

REGO Guardian Application Privacy Policy

Effective Date: September 7th, 2026

REGO Payment Architectures, Inc. ("REGO") provides technology platforms designed for the management of the under-18 age group in the global online market. REGO Guardian ("Guardian") is a parental-consent service: when an app, game, or online platform (a "Platform") needs a parent's permission before a child can do something, Guardian verifies that a responsible adult is who they say they are and is that child's parent or guardian, records the parent's decision, and gives the Platform a signed answer, and nothing else (the "Service"). This Application Privacy Policy covers only the Service, which is provided through the Guardian app for iOS and Android and the Guardian parent portal on the web (collectively, the "App"). There is a separate Website Privacy Policy that covers REGO's websites, including regoguardian.com.

We are concerned about online privacy issues and want you to be familiar with how we collect, use and disclose your Personal Information (as defined below). The most important things to know are: we do not sell your Personal Information; we do not participate with others in any form of tracking; we do not use or support ads; we do not hold your child's legal name, birthday, or photo; and the information used to run your family's Guardian account is provided by parents, not children.

This Policy does not address our practices regarding information that we collect through any website, or by any other means, other than through the App; nor does this Policy govern the collection, use or disclosure of information by any affiliate or subsidiary (collectively, "Affiliated Entities"), by the Platforms you approve, or by other third parties. By using the App, you agree to the terms and conditions of this Policy. If you do not agree, please do not use the App and email us at privacy@regopayments.com to let us know your concern.

Table of Contents

1. Kids Privacy Assured by PRIVO
2. Changes in this Privacy Policy
3. Children Under 13 (US) and Under 16 (EU)
4. Types of Information Collected
5. What We Never Hold
6. How Information Is Used
7. How Verification Works
8. What Platforms Are Told
9. Third-Party Service Providers
10. How Personal Information Is Disclosed
11. Links and Third-Party Sites
12. Data Security
13. Data Retention
14. Changing or Deleting Information
15. Jurisdictional Issues

- 16. A Note to EU Citizens
- 17. Contacting Us

1. Kids Privacy Assured by PRIVO

REGO Payment Architectures, Inc. is a member of PRIVO's COPPA Safe Harbor program. Guardian is under review for inclusion in REGO's certified properties. If you have questions or concerns about our privacy practices, please contact us at contact@regoguardian.com or privacy@regopayments.com. If you have further concerns after you have contacted us, you can contact PRIVO directly at privacy@privo.com.

2. Changes in this Privacy Policy

From time to time, we may need to change this Policy because of changes in the law, technology, our business, or our attempts to better serve user needs. If we decide to change this Policy, we will post the changes within the Policy itself, with a notice in the App or in other places we deem appropriate. If we change how we use your Personal Information, we will notify you here, by email, or by a notice in the App. All information collected after any update is subject to the updated Policy. If we make material changes to how we use Personal Information collected from children under age 13 in the United States or 16 in the European Union, we will notify Parents by email in order to obtain verifiable parental consent for the new use, to the extent required by law, before making the change.

3. Children Under 13 (US) and Under 16 (EU)

We comply with the Children's Online Privacy Protection Act ("COPPA") to the extent it applies to us and to the App, and with GDPR as it relates to children.

Guardian is used by parents. Only a verified parent, guardian, or authorized adult (a "Parent") may create a Guardian account, and only a Parent adds a child to it. A child never creates a Guardian account, never signs in to the App, and is never asked by Guardian for personal information.

A child may encounter Guardian inside a Platform, at the moment the Platform needs a parent's permission. In that moment the Platform shows a short linking code, which the Parent enters in the App so the request reaches the right family. The child is not asked for anything. The code is used once and expires.

Parents provide verifiable parental consent through the App, after Guardian has verified both the Parent's identity and their relationship to the child (see Section 7). Parents may consent to Guardian's use of their child's information without consenting to disclosure to third parties: the only thing a Platform ever receives is the Parent's signed answer described in Section 8, and Guardian shares nothing about a child with anyone else.

4. Types of Information Collected

Guardian gathers two types of information through the App: "Personal Information" and "Non-Personal Information". Personal Information is information that can be used to identify, contact or locate an individual. Non-Personal Information does not reveal an individual's specific identity, such as aggregated information and technical data.

From Parents, when they create and use a Guardian account:

- Mobile phone number. Stored only as a salted cryptographic hash, which lets us recognize you at sign-in but cannot be turned back into your number.
- Display name.
- Email address, if you provide one, for account recovery and to tell you when your sign-in number changes. Never used for sign-in.
- Whether your identity and your relationship to each child were verified, at what assurance level, by which provider, and when. Not the documents themselves (see Section 5).
- Your decisions: each request you approved, limited, or declined, the limits you set, any house rules you save, and receipts of each decision.
- If you choose to add one, a passkey credential for signing in with Face ID, Touch ID, or your device's screen lock. The private key never leaves your device.
- If you allow notifications, a device token so we can tell your phone a request has arrived.

About each child, entered by the Parent:

- A display name the Parent chooses. It does not have to be the child's real name.
- An age band (for example 10 to 12), never a date of birth.
- The relationship type (parent or guardian).
- For each Platform the child is connected to, a distinct pseudonym Guardian generates. No two Platforms receive the same pseudonym, so no two Platforms can connect their records of the same child.

From Platforms, when they ask for a Parent's decision:

- Which Platform is asking, what permissions it is asking for, and its stated purpose.
- The child's pseudonym for that Platform.

Non-Personal Information, collected automatically:

- Server log files: the IP address of the device using the App, the time of each request, and the endpoint used. Used to protect the Service, for example to limit how many sign-in codes one address can request, and to diagnose problems.

Guardian uses Mixpanel for product analytics in the App and the parent portal, so we can see which steps parents complete and where they get stuck. Mixpanel receives a pseudonymous account identifier generated by Guardian (never your phone number, its hash, or your name), the name of the screen or action, the time, and the device type, operating system version, and App version. Events carry no Personal Information, IP-based location is turned off, and Mixpanel is not used to track you across other apps or websites. No analytics code runs on any screen a child sees: the linking code and the embedded ask frame are measured only as anonymous, aggregate counts from Guardian's own server logs. Guardian does not use advertising SDKs, does not fingerprint devices, and does not collect location.

5. What We Never Hold

Legal names, birthdays, photographs, government identity documents, birth certificates, schools, home addresses, locations, and anything a child does inside a Platform. Guardian's systems have no fields for these; adding one would be a code change that fails our own checks, not a setting.

Identity and relationship documents go to our verification partner directly (Section 7). Guardian never receives them and cannot retrieve them.

6. How Information Is Used

Our primary purpose for collecting information is to provide the Service. We use Personal Information in the following ways:

- Sign-in. The hash of your phone number recognizes you; a one-time code is texted to your number, or your passkey confirms it is you.
- Verification. To confirm you are an adult and that you are the child's parent or guardian, so that Platforms can rely on your decision.
- Decisions and receipts. To present each Platform request to you, record what you decided, apply the limits you chose, and give the Platform your answer.
- Notifications. Your device token is used to tell you a request is waiting. Your phone number is used only to text you a sign-in code: one message each time you sign in without a passkey, and never marketing. Message and data rates may apply, and you can reply STOP to any code to opt out of texts. We do not share your mobile number with third parties or affiliates for marketing or promotional purposes. Your email is used for account recovery and sign-in changes.
- Administrative communications. To send you important information about the Service, changes to our terms and policies, or other administrative notices.
- Security and integrity. To detect and limit abuse of the Service, for example repeated sign-in attempts, and to investigate incidents.
- Internal business purposes, such as audits and maintaining the technical functioning of the Service.

We do not use Personal Information for advertising, profiling, or automated decisions about a child. We do not sell Personal Information. We reserve the right to share Non-Personal Information that has been completely aggregated or anonymized, such that no one, including REGO, can associate it with you or your child.

7. How Verification Works

Guardian verifies two things, separately, before any decision you make is passed to a Platform:

1. That you are an adult who is who you say you are. Our identity verification partner, Persona Identities, Inc. ("Persona"), checks a government-issued identity document and a selfie.
2. That you are this child's parent or guardian. Persona checks a relationship document, such as a birth certificate or guardianship order, and confirms that the parent named on it matches the adult verified in step 1.

Both checks happen with Persona directly: the documents are captured in Persona's own interface, checked by Persona, and redacted by Persona at our instruction as soon as the check completes, so the images and the details read from them are gone and only the result remains. What returns to Guardian is the result of each check: verified or not, the assurance level, a reference number for the check, the time it ran, and, for the relationship check, whether the name matched. Guardian does not receive the document, the images, or the names on them. If a check cannot be completed, no relationship is recorded and Guardian tells you what to do next. Nothing is passed to a Platform on your behalf until both checks have cleared.

8. What Platforms Are Told

When you decide on a request, the Platform receives a signed answer containing:

- Whether a verified parent approved, and for which permissions.
- Any limits you set, such as spending limits or features that stay off.
- The child's age band.
- The child's pseudonym for that Platform.
- The time of the decision, and a reference the Platform can use to check later whether the approval still stands.

The Platform does not receive your name, your phone number, your email, your child's display name, or any document. If you revoke an approval, the Platform learns that the approval no longer stands on its next check. Each Platform sees its own pseudonym for your child, so no two Platforms can connect their records. If a Platform asks us for more than this, the answer is no.

9. Third-Party Service Providers

The chart below summarizes the Third-Party Service Providers used by the App, and the data made available to them.

Service provider	Purpose	Personal Information	Non-Personal Information
Microsoft Azure	Cloud infrastructure, including encrypted storage and compute	Data is stored encrypted. Microsoft staff are not able to access it.	IP address, HTTP headers
Lightstream	Azure managed services (operations, monitoring, patching)	Data is stored encrypted. Lightstream staff are not able to access it.	IP address, HTTP headers
Persona Identities, Inc.	Identity verification and parent-child relationship verification	Government identity document, selfie, relationship document, and the names on them, captured in Persona's interface and never sent to Guardian. Parent email or phone, if Persona uses it to run the check.	Device and browser information Persona collects in its interface
Mixpanel	Product analytics for the App and parent portal	Pseudonymous account identifier only	Screen and action names, timestamps, device type, os and app version
Twilio	Text-message delivery of sign-in codes	Parent mobile number	None

Service provider	Purpose	Personal Information	Non-Personal Information
Apple	Push notification delivery (APNs)	Device push token	IP address

Guardian uses no advertising, or attribution provider. Contact us at privacy@regopayments.com for more details on any third party.

10. How Personal Information Is Disclosed

We do not share, sell, rent or trade your Personal Information other than as disclosed below or otherwise within this Policy.

Platforms. A Platform receives only the signed answer described in Section 8, and only for a request you decided on.

Third-Party Service Providers. We work with the third parties in Section 9, who provide services including hosting, data storage, identity verification, text-message delivery, push notifications, and product analytics. We share Personal Information with them for the sole purpose of enabling them to provide those services, under written agreements that require them to keep it confidential and secure.

Assignment. We reserve the right to transfer any and all information that we collect to an Affiliated Entity or a third party in the event of any reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of REGO's business, assets or stock (including without limitation in connection with any bankruptcy or similar proceedings).

Law enforcement; emergencies; compliance. We reserve the right to disclose Personal Information and any other information we collect as we believe to be appropriate (a) under applicable law; (b) to comply with legal process served on us, as required by law and when we believe that disclosure is necessary to protect our rights and/or to comply with a judicial proceeding, court order, or legal process served on us; (c) to respond to governmental requests; (d) to enforce our Terms of Use; (e) to protect our operations or those of any Affiliated Entities; (f) to protect the rights, privacy, safety or property of REGO, the Affiliated Entities, you or others; and (g) to respond to any claims and permit us to pursue available remedies or limit the damages that we may sustain.

11. Links and Third-Party Sites

The App opens our verification partner's pages so you can complete identity and relationship checks, and may contain links to third-party websites, including the Platforms you approve. These sites are not under REGO's control, and we are not responsible for their privacy practices or contents. Information you provide on a third party's site is collected by, and governed by the privacy policy of, that third party. PLEASE NOTE THAT THIS POLICY DOES NOT ADDRESS THE PRIVACY OR INFORMATION PRACTICES OF ANY THIRD PARTIES, INCLUDING, WITHOUT LIMITATION, AFFILIATED ENTITIES AND THE PLATFORMS YOU APPROVE.

12. Data Security

The security of your Personal Information is important to us. We follow generally accepted industry standards to protect the information you submit to us. Unfortunately, no data

transmission over the Internet can be guaranteed to be 100% secure.

All communication with the App uses HTTPS, with TLS 1.3 where available and a minimum of TLS 1.2 otherwise. Personal Information is stored encrypted on Microsoft Azure infrastructure operated by REGO, in accordance with REGO's Information Security Policy and REGO's SOC 2 Type II program. Your phone number is stored only as a salted hash. Sign-in is by a one-time code sent to your phone or by a passkey held on your device; there are no passwords to steal. Approving, limiting, or revoking a permission in the app requires Face ID, Touch ID, or your device's screen lock. Each Platform sees its own pseudonym for your child, so a breach at one Platform cannot expose your child's activity on another.

13. Data Retention

Guardian keeps the working set: your account, verified status, the family members you added, your decisions, and their receipts, for as long as your account is active.

- Sign-in codes expire after five minutes and are deleted after use. Sessions expire and are deleted on sign-out.
- Verification results are kept with your account. The documents behind them are never held by Guardian; Persona redacts them as soon as the check completes.
- Revoking an approval takes effect on the Platform's next check. The receipt of the original approval, and of the revocation, is kept as the record that consent was given and withdrawn.
- Deleting your account (Section 14) deletes your account, the family members only you added, your sign-in on every device, and your passkeys, immediately. The record that consent was given and withdrawn is kept for up to five years, consistent with the REGO Data Retention Policy, under the pseudonyms only, with no name, number, or document attached, as the evidence a Platform is entitled to that a verified parent decided.
- Accounts with no activity for two years are treated as if a deletion request had been made, consistent with the REGO Data Retention Policy. Activity means signing in. If you left an email address, we send a warning thirty days before the deletion date, and signing in at any point keeps the account.
- Server logs are retained for 12 months, per REGO security policy, and then destroyed.
- Deleted data may persist in database backups for up to three months to guarantee recovery from a disaster; backups are destroyed automatically as they age out and are not accessible to staff other than in an emergency.

14. Changing or Deleting Information

Parents can change their own display name and email, and each child's display name and age band, in the App, along with every permission and house rule. Parents can revoke any approval at any time in the App.

Parents can delete their Guardian account from Settings in the App. Deletion requires confirmation and Face ID, Touch ID, or the device's screen lock, and takes effect immediately as described in Section 13. Parents can also remove an individual child from their family in the App.

If you are unable to change or delete information as described above, or wish to exercise any other right over your information, contact us at contact@regoguardian.com or privacy@regopayments.com with your specific request. We will retain and use information as

necessary to comply with our legal obligations, resolve disputes, and enforce our agreements. We are not responsible for deleting information from the systems of Platforms with which you already shared a decision.

15. Jurisdictional Issues

The App is controlled and operated by REGO from the United States, and is not intended to subject REGO or any Affiliated Entity to the laws or jurisdiction of any state, country or territory other than that of the United States. REGO does not represent or warrant that the App or any part thereof is appropriate or available for use in any particular jurisdiction. Those who choose to access the App do so on their own initiative and at their own risk, and are responsible for complying with all local laws, rules and regulations. We may limit the App's availability, in whole or in part, to any person, geographic area or jurisdiction we choose, at any time and in our sole discretion.

16. A Note to EU Citizens

REGO complies with the rights given to EU Citizens under the General Data Protection Regulation (GDPR). These rights are as follows:

- the right to have your personal information updated to ensure it is up-to-date and accurate;
- the right to withdraw your consent to any processing that is currently being done under your consent;
- the right to receive a copy of the personal information we hold about you;
- the right to request that we delete personal information in certain circumstances;
- the right to have us transfer to another controller the personal information that you have provided us with;
- the right to request a restriction on the processing of your data in some limited circumstances;
- the right to request that we stop processing your data.

For more information on how to exercise these rights please contact us at privacy@regopayments.com. If you are an EU citizen and would like to make a complaint about the way we process your personal data, you can contact the relevant Data Protection Authority. The App is not yet available in the EU; REGO Guardian does not currently have an Article 27 representative and will appoint one before the App is available in the EU.

17. Contacting Us

If you have any questions regarding this Policy, our information practices, or accessibility, please contact us by email at contact@regoguardian.com or privacy@regopayments.com, write to us at the address below, or call 1-844-210-4789. Please note that email communications will not necessarily be secure; accordingly, you should not include identity documents or other sensitive information in your email correspondence with us.

REGO Payment Architectures, Inc. 325 Sentry Parkway, Suite 200 Blue Bell, Pennsylvania 19422 Attention: Customer Service

LAST UPDATED: September 6, 2026

Copyright 2026 REGO Payment Architectures, Inc. All rights reserved.