LoyalFork Privacy Policy

Last updated: 11 October 2026. **Version:** 1.2.

LoyalFork provides software that helps businesses run customer loyalty programmes, including digital membership passes for Apple Wallet and Google Wallet. This policy explains how personal information is handled when you use the platform or join a participating business's programme.

Who we are

LoyalFork is operated by CENTEX LTD, company number 14712602, trading as LoyalFork. Our registered office is 167-169 Great Portland Street, 5th Floor, London, England, W1W 5PF. You can contact us about privacy at contact@loyalfork.com.

For merchant accounts, platform administration, support and platform security, LoyalFork is the data controller: we decide why and how that information is used.

For a merchant's customer loyalty records, the merchant is normally the data controller and LoyalFork processes information on its behalf. The merchant decides its programme rules and how it uses customer information. Its own privacy notice explains those decisions. Contact the merchant about your membership or rewards; you can also contact us and we will help direct your request.

Where this policy applies and where information comes from

This policy covers the LoyalFork application, merchant signup and billing administration, staff access, customer enrolment and membership communications supplied through the platform. It does not replace a participating merchant's privacy notice or the notices of independently operated payment, identity or Wallet services. A separately operated marketing website may use different tools; its actual practices must be described in its own applicable notice.

We receive information directly from merchant representatives and customers, from authorised merchant staff who enrol or administer members, from Auth0 identity responses, from Stripe billing events and from Wallet registration/update requests. Operational records arise when people use or request support for the service. Merchants must tell customers when staff provide their information to LoyalFork and identify the relevant programme.

Information we handle

- **Merchant and staff accounts:** names, email addresses, business details, locations, account identifiers, organisation memberships, roles and invitations. Auth0 handles merchant sign-in and provides identity information to the platform.

- **Customer membership:** first name, surname, email address, date of birth, membership identifiers and the business whose programme you join. Information may come from you or from authorised merchant staff. The current public enrolment form requires all four personal details, including date of birth; enrolment cannot be completed without them. Date of birth forms part of the membership record. Programme membership is restricted to adults aged 18 or over; the merchant is responsible for assessing programme eligibility and explaining any additional use of this information.
- **Merchant billing:** selected plan and currency, billing period, Stripe customer/subscription/Checkout identifiers, verified payment and subscription status, billing contact details and records of terms acceptance. Stripe collects payment details through its hosted Checkout and billing portal. LoyalFork does not collect full payment card numbers or card security codes through its application.
- **Loyalty activity:** points or stamps, balances, rewards, redemptions and records of changes made by merchant staff or the platform.
- **Wallet information:** pass identifiers, registration and device push identifiers where applicable, pass authentication information, and delivery or refresh status. Pass content may include your membership identifier and balance.
- **Communications and technical records:** invitations, welcome-email delivery records, support correspondence, and operational or security records associated with platform use, including request identifiers, timestamps, request paths, error details and delivery or refresh status. Hosting and authentication services may also handle connection information such as IP addresses.

Please do not send us payment card details or sensitive personal information in support requests.

Why information is used

For processing where LoyalFork is the controller, our intended purposes and legal bases are:

Purpose	Legal basis
Set up and provide the platform to an individual merchant contracting with us	Performance of our contract with that merchant
Manage accounts for staff and representatives of business customers	Legitimate interests in administering the business relationship and authorised access
Respond to support requests and maintain reliable platform operations	Legitimate interests in helping users and maintaining the service; contract where the requester is our contracting customer
Administer merchant subscriptions, verify payments and provide billing support	Contract with an individual merchant; legitimate interests in administering business-customer subscriptions; legal obligation for records required by law

Protect accounts, investigate misuse and establish or defend legal claims	Legitimate interests in protecting users, the platform and our legal rights
Meet a specific legal requirement	Legal obligation, where that requirement applies

Where we rely on legitimate interests, we consider the impact on your rights and interests. You may object to this processing.

For customer loyalty data, we follow the merchant's lawful instructions to enrol members, maintain balances, record rewards, send configured communications and provide or update Wallet passes. The merchant must explain the purposes and legal bases in its privacy notice.

Loyalty rules can calculate balances and reward eligibility automatically. Contact the merchant if you want an explanation of its rules or believe a balance or eligibility result is incorrect.

Required information and automated programme rules

Merchant name, owner contact, country, language, plan and terms acceptance are needed for the current paid signup journey. Omitting required fields prevents signup. Payment information requested by Stripe is supplied directly to Stripe; declining a required payment field may prevent purchase.

The current public customer form requires first name, surname, email and date of birth. This is a platform form requirement, not a statement that the law requires every loyalty programme to collect birth dates. Merchants must explain why the information is needed for their programme. A customer who does not provide the required fields cannot use the current public enrolment flow and may contact the merchant about alternatives or a privacy concern.

Programme rules automatically calculate points/stamps, balances and reward readiness from recorded activity and the merchant's settings. Billing status can automatically restrict merchant operations after non-payment or cancellation. These are service rules rather than a claim that we undertake legally significant automated profiling of customers. Contact the merchant about a loyalty result, or CENTEX LTD about a platform/billing restriction, to request an explanation and review. A stale Wallet display does not override the authoritative membership record.

Emails and marketing

The platform sends account invitations and membership service messages, such as a welcome message containing your membership identifier and optional Wallet links. Promotional email campaigns are not part of the current service.

Merchants must keep membership service message content related to administering the membership. Promotional content may count as marketing even when included in a welcome message.

Merchants are responsible for establishing a lawful basis for their communications and meeting applicable electronic marketing rules. Agreeing to terms or reading this policy does not give consent to marketing. Any future promotional messaging will require a separate lawful arrangement and an appropriate way to opt out before it is enabled.

Who receives information

Authorised merchant staff can access their organisation's loyalty information. Authorised LoyalFork administrators may access information to support and operate the service.

Providers may handle information needed to deliver specific functions:

- Auth0, part of Okta, provides merchant authentication.
- Apple and Google receive information needed for their Wallet services when you choose to add or use a pass. Their own privacy notices also apply to their services.
- Brevo provides email delivery for platform invitations and membership service messages; Auth0 may also deliver identity setup and password-related messages.
- Cloudflare provides public-site proxying, HTTPS delivery and security services and may handle connection metadata such as IP addresses and request information.
- Amazon Web Services provides hosting and database services through Lightsail in London, UK (`eu-west-2`), and private backup storage.
- Stripe provides hosted merchant Checkout, recurring subscription billing and the billing portal. It receives payment and billing information needed to process payments and administer subscriptions; its privacy notice also explains its processing.

We may also disclose information to professional advisers or public authorities where necessary for legal advice, legal obligations or legal claims.

QR codes, logos and camera access

Merchant logos and branding appear on public enrolment pages, printable signup posters, emails and Wallet passes. Merchants must not upload private or unauthorised images as public branding. A signup poster links to the merchant's enrolment page; it does not contain a customer's membership code.

Customer email QR images and Wallet links use customer-specific addresses. Anyone who receives or is given one of these links may be able to view the membership code or add the pass. Keep private links and codes confidential. Email software may request these images when displaying a message.

Staff can choose to use a device camera to scan a loyalty code. Camera access requires browser permission. The scanner processes camera frames in the browser to read the code; scanned identifiers are sent to the platform for membership lookup. The scanner does not upload or store

camera video as a platform feature, and stops the camera when scanning ends or the scanner is closed. Browser site permissions can be managed in browser settings.

International transfers

Providers may process information in the UK, the European Economic Area or other countries, depending on the function and their service arrangements. Where a restricted international transfer is involved, applicable data protection law requires an appropriate transfer arrangement, such as an adequacy decision or approved contractual safeguards. Contact contact@loyalfork.com to request details of the destinations and safeguards applicable to your information.

Cookies and browser storage

The application uses the following cookies and browser storage:

Item	Purpose	Duration
`auth0_state` cookie	Checks that the sign-in response belongs to the sign-in request	Up to 10 minutes; cleared after successful sign-in
`session` cookie	Maintains authenticated platform access	Up to 8 hours; cleared on sign-out
Selected merchant organisation in local storage	Remembers which organisation you selected	Until cleared or replaced
Staff language preference in local storage	Remembers your chosen interface language	Until cleared or reset
Selected workspace view in session storage	Restores your workspace navigation	For the browser page session

Auth0 may use additional cookies on its hosted sign-in pages. Its own privacy and cookie information applies to those pages.

Clearing required cookies may prevent sign-in from working.

Security and incident handling

We use access restrictions, tenant separation, authentication, HTTPS and controlled server-side storage to protect information. Access is limited to authorised staff, operators and providers for their permitted purposes. No internet service or device can be guaranteed completely secure. Notify contact@loyalfork.com if you suspect unauthorised access or a disclosed private membership link.

For an incident involving customer data processed for a merchant, we notify and assist that merchant without undue delay in accordance with applicable duties. Where CENTEX LTD is the controller, we assess and fulfil our own notification obligations. We inform affected individuals where required and explain appropriate protective steps without disclosing credentials or other people's information.

How long information is kept

Retention depends on the purpose of the information and any applicable legal requirement. Customer loyalty records are retained according to the merchant's documented instructions, subject to lawful exceptions.

Information	Retention period or criterion
Merchant accounts and staff memberships	While needed to operate the active merchant account; remaining account information is deleted within 30 days after the post-closure export window ends, unless a specific lawful exception applies
Customer profiles and loyalty transactions	While the merchant's programme is active and the records are needed, until the merchant requests membership closure or deletion; remaining programme data is deleted within 30 days after the merchant's 30-day post-closure export window ends, subject to documented lawful exceptions
Email, invitation and Wallet operational records	Up to 90 days after the relevant event; current membership/pass identifiers and registrations remain while needed to provide an active membership or pass
Security and operational logs	Up to 30 days
Support correspondence	Up to 12 months after the support matter closes
Backups	Up to 30 days before expiry

We process verified deletion requests within the applicable legal time limits rather than automatically waiting for account closure. If information must be retained for a specific legal requirement or an existing dispute, we restrict its use and retain only what is necessary for that purpose. Account closure includes a 30-day merchant export window; the following deletion period is at most 30 days, so remaining active-system records are normally removed within 60 days of closure.

Deleted information may remain in restricted backups until they expire. If a backup is restored, we reapply recorded deletions before returning the restored data to normal use.

Pending merchant applications have a seven-day application validity period; expiry prevents reuse of that application and is not the same as immediate deletion. Retention after expiry is limited to what is needed for payment reconciliation, support, security and applicable recordkeeping. Paid-but-unprovisioned records must be retained for recovery rather than deleted as abandoned applications.

Billing, terms-acceptance and transaction records may be retained separately where needed for applicable legal obligations, disputes or financial recordkeeping. We determine the retention by the applicable accounting/tax record requirements, the relevant transaction or financial period, and any ongoing dispute or legal hold; we restrict further use when the operational purpose ends. Contact us for the retention periods applying to your account. Account closure or removing a Wallet pass does not necessarily erase all related records. We explain any applicable retention when handling a deletion request.

Exercising your right to object

You may object to processing based on legitimate interests by contacting contact@loyalfork.com and identifying the relevant activity. We will assess your circumstances and explain whether there are lawful grounds to continue. Where applicable, an objection to direct marketing must be honoured; accepting service terms does not waive that right. Contact the merchant for communications or programme processing it controls.

Your rights and complaints

Depending on the circumstances and legal basis, you may have rights to access your information, correct inaccuracies, request erasure, restrict processing, object to processing and receive or transfer certain information. Where processing relies on consent, you can withdraw it without affecting earlier lawful processing.

Contact contact@loyalfork.com to exercise your rights. You do not need to use a particular form. For merchant-controlled loyalty information, contact that merchant or ask us to help route your request. We may need information to verify your identity and locate the correct records without disclosing someone else's data. We handle requests within the applicable legal time limits, ordinarily within one month of receiving the request where the applicable rules provide that period, and explain any lawful restriction or permitted extension. There is normally no fee; any legally permitted exception must be explained.

You can complain to the UK Information Commissioner's Office at ico.org.uk/make-a-complaint. Where EU data protection law applies, you may also complain to a competent supervisory authority, including in the EU country where you live, work or believe an infringement occurred. In Spain, you can contact the Agencia Española de Protección de Datos (AEPD).

You may contact us first so we can try to resolve your concern. For requests about your rights, the AEPD explains when you should first contact the controller before making a complaint.

Children

Programme membership is intended for customers aged 18 or over. We do not knowingly offer membership to children. The current enrolment forms collect a birth date but do not automatically enforce the 18+ threshold or verify identity or age. Merchants must check eligibility before enrolling

customers and contact us about ineligible memberships. Contact us or the relevant merchant if you believe a child has enrolled so that we can investigate and take appropriate action.

Planned birthday offers

Automatic birthday offers and birthday emails are not currently enabled. Before introducing them, we will update the relevant privacy information to describe birthday-based eligibility and communications, and require merchants to explain their offer rules and lawful use of birth-date information. Collection of a birth date or acceptance of platform terms does not constitute consent to promotional birthday emails.

Changes to this policy

We will update this policy when our practices change and show the effective date. Where required, we will bring important changes to your attention before new processing begins.