REGO Application Privacy Policy

Effective Date: July 1, 2025

REGO Payment Architectures, Inc. (“REGO”) provides technology platforms designed for the management of the under-18 age group in the global online market. Our Mobile Apps and Web Apps are part of an online system that enables parents to control and guide their children through their online transactions and allows children to make parent-authorized purchases through the Internet (the “Service”).

This Application Privacy Policy covers only this Service. There is a separate Website Privacy Policy that covers REGO's websites, including www.regopayments.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 nor support ads, we do not even require the actual name of your child, and the data used to support your family’s requests is data provided by parents, not children. This Privacy Policy (the “Policy”) describes our practices in connection with Personal Information that we collect through our Service which is provided through mobile applications on iOS and Android phones and tablets, as well as a “web app” version (collectively, the “App”).

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”) or by third parties. By using the App, you agree to the terms and conditions of this Policy. If you do not agree to the terms and conditions of this Policy, please do not use the App and email us at privacy@regopayments.com to let us know your concern.

Table of Contents

- Kids Privacy Assured by PRIVO: COPPA Safe Harbor Certification & GDPR*kids*™
- Changes in this Privacy Policy
- Children Under 13 (US) and Under 16 (EU)
- Types of Information Collected
- How Information Is Used
- Third-Party Service Providers
- How Personal Information Is Disclosed
- Links and Third-Party Sites
- Data Security
- Data Retention
- Changing or Deleting Information

- Jurisdictional Issues
- A Note to EU Citizens
- Contacting Us

Kids Privacy Assured by PRIVO: COPPA Safe Harbor Certification

REGO Payment Architectures, Inc. is member of PRIVO's COPPA Safe Harbor and **GDPR***kids*™ Privacy Assured. PRIVO is an independent, third-party organization committed to safeguarding children's personal information collected online.

COPPA Safe Harbor Certification

The Program certification applies to the digital properties listed on the validation page that is viewable by clicking on the PRIVO COPPA certification Seal. The certification Seal posted on this page indicates REGO Payment Architectures, Inc. has established COPPA compliant privacy practices and has agreed to submit to PRIVO's oversight and consumer dispute resolution process. If you have questions or concerns about our privacy practices, please contact us at (267) 465-7530 or privacy@regopayments.com. If you have further concerns after you have contacted us, you can contact PRIVO directly at privacy@privo.com.

GDPR*kids*™ Privacy Assured

The Program applies to the digital properties listed on the validation page that is viewable by clicking on the PRIVO **GDPR***kids*™ *Verified Shield*. The PRIVO **GDPR***kids*™ Privacy Assured Program supports child directed services known as Information Society Services under the General Data Protection Regulation (GDPR), to comply with the requirements of this legislation. It impacts any child directed service in an EU Member State and any service globally that collects and or processes the personal data of children and minors. There is no safe harbor for the GDPR to date, but to ensure this company's services meet the program requirements, we conduct regular monitoring and consulting.

REGO Payment Architectures, Inc. will be awarded the **GDPR***kids*™ Verified Shield before the app is available in the EU.

Changes in this Privacy Policy

From time to time, we may need to change our Privacy Policy because of changes in the law, technology, our business, or our attempts to better serve user needs. If we decide to change our Privacy Policy, we will post the changes within the Privacy Policy itself, with an alert on the home screen or in other places we deem appropriate. If we change how we use your Personal Information (defined below), we will notify you here, by email, or by means of a notice on our home screen. We reserve the right to modify this Privacy Policy at any time, so please review it frequently. All information collected after any updates to the Privacy Policy will be subject to the new policy. If we make material changes to how we use the Personal

Information (defined below) 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 of the child's Personal Information, to the extent required by law, prior to making the changes.

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

We are very concerned about the safety of children online. We comply with the Children's Online Privacy Protection Act of 2000 ("COPPA") to the extent it applies to us and to our App, and with GDPR as it relates to children. Only a parent, guardian or authorized adult ("Parent") may create an account for a child in our App. The Parent provides all information required to set up a parent profile and child profile(s), including the child's User ID and Password. A child's use of the App and participation and access to the App is currently not conditional upon his/her providing any Personal Information – they only need their User ID and Password. In any event, a child's use of the App and participation and access to the App will not be conditional upon his/her providing any more Personal Information than is reasonably necessary for them to participate in an activity. Parents are required to provide full verifiable parental consent before providing personal information about their child. Parents have a right to consent to our use of their child's Personal Information without having to consent to the disclosure of that information to third parties, as we do not share your child's Personal Information with any third party, other than service providers and agents necessary to provide the Service.

Types of Information Collected

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

We collect the following Personal Information from Parents when they create an account in our App:

Parent's first and last name, street address, zip code, parent email address, telephone numbers, parent profile name, child nickname, child password, child gender, child date of birth, time zones, transaction thresholds, allowed merchants

We may use this information to identify the parent and obtain full verifiable parental consent for their child's use of the App.

We may collect bank account information, including account number and balance, to use for transfers to and from the family accounts.

For security reasons, we do not store debit card information on our servers; we use the financial institution's core and card service provider to store and transmit that information in accordance with PCI (Payment Card Industry) Data Security Standards.

We also gather purchasing and transaction information based on purchases made using the Service for reporting to Parents, for use in resolving any disputes, and to satisfy obligations to the financial institution that issues the debit card we use for the child's account, as well as to the card network itself. This purchasing and transaction information may be compiled and analyzed on an individual or account basis for the purpose of providing enhanced services and features to the individual or account. Some of this data may be abstracted and/or anonymized in order to be used in an aggregated basis by us for any purpose. For instance, we might use such data to determine that the most common food purchase among 14-year-old boys is pizza. We never sell information that personally identifies a child to any party.

We collect the following information from children (a) when they use the Wishlist functionality on our App or a merchant's site: the URL for the merchant site and the particular products, services, games or other items they wish to purchase from the merchant using the Service, and (b) particular merchants they would like their Parents to authorize as approved merchants.

When you visit and interact with the App, REGO and its third-party service providers may also collect other information (for example, a catalogue of the screens you use). This Information is generally collected through the App from server log files, environmental variables, and database entries.

- Server Log Files. Your Internet Protocol (IP) address is a number that is automatically assigned to the device that you are using by your Internet Service Provider (ISP). This number is identified and logged automatically in our server log files whenever you use the App, along with the time(s) of your visit(s) and the screen(s) that you used. IP addresses may be used for purposes such as calculating App usage levels, helping diagnose problems with the App, administering the App, and enhancing security.
- Environmental Variables. Certain environmental variables, such as your MAC address, device identifier, device type (iPhone or Android), screen resolution, and Operating System version may be collected. These environmental variables are collected by most Apps and websites, and can be used to optimize your experience in the App and to enhance security.
- Database Entries. The App stores the account information in a database, along with information on transactions, and the use of the App itself. This may include items you search for or view with the App, allowing you to find them more easily in the future—for instance, as suggestions in "type ahead" the next time you search.

How Information Is Used

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

1. Purchase Transactions. We will use Personal Information and credit card information to process approved purchase transactions initiated by a child using the Service and to enable the delivery of products purchased using the Service. Purchase and transaction information will be used for reporting to Parents and for repudiation purposes.

2. Notifications and Alerts. Emails, telephone numbers and device identifiers will be used to provide Parents with transaction alerts, approval requests or other reporting, notices or alerts that Parents elect to receive in their parent profiles, child profiles or otherwise as part of the Service.
3. Administrative Communications. From time to time, in our sole discretion, we may use Personal Information to send you important information regarding the Service, changes to our terms, conditions, and policies and/or other administrative information.
4. Internal Business Purposes. We may also use Personal Information for our internal business purposes, such as audits, research and analysis to maintain, protect and improve the Service, ensure the technical functioning of the Service and develop new services. Some information, such as date of birth, is used to ensure appropriate compliance with State and Federal law is being maintained based on age as ages change and new laws are created.
5. Security. REGO may use Wireless Features as an aid in identifying you and reducing the risk of fraud. This includes, but is not limited to, collecting the geo-location of both adults and children. While geo-location information is not disclosed to third-parties, it may be kept solely for security reasons, such as identifying when a device is used at a location significantly distant from your usual area.

We reserve the right to share such Non-Personal Information, which does not personally identify you, with Affiliated Entities and other third parties, for any purpose. Any such information is first completely abstracted and/or anonymized in such a fashion that no one—including REGO—can associate it back to you or your child.

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 storage	Data is stored encrypted. Microsoft staff are not able to access it. Includes IP Address	ISP Location HTTP Headers
Armor	Security-as-a-Service	Security staff may encounter PI when investigating an incident	Server Logs Network Logs Database Logs
Twilio	Text messaging	Parent mobile number Child mobile number (if different)	N/A
Telnyx	Text messaging	Parent mobile number	N/A

		Child mobile number (if different)	
Lightstream	Azure managed services	Data is stored encrypted. Lightstream staff are not able to access it. Includes IP Address	ISP Location HTTP Headers
PrincipiaRAID	Incident response	Security staff may encounter PI when investigating an incident	Server Logs Network Logs Database Logs
Google Firebase	Push Notifications	IP Address Device ID	N/A
Branch.io	Deep Linking, Attribution	IP Address Device ID	Internal User ID Promotion ID

Contact us at privacy@regopayments.com for more details on any third-party.

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 Privacy Policy.

1) Purchase Transaction Merchants. We will share with participating merchants and their agents and service providers transaction information for authorized purchases and the physical address provided for delivery of products purchased from the participating merchant using the Service. We will share debit card information and, to the extent necessary, Personal Information with participating merchants and their payment processors to process approved purchase transactions initiated by a child using the Service. Unless otherwise requested by the parent, this information will always be information provided by the parent (e.g. shipping address) rather than the child.
2) Third Party Service Providers. We work with third parties who provide services including, but not limited to, debit card processing, operating and hosting our App, data storage, email and/or text messaging delivery services and contractors who assist with programming and technical aspects of our App. We reserve the right to share Personal Information with such third parties for the sole purpose of enabling them to provide such services.
3) 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).
4) 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 and terms and conditions of the Service; (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.

Links and Third-Party Sites

The App may contain links to third party websites. These linked sites (including without limitation the websites of Affiliated Entities) are not under REGO's control and we are not responsible for the privacy practices, the contents of or any products or services sold from any such linked site. We provide such links only as a convenience, and the inclusion of a link on the App does not imply endorsement of the linked site by REGO. If you provide Personal Information through any such third-party website, your transaction will occur on such third party's website (not the App) and the Personal Information you provide will be collected by, and controlled by, the privacy policy of that third party. We recommend that you familiarize yourself with the privacy policies and practices of any such third parties. PLEASE NOTE THAT THIS POLICY DOES NOT ADDRESS THE PRIVACY OR INFORMATION PRACTICES OF ANY THIRD PARTIES, INCLUDING, WITHOUT LIMITATION, AFFILIATED ENTITIES AND PARTICIPATING MERCHANTS.

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. Once we receive your information, we use HTTPS encryption to transmit sensitive information such as debit card numbers and user ID and passwords. We specifically use TLS 1.3 where available, and a minimum of TLS 1.2 otherwise. All Personal Information you provide for the Service is stored on secure third-party infrastructure in accordance with their security procedures and the Payment Card Industry Data Security Standard. SSO authentication with the financial institution is used so that only the Parent can access and view the Personal Information and certain other account information, and a child's User ID and password are needed to make a transaction using the Service. We recommend that you inform your children that they should not divulge user IDs and passwords to anyone. Ultimately, you are responsible for maintaining the secrecy of your child's User ID and password and REGO shall not be responsible or liable in any way for damages or losses resulting from a Parent or child divulging or not protecting the child's user ID and/or password.

Data Retention

The App retains user data until a deletion request has been made, and the compliance obligations have expired (no longer than 5 years.) We will mark accounts as inactive after two years without activity, at which point we will treat it the same as if a deletion request had been made. If there is a balance in such an account, we will first seek to return the funds to the user either via electronic transfer back to the original source of the funds, or via check. We store a record of transactions, including the purchase history, for as long as long the account is active and for a period of 366 days after the last transaction as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements. Data that has been deleted is no longer readily available to the application nor reporting systems.

After the compliance obligations have expired, user data that has been marked as deleted will be destroyed. Some information may continue to exist in database backups for up to an additional 3 months to guarantee we can recover from a database disaster. These database backups are automatically destroyed as they age out, and are not accessible to staff other than in the case of an emergency. We have geographically redundant, geo-replicated databases which also generally eliminates the need to access backups.

Changing or Deleting Information

If Parents would like to review, correct, update or delete Personal Information or Non-Personal Information that was previously provided by Parents to us through the App, or collected from their child, they may do so by logging into their account and correcting, updating or deleting such information in the Parent profile or child profile(s). Please note that if required information is deleted, the Service will not function and can no longer be used. If a Parent deletes all information from the Parent profile their account will be closed and all information except transaction information will be deleted in our system. Parents may also elect to delete an entire child profile, in which event such child may no longer use the Service. If a Parent is unable to correct, update or delete their information as described above or wishes to refuse further contact with their child by the App, they should contact REGO at privacy@regopayments.com with their specific request. Please note that we may need to retain certain transaction information for record keeping and reporting purposes, and there may also be residual non-personal information that will remain within our databases and other records, which will not be destroyed. We are not responsible for deleting information from the databases of third parties with whom we have already shared information. We will retain your information for as long as your Account is active or as needed to provide you services.

If you wish to cancel your Account or request that we no longer use your Personal Information to provide you Services, Parents should log into their Parent profile in their Account and select the "delete" button, and if your attempt to close your account online is unsuccessful, you should contact us at privacy@regopayments.com. We will retain and use your information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements. If you no longer wish to receive electronic newsletters and/or promotional emails that we may send to you, you may opt-out of receiving them by following the opt-out instructions included in each newsletter or email, or logging into your Parent profile and updating the communication settings. If your attempts to opt-out by these methods are unsuccessful, you should email us at privacy@regopayments.com with your request.

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.

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.
- 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.
- right to request that we stop processing your data.

For more information on how to action 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 (DPA). Please contact us using the details below to find out more.

Contacting Us

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

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

LAST UPDATED: April 23, 2026

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