

Hexa Hexa!

Privacy Notice

English

Version 2 October 2026 • Effective from 2 October 2026

2026-10-02

This Privacy Notice explains how we handle personal data in Hexa Hexa!, its open beta and the website at hexahexa.net, and how you can exercise your rights. Acknowledging this notice does not mean consenting to every use of data described in it. The Terms of Service are provided separately.

1. Controller, scope and contact
2. Information we process
3. Why we process information and our legal grounds
4. What other players can see
5. Providers and other recipients
6. International processing
7. Cookies and information on your device
8. How long information is kept
9. Your choices and data protection rights
10. Updates to this notice

1. Controller, scope and contact

Mikołaj Wiśniewski, a sole trader conducting business under the name LYNXCODE Mikołaj Wiśniewski, Polish tax identification number (NIP) 5662028075, at ul. Południowa 21B/1, 06-450 Głinojeck, Poland, is the controller of personal data processed to provide Hexa Hexa!. Privacy requests can be sent to contact@hexahexa.net or by post to that address. This notice covers the game, account website and communications with us; app stores and providers may separately process data under their own notices.

2. Information we process

Account information: email, username, selected country, password hash, internal account ID, language, avatar, tutorial status, account creation and update dates, verification status, last login, activity flags and the recorded policy-acceptance time. Country is supplied by you; it is not GPS location. Current registration does not request your legal name, postal address, phone number or birth date.

Authentication and security information: login sessions, authentication and password-reset tokens, source IP addresses, browser user-agent information, request and session times, and information used to limit abusive requests and investigate faults. Your password is submitted for authentication and stored as a hash in the account database. This does not mean passwords can never appear in local diagnostics; see section 7.

Gameplay and progression: deck names and contents, collection and cosmetic ownership, selected cosmetics, packs and randomized outcomes, pack-opening counters, currency balances, grants and spending history, daily rewards and claims, challenge progress, matchmaking entries and responses, opponents, moves, cards, dice outcomes, scores, modes, formats, turn timing, connection readiness, match results, ratings and profile statistics. Internal game, transaction and request identifiers link these records to your account.

Technical and support information: server errors, job failures and bot diagnostics can include account or game identifiers and game state. When you email us, we receive your email address, message and any attachments you choose to send. Hosting and communications providers also process connection information needed to provide their services.

The game and website do not include advertising or marketing analytics SDK, automatic client crash-log upload, in-game text or voice chat, or collection of contacts, microphone, camera or precise location data. It does not collect payment-card details through the current store. This does not describe independent processing by an operating system, app store or provider outside our implementation.

3. Why we process information and our legal grounds

The legal grounds below apply where the GDPR governs our processing. Agreeing to our terms or reading this notice is not blanket consent. The minimum account age is 13. Where a processing activity requires consent and applicable law requires authorization by a parent or legal guardian, we must obtain and verify that authorization before that activity starts.

Providing the service — creating and authenticating accounts, restoring access, saving collections and decks, running matches and requested matchmaking, recording results, awarding and spending virtual currency, and sending necessary account messages: processing necessary to perform our agreement with you or take steps at your request before an agreement (Article 6(1)(b)). The registration form requires an email address, username, country and password; without those fields it cannot create an account. Email and password provide account access, the username identifies you in the game, and your selected country appears on your profile.

Security, abuse prevention, investigating bugs, maintaining reliable gameplay, responding to general support inquiries and defending legal claims: our legitimate interests in a secure and fair service and helping people who contact us (Article 6(1)(f)), subject to necessity, proportionality and your rights. Relevant data can include identifiers, connection records, gameplay, wallet history, diagnostics and correspondence. Support needed to fulfil our agreement with you instead relies on Article 6(1)(b).

Compliance with a specific legal obligation, including applicable data-rights requests: Article 6(1)(c), where such an obligation applies to us. If a future optional feature requires consent, we will request it separately, explain the purpose and allow withdrawal without affecting earlier lawful processing. The current account checkbox is not marketing consent.

Game rules automatically determine matchmaking, scores, rewards and ratings. These are in-game decisions; we do not use them to make decisions with legal or similarly significant effects on you. Contact us to contest an account restriction or an incorrect result. This does not exclude rights that apply to a particular decision.

4. What other players can see

Other signed-in players can search for your profile by username and see your username, avatar, selected country, joining month and year, ratings and rank, games played and wins, collection-completion percentage, and up to ten recent match results. Match history includes information such as commander, outcome, scores, mode, format, relative date and an account identifier. Profile responses do not include your email or password.

Opponents receive your player identifier, username, country, selected dice appearance and gameplay information used to run and display the match. Do not put private or sensitive information in usernames or other game fields. The current service does not provide a setting to make the listed profile information private.

5. Providers and other recipients

Authorized people operating and supporting the service may access relevant data for the purposes above. We use Laravel Cloud to host the application, MySQL database and cache in London, United Kingdom. These services handle account and gameplay data, connection records and operational information needed for hosting and security. Daily database backups have seven-day retention.

Ably provides real-time delivery. It processes account-linked client and channel identifiers, connection information, and notifications about games, matchmaking, ratings and virtual balances. The game connects directly to Ably as part of using the service. Its privacy information is at <https://ably.com/privacy>.

Resend (Plus Five Five, Inc.) sends account-verification, password-reset and account-deletion confirmation emails, and outgoing support replies. It processes recipient addresses, message content including account links, and delivery information. Ireland (eu-west-1) is the selected sending region. Support messages addressed to contact@hexahexa.net are forwarded through Cloudflare Email Routing to a Google/Gmail mailbox. These services handle the sender's address, message content, attachments and delivery information; sent support replies are also kept as correspondence.

Computer-controlled opponents use algorithms running within our backend. The current implementation does not send match state or player information to an external AI provider to generate bot decisions. This concerns bot decision processing; hosting and real-time delivery still involve the providers described in this section.

We may disclose relevant data where required by law, to protect rights or investigate abuse where lawful, or to advisers assisting with a legal claim under appropriate confidentiality. Any material new recipient or processing purpose requires an updated notice and, where necessary, a new legal ground.

6. International processing

Our application servers and database are hosted in London, United Kingdom, outside the European Economic Area (EEA). The European Commission recognizes the United Kingdom as providing an adequate level of protection under the GDPR. Transfers from the EEA to the United Kingdom within the scope of that decision rely on it.

Resend states that its account data, including email metadata, logs and API records, is stored in the United States regardless of the sending region. Its published data processing agreement includes EU Standard Contractual Clauses for relevant transfers: <https://resend.com/legal/dpa>. Selecting Ireland for sending email does not mean that all email-related data stays in Ireland.

Other providers may also process information outside the EEA, including in the United States. Google operates servers worldwide: <https://policies.google.com/privacy>. Cloudflare mail forwarding, Gmail, Ably and access by supplier staff or subprocessors may involve locations outside our hosting region. Where the GDPR requires safeguards for a transfer, an applicable adequacy decision or appropriate safeguards, such as EU Standard Contractual Clauses with any necessary additional measures, are required. A selected hosting region does not cover every onward transfer.

Contact contact@hexahexa.net for information about processing locations and applicable transfer safeguards, including how to obtain a copy of them. Supplier privacy information and transfer terms are also available at <https://ably.com/privacy>, <https://ably.com/data-processing-addendum>, <https://www.cloudflare.com/privacypolicy/> and <https://policies.google.com/privacy>.

7. Cookies and information on your device

The website uses a session cookie to maintain your login and form state and an XSRF-TOKEN cookie to protect requests. Their default lifetime is 120 minutes, renewed as you use the site. Server-side sessions can contain your account ID, IP address, browser user agent and last activity.

If you select Remember me, a separate login cookie can last up to 400 days under the current framework configuration. The website_locale cookie stores your language preference for 365 days. Browser controls let you inspect or remove cookies; removing login or security cookies can sign you out or interrupt forms. The website does not set advertising or analytics cookies. Any consent required for additional storage must be obtained separately before it is used.

The game saves an authentication token in an encrypted local file, plus settings such as audio, graphics, matchmaking preferences and selected dice appearance. It also caches card metadata. Logging out removes the saved authentication token. Other local files have no fixed automatic expiry and can remain until removed through app or device storage controls; uninstall and backup behavior depends on the platform.

The game can write request data, including authentication details, and received game events to local diagnostic logs. It does not automatically upload those logs to us. Do not share logs with us or other people until passwords, authentication tokens and other private information have been removed. Optional developer-console history can also be stored locally. These files follow the device-storage handling described above.

The website checks browser and platform information locally to choose a suitable download button. It does not send a separate device fingerprint or analytics event for that selection; ordinary web requests still expose connection and browser information to the server.

8. How long information is kept

Detailed game-log database entries use a one-week calendar-date cutoff, checked by a daily cleanup job. In normal operation this keeps roughly seven to eight days of records; scheduling or queue delays can postpone removal. Only the ten most recent profile-match-history entries remain as new results are recorded. Processed challenge-progress batches are scheduled for removal after seven days. These cleanup rules do not erase the separately stored full games, account statistics or wallet history.

Game authentication tokens currently expire after one week; password-reset and account-deletion confirmation links normally expire after 60 minutes. Expiry prevents further use but is not a promise that the underlying record is deleted at that moment. Likewise, marking an account inactive after 14 days does not delete the account or its collection.

Core account data, collection, progress and full match records are retained for as long as needed to maintain the account and provide the game, without a fixed expiry based solely on the record's age. This does not override the shorter cleanup rules above, applicable erasure rights or the need to review whether inactive or obsolete records remain necessary. Confirmed account deletion removes the departing player's identifiable match data.

We retain support correspondence, including received and sent messages and attachments under our control, for 12 months after the last substantive exchange, then delete it. If specific information is needed to handle an ongoing complaint or legal claim, or to comply with a legal obligation, we retain only that information for as long as necessary for that purpose.

Daily automatic database backups have a seven-day retention period. Deletion from the live application does not rewrite earlier backups: residual data remains until those backups expire. Laravel Cloud separately documents roughly eight-day retention for MySQL binary logs recording database changes, subject to earlier cleanup when storage is running low. Backup and recovery copies are for recovery and related security needs. If a backup is restored, previously completed erasures must be reapplied before the restored data returns to normal use.

Hosting application and access logs have up to one-day retention under our Laravel Cloud Starter configuration; a storage quota can shorten that period. Verbose bot file logging is disabled in the production configuration. Other diagnostic records, including failed-job records and diagnostic extracts, are kept only while needed to investigate and resolve the relevant fault or security incident, or for a specific legal obligation or claim. They are removed when that purpose ends; the weekly game-log cleanup does not remove all of these records. Providers may keep their own operational or delivery records under their service retention rules and legal obligations, separately from our support mailbox.

Confirmed website deletion removes the account, owned collections and progress, balances and wallet event records, authentication records, the departing player's own match history and full games involving that player. Other players keep their own result summaries and statistics with the shared-game link removed. Related game-log database records, database queue payloads, cached game state and accessible structured bot diagnostic files are also cleaned. Delivered email, support correspondence, hosting logs and backup/recovery copies follow their separate lifecycles; they are not all erased immediately by that request. Any justified longer retention must be limited to the relevant data, purpose and duration.

9. Your choices and data protection rights

Where applicable under data protection law, you may request access and a copy of your personal data, correction, erasure, restriction, and portability of eligible data. You may object to processing based on legitimate interests; we must assess your circumstances and stop unless a lawful overriding reason applies. You may withdraw any consent you have separately given without affecting processing that was lawful before withdrawal. These rights have conditions and exceptions; account closure does not automatically require erasure of every record.

Send requests to contact@hexahexa.net. We may request proportionate information to verify your identity, but do not send us your password. If additional evidence is needed, we will explain why and what information is necessary. Account deletion is available through My account on the website, with your current password and an additional email confirmation. Contact us if you cannot complete that flow. Requests for access, a copy of your data, correction or other rights can be made by email; there is no self-service export tool.

For requests covered by the GDPR, we normally respond within one month. If complexity or the number of requests justifies an extension, we may use up to two additional months and will explain the extension within the first month. Requests are normally free; exceptions and any refusal must meet applicable law and be explained.

You may complain to the competent data protection authority, including in the EU/EEA country of your habitual residence, place of work or the alleged infringement. In Poland, you can complain to the President of the Personal Data Protection Office (Prezes Urzędu Ochrony Danych Osobowych, UODO); information on complaints is available at <https://uodo.gov.pl/pl/493/155>. You do not have to contact us first. Rights under other applicable local laws remain unaffected.

10. Updates to this notice

This notice shows its version and effective date. We will explain material changes and inform you before using data for a materially different purpose where required. We will obtain separate consent where the law requires it. An updated notice does not by itself authorize new processing or retrospectively validate earlier processing.