collect and process the following categories of personal data, depending on the product or services you are using:

Direct from the User Interaction: (e.g., Using the products, filling out forms, email correspondence).

- **Identity Data:** Name, title, date of birth, identity proof, nationality.
- **Contact Data:** Address, email address, phone numbers.
- **Personalization Data:** Message text, uploaded photo or video (if you choose to include them). This content is processed solely to personalise your order or service delivery.
- **Usage Data or Analytics Data:** Information, pseudonymous form, about how you use our products, and services to help improve the Service, enhance user experience
- **Marketing and Communications Data:** Preferences for receiving marketing materials and communication history if opted by you.
- **Chat and voice support data** – chat messages, voice recordings and transcripts.

Passive Collection:

In Addition, we may passively collect the following **technical information** only for service functionality, security, and debugging purposes:

- **App Information**: App Version, App Version Code, Partner App Version, IP Address, LatLng
- **Device Data**: Device ID, Device Type, OS Version, FCM-token, Device-Token
- **Display & Localization**: Screen Density, Locale

Data from Other Controller / Joint-Controller / Processor:

- **Loyalty data**: For example Magenta Hearts balance fetched from other trusted and contracted Joint-Controller for related loyalty operations when applied. We do not obtain personal data from publicly available sources.
- **Payment data** – limited metadata for payment status and confirmation (but not card details).

We do not intentionally collect or process special-category data (e.g., biometric, health, or political information). If such information is incidentally provided, it is deleted or anonymised immediately.

How We Process and Store Data

We collect and process personal data only for specified, lawful purposes related to the delivery and improvement of our services — for example, providing and operating our SDK and platform features, authenticating users, processing transactions, delivering notifications, supporting customers, ensuring security, and analysing performance.

Our processing follows the principles of lawfulness, fairness, transparency, data minimisation and accuracy. Data is stored securely using encryption, access controls and monitoring systems to prevent unauthorised access, alteration or loss. Where appropriate, data is pseudonymised or anonymised to enhance privacy protection.

Certain customer-support and communication features may use automated or AI-assisted technologies, operated securely on trusted cloud platforms such as Microsoft Azure or Amazon Web Services (AWS), to help generate and improve responses; all such processing is supervised by Nuclei India, limited to service-quality improvement, and does not involve any automated decisions that produce legal or similarly significant effects on individuals.

Legal Basis for Processing

We process personal data only when there is a lawful basis to do so under the General Data Protection Regulation (GDPR), and other applicable laws.

Depending on the specific context, processing may rely on one or more of the following legal bases:

- **Contractual Necessity:** when processing is required to perform a contract with you or your organisation, or to take steps at your request before entering into a contract. This includes delivering and operating our Software Development Kit (SDK) and platform features, managing user accounts, processing transactions, and providing customer support.
- **Legitimate Interest:** when processing is necessary for our legitimate business interests, such as ensuring the security and reliability of our systems, preventing misuse or fraud, analysing usage patterns, and enhancing product performance. These activities reflect our legitimate interests in maintaining a secure, reliable, and continuously improving platform for users, provided that such interests do not override your fundamental rights and freedoms.
- **Consent:** when you have clearly agreed to the processing of your personal data for one or more specific purposes, such as receiving marketing communications or enabling optional features. You may withdraw your consent at any time by contacting us or by provided user flows within the platform. Withdrawal of consent will not affect the lawfulness of processing carried out before such withdrawal.
- **Legal Obligation:** when processing is required to comply with a legal or regulatory obligation, such as tax, accounting, or record-keeping requirements.

We process personal data only for clearly defined and lawful purposes.

Most processing occurs to deliver and operate our SDK and related services—for example, authenticating users, enabling features, or

maintaining system functionality. Such processing is carried out because it is necessary for the performance of a contract or to take steps at your request before entering into one.

We also process data to manage transactions and fulfilments, such as booking, loyalty, or gift-card operations. This is done on the basis of contractual necessity and, where accounting or regulatory retention is required, to meet our legal obligations.

For customer-support interactions, including our chat and voice-based assistance, we process chat messages, voice recordings and related logs. These are handled under our legitimate interest in providing and improving support quality, are encrypted, and are retained only for a short operational period before secure deletion or anonymisation.

Certain technical and telemetry data (such as device identifiers, IP addresses or crash logs) are processed to ensure system security, detect abuse, and debug errors. This is done under our legitimate interest in maintaining the safety and reliability of our services and retained only as long as necessary to detect or resolve issues.

Where you have opted in, we use your contact information for marketing and promotional communications on the basis of consent. You can withdraw your consent at any time by following the unsubscribe link in our communications or by contacting us directly.

For analytics and service-improvement purposes, we process aggregated usage data under our legitimate interest in understanding product performance and user engagement. Such data is retained in anonymised form or deleted once the analysis is complete.

Payments made through our platform are facilitated by **Braintree (PayPal Europe)**. Payment-related metadata is processed as contractually necessary to authorise and complete transactions.

Card details are never accessed or stored by Nuclei and are processed directly by the payment provider in accordance with its legal obligations.

Data Retention and Deletion

In some cases, providing certain personal data is a contractual or statutory requirement. Without such data, we may be unable to provide you with access to certain SDK or platform features or to complete specific transactions (for example, payment processing or fulfilment).

We retain personal data only for as long as it is necessary to fulfil the purposes described in this Notice or to comply with legal, accounting, or regulatory requirements.

The exact retention period depends on factors such as:

- the type of data and the service or transaction it relates to;
- the legal or contractual obligations that apply (for example, financial-record retention laws);
- the need to resolve queries, disputes, or prevent fraud; and
- whether you have given consent for extended use.

When personal data is no longer required, it is securely deleted or irreversibly anonymised in accordance with our internal Data Retention Policy, which defines specific time frames and deletion methods.

Payments Processing

Payments within the Service are processed through a third party payment gateway. Payment information is collected and processed directly by the payment processor or the bank for authorising and completing transactions.

Nuclei does not store or access your card details.

Cookies and Similar Technologies

We use cookies and similar technologies (such as tokens or local-storage identifiers) to help our website function properly, remember your preferences, measure performance and improve our services.

Cookies are small files or identifiers placed on your device to recognise your browser or app session and to enable certain features. Some are essential for core functionality (for example, authentication or session management), while others are optional and help us understand usage patterns or improve performance.

Essential cookies are processed on the basis of our legitimate interest or contractual necessity. Optional or analytical cookies are used only with your consent, in accordance with the **EU ePrivacy Directive** (2002/58/EC) and Article 6(1)(a) GDPR.

Session cookies expire automatically when you close your browser or end the session. All cookie data is transmitted securely (HTTPS) and, where applicable, marked as Secure and HttpOnly.

For detailed information about each category of cookie, the legal basis, and retention periods, please see our **Cookie Details Annex**.

Joint Controllers

For some partner services, we and the partner decide together how certain data is used. This applies to loyalty data and to limited data about your activity used to make the partner's offers more relevant to you. For this processing, we and the partner are joint controllers. Each party handles requests relating to the processing it carries out. You may contact either party.

Sharing and International Transfers

We share personal data only with authorised partners and trusted sub-processors who assist us in operating our SDKs, websites, and related services—for example, providers of hosting, infrastructure, notifications, communication, analytics, or customer support.

Transfers of personal data may occur between **Nuclei group entities** (e.g., Nuclei Technologies Unipessoal Lda in the EU and CDNA Technologies Pvt Ltd in India) and our approved sub-processors, depending on the service and region in which you use our products.

When such transfers involve countries **outside the European Economic Area (EEA)**, we ensure that your personal data remains protected through one of the following (or combination of) safeguards:

- **Standard Contractual Clauses (SCCs)** approved by the European Commission;
- An **adequacy decision** by the European Commission confirming that the destination offers an equivalent level of protection;
- A **Data Processing Agreement (DPA)** incorporating security and confidentiality obligations; or
- Other legally recognised mechanisms under Articles 44–49 GDPR.

We do **not sell** personal data. All third parties that process data on our behalf are bound by written contracts that require them to maintain appropriate technical and organisational safeguards consistent with GDPR and our internal information-security standards.

Push Notifications through Partners: In certain integrations, notifications are delivered via our partner's technical infrastructure (for example, through Deutsche Telekom(DT) - Europe's application using Google Firebase Cloud Messaging or Apple Push Notification Service). In these cases, those services are engaged and managed by our partner, and Nuclei does not directly contract with or instruct those providers. Accordingly, they are not sub-processors of Nuclei.

Data Hosting and Administration: While data for each region is hosted locally (for example, in EU data centres for European clients), infrastructure administration and support are centrally managed by Nuclei's India-based operations team under intra-group Standard Contractual Clauses (EU 2021/914, Module 2 – Controller to Processor) and strict access controls.

For transparency, a current overview of the categories of sub-processors we use—including region, purpose, and applicable safeguards—is maintained in our **Sub-Processor Register**. This register is updated whenever new vendors are added or replaced, with notice provided to affected partners at least 30 days before activation.

Automated Decision-Making and Profiling

We do not make decisions about individuals that are based solely on automated processing, including profiling, which produce legal effects or similarly significant impacts (as defined under Article 22 of the GDPR).

Any personalisation or recommendations offered within our services are limited to enhancing user experience and do not have any legal or significant effect on users. All AI-assisted or machine-learning features are used strictly to support human-driven customer service and product improvement.

Your Data Protection Rights

You may exercise your rights of *access*, *rectification*, *erasure*, *restriction*, *portability*, *and objection*, *and withdraw consent* where applicable, by emailing **privacy@gonuclei.com**. We may request proof of identity before processing your request.

Your request will be responded to within **30 days**. If additional time is needed due to complexity or volume of requests, we will inform you within this period and provide an estimated response time.

If you believe that your personal data has been processed unlawfully or that your data-protection rights have been infringed, you have the right to lodge a complaint with a competent supervisory authority in the European Economic Area, in particular in the country of your habitual residence, place of work, or where the alleged infringement occurred.

Security of Your Personal Data

We apply appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

These measures include **encryption** in transit and at rest, strict **access control** based on roles, monitoring and logging of system activities, regular **security reviews**, and staff **awareness training**.

Our information-security management system is certified to **ISO 27001:2022**, and data is processed within **regional data centres** in accordance with applicable localisation and transfer-safeguard requirements.

We also evaluate our third-party service providers for compliance with recognised security standards and require them to implement equivalent safeguards.

Data-Breach Notification: If a personal-data breach occurs that is likely to result in a risk to individuals, we will notify the appropriate supervisory or regulatory authority and, where required, the affected individuals in accordance with applicable data-protection laws (for example, Articles 33 and 34 of the GDPR).

Children's Data

Our services are not intended for children under 16. If we discover such data was collected, we will delete it.

Updates to This Notice

We may update this Notice to reflect changes in our processing or legal obligations. Material changes will be communicated through our website or SDK interfaces. The latest version will always be available at our website.

Contact Us

If you have any questions about this Privacy Notice or how we handle your personal data, please contact:

DPO: Vimal Sharma (privacy@gonuclei.com)

Main Entity (Primary Controller): CDNA Technologies Pvt. Ltd. (India) F1-4141, Sobha Arena The Park Thalaghattapura PO, Kanakapura, Main Road, Uttarahal, Bangalore, 560062, India (info@gonuclei.com)

EU Representative: Nuclei Technologies, Unipessoal Lda Rua Quinta da Lobita N° 65, 3° A 2775-621 Carcavelos, Portugal (info@gonuclei.com)

Visit this link to read about out Terms and Conditions.