SPRING TECHNOLOGIES FZCO

CURD Privacy Policy

Version 9

Field	Value
Date	13 October 2026
Applies to	Registered users, business users, guests, and people identified at a merchant counter
Referenced	At sign-up and at guest checkout. Granular consents are given in the app
Companion documents	Terms of Use, CURD Merchant Agreement

1. Who we are and what this policy covers

1.1 CURD is operated by Spring Technologies FZCO, a free zone company incorporated in Dubai, United Arab Emirates. In this policy, "CURD", "we" and "us" mean Spring Technologies FZCO. We are the controller of the personal data described here.

1.2 This policy explains what personal data we collect, why we collect it, who we share it with, how long we keep it and what rights you have.

1.3 We process personal data in accordance with UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data and its implementing regulations, and with other laws that apply to us.

1.4 This policy forms part of your agreement with us alongside the CURD Terms of Use. If you use CURD as a business, the CURD Merchant Agreement also applies and contains further obligations about data you send us.

2. Who this policy applies to

2.1 It applies to four groups of people, and not everything in it applies to everyone:

You are	What applies
A registered user	All of it
A business user or administrator	All of it, plus section 9 on data you send us about your own customers
A guest — you scanned a table code and paid without an account	Sections 3, 8, 11, 12, 15 and 16 in particular. Section 8 is written for you
Someone identified at a shop counter	You may not have a CURD account. Section 9.3 explains what happens when a business gives us your mobile number

3. What we collect

3.1 Information you give us

- Your mobile number, which is required to open an account and which we verify by one-time code.
- Your name, email address, profile photo, date of birth where you provide it, interests and preferences.
- Your delivery and billing addresses.
- Content you post — reviews, ratings, photos, posts, comments and messages.
- Information you give us when you contact support, including the content of your message.
- For businesses: trade licence, ownership and control information, identification documents for authorised signatories, bank and payout details, and branch information.

3.2 Information we collect automatically

- Device information — device model, operating system, app version, language, time zone and a device identifier.
- Log information — IP address, dates and times of access, pages and screens viewed, and actions taken.
- Location, where you permit it, and approximate location derived from your IP address.
- QR scan events, including which table or profile code was scanned and when.
- Table session identifiers, which link the people ordering at one table to one bill.
- Cookies and similar technologies, described in section 12.

3.3 Information about your transactions

- What you ordered or booked, from which business and which branch, the amount, the date and the rail used.
- Tips you leave, and which items you selected when splitting a bill.
- Loyalty points and CURD Coins earned, held on hold, unlocked, applied and cancelled.
- Refunds, cancellations, disputes and chargebacks.
- Payment metadata — the last four digits of a card, its type, the issuing country and a payment token. See section 5.

3.4 Information from other sources

- From merchants, where a business logs a purchase you made in store, or sends us your details through its own systems.
- From a merchant's point-of-sale system, where it is connected to CURD. See section 9.
- From our payment providers, including the outcome of a payment and of any verification they perform.
- From identity and business verification checks carried out when you or your business are onboarded.
- From Google, where business location and profile information is used to build or verify a listing.
- From people who refer you, who give us your contact details in order to send an invitation.

4. Why we use it, and on what basis

4.1 Under UAE data protection law we process personal data with your consent, or where the law permits processing without consent for one of the grounds shown below. Where we rely on your consent you may withdraw it at any time, and section 15 explains how.

What we do	Why	Basis
Create and run your account	So you can use CURD	Necessary to perform our contract with you
Process orders, bookings and payments	So your purchase works and the merchant is paid	Necessary to perform our contract with you
Verify your identity, and verify businesses	To meet our legal obligations and prevent fraud	Legal obligation
Calculate, hold and credit rewards, loyalty points and Coins	So you receive what you have earned	Necessary to perform our contract with you
Identify you at a shop counter from your mobile number	So an in-store purchase can be credited with rewards	Your consent, which you can withdraw — see 9.3
Detect and investigate fraud, abuse and manipulation of rewards	To protect users, merchants and CURD	Our legitimate interests
Recommend businesses, offers and content	To make CURD useful to you	Our legitimate interests. You may object — see section 10
Provide customer support	To resolve your query	Necessary to perform our contract with you
Send you service messages	So you know about payments, orders and expiring rewards	Necessary to perform our contract with you
Send you marketing	To tell you about offers and features	Your consent
Keep tax and accounting records	Because the law requires it	Legal obligation
Determine where a service is used for tax purposes	To apply the correct VAT treatment	Legal obligation
Improve and secure the platform	To keep CURD working and safe	Our legitimate interests
Respond to lawful requests and defend claims	To meet our legal obligations	Legal obligation, and establishment or defence of legal claims

5. Payment and financial information

5.1 We do not collect or store your full card number, expiry date or security code. Those are collected and processed directly by our payment provider, Stripe, under its own security standards.

5.2 What we receive and hold is payment metadata: a payment token, the last four digits of the card, the card type, the issuing country, the amount, the currency, and whether the payment succeeded.

5.3 For businesses we hold connected account identifiers and payout information necessary to settle funds. Bank details for payouts are held by our payment provider.

5.4 The card issuing country and your IP address may also be retained as evidence of where a service was used, which we are required to keep for tax purposes.

6. Rewards, loyalty and CURD Coins

6.1 We keep a record of rewards you earn, rewards held on hold, the action needed to unlock them, whether you confirmed it, and rewards that lapsed unclaimed.

6.2 We keep a record of loyalty points issued to you by a merchant, and of CURD Coins issued to you, applied by you and cancelled.

6.3 Where a reward is earned against a mobile number that does not match a CURD account, we hold it against that number for 30 days so the person can claim it if they register. If they do not, the record is discarded.

6.4 Where a reward depends on you doing something — leaving a review, sharing a post, completing a referral — we record your confirmation that you did it. We do not monitor your social media accounts and we do not check the platform you posted on.

7. Child safety

7.1 CURD is not for people under 18 and we do not knowingly collect personal data from children.

7.2 We have zero tolerance for child sexual abuse and exploitation. Where we identify content or conduct of that kind we remove it, terminate the accounts involved, preserve the relevant records, and report to the competent authorities in the United Arab Emirates and to relevant international bodies. We cooperate fully with law enforcement, and we will disclose personal data where required to do so for this purpose.

7.3 If you believe a child has given us personal data, contact us using the details in section 18 and we will delete it.

8. If you use CURD without an account

8.1 You can scan a code at a table, view the menu, order and pay without registering. This section explains what happens to your information when you do.

8.2 We identify your session by a device identifier rather than by an account. We collect the table code you scanned, what you ordered, what you selected to pay for, any tip, and your payment metadata.

8.3 Everyone who scans the same table code joins the same bill. That means order and payment information for that table is visible to the other people at it. No other information about you is shared with them.

8.4 If you create an account afterwards, we connect that transaction to your new account so you receive any rewards it earned. We match it using the email address or mobile number you register with.

8.5 If you never create an account, we keep the transaction record because the merchant and we are required to keep records of sales, and we discard the session and device information once it is no longer needed.

9. Merchants, their systems and their tills

9.1 Our role and theirs

9.1.1 A merchant is a separate controller of the personal data it holds about its own customers. We are the controller of the personal data we collect through CURD for the purposes described in this policy.

9.1.2 Where a merchant sends us personal data about its customers, the merchant is responsible for having a lawful basis to do so and for giving any notice required. We tell merchants this in the Merchant Agreement.

9.1.3 When you buy from a merchant through CURD, we give the merchant what it needs to fulfil and account for the sale — your name, the order, the delivery address where relevant, and the amounts. We do not give it your full profile or your history with other businesses.

9.1.4 Where a business subscribes to promotional services, we make available to it the content you have created on CURD about that business — your reviews, ratings, posts, comments, photographs and videos relating to it — together with your display name. We do not make available your contact details, your profile, or your activity with any other business. The business may view and analyse that content within CURD, and may not copy or reuse it elsewhere without asking you.

9.2 Connected point-of-sale systems

9.2.1 Many businesses run their own till system. Where one is connected to CURD, information about your purchase passes between that system and ours so the order, the payment and any reward line up.

9.2.2 What passes to the till system is limited to what it needs to record the sale and credit a reward. What comes back to us is the transaction record.

9.2.3 Some integrations are built by the till provider rather than by us. Those providers are bound by our POS Partner API Terms, which limit what they may receive, what they may retain and what they may do with it.

9.3 Being identified at a shop counter

9.3.1 At a counter you can be identified in one of two ways: by giving your mobile number to a member of staff, or by showing your CURD profile code.

9.3.2 If you give your number, the business's system asks us whether that number belongs to a CURD account. We return only an opaque identifier, your first name, and a summary of what rewards you are eligible for.

9.3.3 We do not return your email address, your postal address, your profile, your purchase history with other businesses, or anything else.

9.3.4 This happens because you chose to give your number in order to earn a reward. You can turn it off at any time in your privacy settings, and if you do, in-store purchases will not earn rewards unless you show your profile code instead.

9.3.5 The business must tell you why it is asking for your number. We require this of them, but we cannot give that notice ourselves at a counter we do not control.

9.3.6 Your profile code resolves through a short-lived signed token, not a permanent identifier, so a screenshot of it cannot be reused.

9.3.7 We limit how often and how quickly a business or till provider may look up numbers, and we log every lookup, so that the facility cannot be used to test whether numbers belong to CURD users.

10. Automated processing and machine learning

10.1 We use automated systems, including machine learning models, to recommend businesses and offers, rank search results and content, work out which rewards you are eligible for, and detect fraud and abuse.

10.2 Those models are built and operated by CURD on our own infrastructure. No third party processes your personal data in order to produce them.

10.3 We do not sell your personal data, and we do not share it with any third party for the purpose of training their artificial intelligence models.

10.4 Reward eligibility is determined automatically against published rules. If you believe a decision about a reward is wrong, contact us and a person will review it.

10.5 You can object to profiling for recommendation purposes, and you can influence what you see through your settings. Objecting does not stop us using automated checks that we need for fraud prevention or to meet a legal obligation.

11. Device permissions

11.1 CURD asks for the following permissions. You can refuse any of them, and change your mind later in your device settings. Refusing one only limits the feature that needs it.

Permission	Why we ask
Camera	To scan a table code, a profile code or a QR code. This is how most CURD interactions begin
Photos and media	So you can add photos to a review or a post
Location	To show businesses near you and to help identify the branch you are at
Notifications	To tell you about orders, payments, expiring rewards and security alerts
Contacts	Only if you choose to invite someone. We use the contact you select and do not upload your address book

12. Cookies and similar technologies

12.1 We use cookies and similar technologies on our website and in the scan-to-order web experience.

12.2 Strictly necessary cookies keep your session working, keep your table order attached to your device, and protect against fraud. These cannot be switched off.

12.3 Analytics cookies help us understand how CURD is used. Preference cookies remember your choices. Marketing cookies, where used, help measure campaigns. These require your consent and you can withdraw it.

12.4 The scan-to-order experience uses a session identifier that links your device to a table for the duration of your visit, and expires after a period of inactivity.

13. Who we share it with

13.1 We do not sell your personal data. We share it only as described here.

Who	What for	Category
Merchants you buy from	To fulfil and account for your order and credit rewards	Separate controller
Connected point-of-sale providers	To record the sale and credit a reward at the till	Processor or separate controller, depending on the integration
Stripe	Payment processing and payout	Processor and separate controller for its own compliance
Amazon Web Services	Hosting and infrastructure	Processor
Firebase	App infrastructure, messaging and analytics	Processor
Branch.io	Deep links and attribution	Processor
Zoho Books	Accounting and invoicing	Processor
Google	Business location and profile data; analytics	Separate controller
Meta	Advertising measurement, where you have consented	Separate controller
Professional advisers, auditors and insurers	To run and account for our business	Separate controllers
Authorities, regulators and law enforcement	Where required by law or to protect people from harm	Separate controllers
A buyer or successor	If our business is sold or reorganised	Separate controller

13.2 Where a party acts as our processor, it acts on our instructions under a written agreement and may not use your data for its own purposes.

13.3 We keep this list current. Where we add a processor that materially changes how your data is handled, we update this policy.

14. Where your data is held, and transfers

14.1 Your personal data is stored on infrastructure located in the United Arab Emirates.

14.2 Some of the providers in section 13 operate internationally, so limited categories of data may be processed outside the United Arab Emirates — for example when a payment is authorised, or when support is provided.

14.3 Where data is transferred out of the United Arab Emirates we do so only where the receiving country is recognised as providing an adequate level of protection, or where an appropriate safeguard such as a contract containing approved terms is in place, or where another basis permitted by UAE law applies.

14.4 You can ask us which safeguard applies to a particular transfer using the details in section 18.

15. How long we keep it

15.1 We keep personal data only as long as we need it, and longer where the law requires. Some records must be kept even after you close your account.

What	How long	Why
Account profile data	While your account is open, then 90 days	So you can reopen or recover an account
Transaction and order records	5 years from the end of the tax period	Tax and accounting law
Tax invoices and place-of-use evidence	5 years from the end of the tax period	Tax law
Verification records for businesses	5 years after the relationship ends	Anti-money-laundering law
Reward, loyalty and Coin records	While your account is open; transaction-linked records for 5 years	To run the programme and to meet record-keeping duties
Rewards held against an unregistered number	30 days	So the person can claim on registering

Guest session and device data	90 days, except the transaction record	So the order works and disputes can be resolved
Support correspondence	24 months	To handle follow-up and complaints
Log and device data	12 months	Security and fraud prevention
Marketing consent records	While consent is held, then 2 years	To show that consent was given and withdrawn
Records relating to a dispute or claim	Until resolved, then as long as a claim could be brought	To establish or defend legal claims

15.2 When you ask us to delete your data, we delete your profile and content and stop using your data to personalise CURD. We keep transaction, tax and verification records for the periods above because we are required to, and we restrict their use to those purposes only.

16. Your rights

16.1 You have the right to: be told how your data is used; get a copy of it; have inaccurate data corrected; have data deleted where we have no continuing basis to keep it; restrict how we use it; object to processing based on our legitimate interests, including profiling for recommendations; receive certain data in a portable form; and withdraw consent at any time where we rely on it.

16.2 Withdrawing consent does not affect anything we did before you withdrew it, and does not affect processing we carry out on another basis, such as a legal obligation.

16.3 To exercise a right, use the controls in your account settings, or contact us using the details in section 18. We will ask you to verify your identity.

16.4 We will respond within 30 days. If your request is complex we may extend that, and we will tell you if we do. If we cannot do what you ask, we will explain why.

16.5 We do not charge for this, unless a request is manifestly excessive or repetitive.

16.6 If you are not satisfied with our response you can complain to the UAE Data Office.

17. Security, and changes to this policy

17.1 We protect personal data using encryption in transit and at rest, access controls, one-time code authentication, logging, and regular review. No system is perfectly secure, but we take these obligations seriously.

17.2 We are not in scope for full card data because our payment providers handle card details directly. Integration credentials issued to merchants and till providers are restricted, logged and revocable.

17.3 If a personal data breach occurs that is likely to harm you, we will notify you and the UAE Data Office as required by law.

17.4 We may update this policy. Where a change is material we will tell you before it takes effect. The version and date are shown at the top of this document.

18. Contact us

18.1 Spring Technologies FZCO, IFZA Business Park, Dubai Silicon Oasis, Dubai, United Arab Emirates.

18.2 Data protection enquiries and requests: support@curd.network.

18.3 General enquiries: support@curd.network. Child safety reports: support@curd.network, or the in-app reporting tool.

18.4 You may also complain to the UAE Data Office.