SECTION 1 — DEFINITIONS

1.1 User / You / Your
1.2 VCQRU / We / Our / Technology Platform
1.3 Brand / Brand Partner / Principal Company
1.4 Services
1.5 Portal / Website / App / Interface
1.6 OTP Login / Authentication
1.7 Personal Data
1.8 Financial Data
1.9 KYC Information
1.10 Location Data
1.11 Scan Data / Verification Data
1.12 Reward Data / Loyalty Transaction Data
1.13 Fraud / Misuse
1.14 Consent

SECTION 2 — SCOPE OF THIS POLICY

2.1 Who This Policy Applies To
2.2 Which Services Are Covered
2.3 What Is Not Covered by VCQRU
2.4 Platforms Covered
2.5 Geographic Scope
2.6 Legal Scope

SECTION 3 — CATEGORIES OF DATA COLLECTED

3.1 Personal Identification Information (PII)
3.2 Contact Information
3.3 Address Information
3.4 Government Identification (KYC)
3.5 Financial Information
3.6 Product Scan Data
3.7 Scan Behavior Intelligence
3.8 Location Data
3.9 Device Information
3.10 Network Information
3.11 OTP Authentication Logs
3.12 User Activity Data
3.13 Loyalty Program Data
3.14 Payout History
3.15 Customer Support Data
3.16 Document Upload Data
3.17 Notification Data
3.18 Behavioral Analytics
3.19 Error & Failure Logs
3.20 Automated Fraud Signals

9.3 What VCQRU Is Not Responsible For
9.4 User Responsibilities (Summary)

SECTION 10 — SPECIAL CLAUSES & CONDITIONS

10.1 Multiple Account / Device Fraud
10.2 QR Code Duplication / Sharing
10.3 Location Spoofing / VPN Misuse
10.4 Device/Browser Manipulation
10.5 Fake User Information
10.6 Wrong UPI/Bank Entry
10.7 Wrong Product Scan
10.8 Brand Final Authority
10.9 Fake Product Handling
10.10 Duplicate Reward Attempts
10.11 Taxation Clause
10.12 Refund & Cancellation
10.13 User Misconduct
10.14 Blacklisting
10.15 Scan Result Accuracy
10.16 System Limitations
10.17 Force Majeure

SECTION 11 — USER CONSENT & DECLARATION

11.1 Consent to Data Use
11.2 Consent to Share with Brand
11.3 Consent to Share with Payment Partners
11.4 Consent for KYC
11.5 Consent for Fraud Detection
11.6 Consent for Service Communication
11.7 Acknowledgement of Brand Responsibility
11.8 Consent to Data Retention
11.9 Consent to System Limitations
11.10 Consent to Responsible Behaviour
11.11 OTP as Digital Signature
11.12 Contact for Consent Withdrawal

SECTION 1 — DEFINITIONS

This section clearly defines every important term used in the policy.
This is crucial for legal clarity and to avoid user misinterpretation.

1.1 "User", "You", "Your"

Refers to any individual who:

- Scans a QR/security code on a product
- Verifies product authenticity using VCQRU's system
- Participates in loyalty, cashback, or reward programs
- Enters personal, financial, or KYC information
- Logs into any VCQRU-powered portal, webpage, mobile app, or service
  Users include:
- Consumers
- Channel partners (mechanics, electricians, carpenters, plumbers, painters, retailers, dealers)
- Distributors
- Employees of brand partners
- Any person redeeming benefits offered by brands

1.2 "VCQRU", "We", "Our", "Technology Platform"

VCQRU Private Limited, provider of:

- Anti-counterfeit authentication technology
- Loyalty and cashback processing systems
- QR-code security mechanisms
- Product verification APIs
- KYC and payout orchestration
- Fraud analytics and monitoring tools

VCQRU **does not manufacture, market, distribute, or sell any product**, nor does it approve any financial benefit on its own.
VCQRU is a **technology intermediary** acting on behalf of brands.

1.3 "Brand", "Brand Partner", "Principal Company"

Refers to the company whose:

- Products you purchase
- Products you verify
- Loyalty or reward programs you participate in
- Terms & benefits you follow

All authenticity decisions, benefit approvals, payouts, warranty, refunds, and complaint handling are **solely the responsibility of the Brand**.

1.4 "Service(s)"

Includes all features you use through VCQRU, such as:

A. Anti-Counterfeit (AC) Services

- Scanning QR codes
- Entering security codes
- Viewing authentication results
- Receiving duplicate/fraud warnings
- Receiving product safety alerts

B. Build Loyalty (BL) Services

- Creating user profile
- Earning points
- Redeeming rewards
- Receiving cashback (UPI/NEFT)
- Completing KYC
- Tracking loyalty history

C. Platform & Technical Services

- OTP login
- Scan history
- Notifications
- Payment processing
- Fraud detection
- Customer support

1.5 “Portal”, “Website”, “App”, “Interface”

Any digital channel powered by VCQRU, including:

- Brand-specific portals
- Verification pages
- Mobile websites
- Progressive Web Apps
- Embedded widgets
- WhatsApp/Chatbot authentication flows
- APIs used by brands

Any interaction with these channels is considered an interaction with the Service.

1.6 “OTP Login” / “Authentication”

A security method where the user provides:

- A mobile number
- A one-time password sent via SMS/WhatsApp
  This verifies the user’s identity and links all actions to their account.

OTP is used for:

- Preventing identity fraud

- Preventing misuse of points
- Tracking genuine usage
- Improving verification accuracy
- Blocking automated or bot-driven abuse

1.7 “Personal Data”

Any information that identifies you directly or indirectly, including:

- Name
- Mobile number
- Email
- Address
- Photo
- Device ID
- IP address
- Location
- UPI ID
- Bank details
- KYC documents
- Scan history
- Reward history

This data is collected with user consent and used only for service delivery.

1.8 “Financial Data”

Includes:

- UPI ID
- Bank account number
- IFSC code
- Account holder name
- PAN/Aadhaar (only if needed for regulatory compliance)

This data is used **only** for processing payouts instructed by the brand.

VCQRU never collects:
❌ ATM PIN
❌ CVV
❌ Passwords
❌ Net banking credentials

1.9 “KYC Information”

Documents and details required by brands for user verification or compliance, such as:

- PAN
- Aadhaar

- Voter ID
- Driving License
- GST (for dealers/distributors)
- Any photo identity required by the brand

Collected only when mandated by the brand or by law.

1.10 “Location Data”

Geo-information captured during scanning or reward activity for:

- Fraud detection
- Preventing region misuse
- Counterfeit analysis
- Supply-chain leakage detection
- Complying with scheme/market restrictions

Collected only with permission.

1.11 “Scan Data” / “Verification Data”

Includes:

- Security code
- QR value
- Product batch
- First scan time & location
- Number of scans
- Device used
- Result (Genuine/Invalid/Duplicate/Suspicious)

This data is essential for detecting counterfeit patterns.

1.12 “Reward Data” / “Loyalty Transaction Data”

Includes:

- Points earned
- Cashback requests
- Redemption history
- UPI/NEFT payout logs
- Failed or suspicious transactions
- Scheme eligibility status
- Audit logs

Used to process benefits accurately and securely.

1.13 “Fraud” / “Misuse”

Covers all actions such as:

- Scanning the same code multiple times intentionally
- Using fake or tampered QR codes
- Using VPN or location spoofing
- Creating multiple accounts for extra benefits
- Entering incorrect UPI or bank details repeatedly
- Using someone else's documents for KYC
- Trying to hack or bypass systems
- Manipulating device/browser scripts

Brands may initiate action against fraud.

1.14 "Consent"

Means you voluntarily:

- Accept the policy
- Share your information
- Agree to usage of data for legitimate needs
- Permit VCQRU and brands to process your information for the defined purposes
- Understand the brand owns authenticity & rewards decisions

Consent is given when you:

- Enter OTP
- Login
- Scan a product
- Submit your details
- Proceed to use any feature of the service

SECTION 2 — SCOPE OF THIS POLICY (EXTREMELY DETAILED)

2.1 Who This Policy Applies To

This policy applies to ALL users regardless of:

- Region
- Language
- Type of brand
- Type of product
- Type of reward
- Whether accessed through mobile, web, or app

If a user interacts with a brand using VCQRU's platform, this policy applies.

2.2 Which Services Are Covered

This policy governs:

1. QR code scanning
2. Product authenticity verification
3. Duplicate scan alerts
4. Reward/point/cashback systems
5. Loyalty portals
6. UPI/NEFT payouts
7. KYC validation
8. Customer identity verification
9. Support interactions
10. Data submission
11. Storage & processing
12. Security measures
13. Fraud detection
14. Backend systems used by brands
15. In-app or web-based incentives

2.3 What Is Not Covered by VCQRU

VCQRU does **NOT** handle:

- Product quality
- Expiry date accuracy
- Refund of fake or damaged goods
- Warranty or service claims
- Brand-specific redemption rules
- Commercial offers from sellers
- Brand-generated marketing content

These are controlled **exclusively by the brand**.

2.4 Platforms Covered Under This Policy

This applies to:

- VCQRU
- Brand portals powered by VCQRU
- Verification pages on any brand website
- Mobile web pages
- Progressive Web Apps
- Brand apps using VCQRU APIs
- WhatsApp or chatbot flows using VCQRU backend

Users will encounter this policy anywhere VCQRU technology is used.

2.5 Geographic Scope

This policy applies across:

- All Indian states and union territories
- International markets where brand uses VCQRU solutions

- Any region where the product is sold and authenticated
- All regions where loyalty benefits are offered

User location does not reduce policy applicability.

2.6 Legal Scope

This policy aligns with:

- India's DPDP Act
- IT Act 2000 & IT Rules 2021
- RBI & NPCI guidelines (for payouts)
- Industry-specific regulations (for pharma, FMCG)
- Brand-specific compliance requirements

SECTION 3 — CATEGORIES OF DATA COLLECTED

3.1 PERSONAL IDENTIFICATION INFORMATION (PII)

This includes:

- Full Name
- Mobile Number
- Email Address
- Gender
- Date of Birth
- User Photo (if required)

Why we collect this:

- To verify your identity
- To create a unique profile for reward or security purposes
- To ensure only genuine users participate in brand schemes
- To avoid impersonation and prevent fraud
- To allow brands to contact you in legitimate product safety cases

How it helps:

- Prevents fraudulent claims
- Ensures reward payouts go to the correct person
- Enables accurate support resolution

3.2 CONTACT INFORMATION

- Mobile number
- WhatsApp-enabled number
- Alternate contact (if provided)

Purpose:

- OTP login
- SMS or WhatsApp delivery of verification results
- Support follow-ups
- Counterfeit product safety warnings

Why it is important:

Without a verified mobile number, VCQRU cannot provide safe authentication, tracking, or rewards.

3.3 ADDRESS INFORMATION (BL only when needed)

- Street address
- City, State
- Pincode

Purpose:

- Delivery of physical gifts or rewards
- Region-based scheme eligibility
- Compliance for some industries (pharma, agro, automotive)

3.4 GOVERNMENT IDENTIFICATION (KYC documents — when required by brand)

Includes:

- PAN
- Aadhaar
- Driving License
- Voter ID
- Business GST (for dealers)

Purpose:

- For payouts above certain limits
- To comply with brand rules
- To avoid fraudulent or duplicate identities
- To satisfy legal & tax compliance (e.g., Section 194R)

VCQRU DOES NOT:

- Collect KYC unless the brand mandates it
- Store raw Aadhaar numbers without encryption
- Use KYC for marketing

3.5 FINANCIAL INFORMATION (FOR PAYOUTS ONLY)

Includes:

- UPI ID
- Bank Account Number
- IFSC Code
- Beneficiary Name

Why collected:

- To process cashback and NEFT rewards
- Validate payment with correct beneficiary
- Prevent payout fraud

Security:

- Stored in encrypted form
- Shared ONLY with banks/NPCI-approved payment partners
- Never used for auto-debit

What VCQRU NEVER collects:

❌ ATM PIN
❌ CVV
❌ Password
❌ Net Banking Login

3.6 PRODUCT SCAN DATA (AC)

Includes:

- Secret security code
- QR code value
- Product batch number
- Manufacturing data (if coded in QR)
- First scan record
- Scan sequence
- Scan pattern
- Associated brand

Purpose:

- To check whether product is genuine
- Detect duplicate or counterfeit products
- Identify market-level counterfeit clusters
- Help brands take action

Why essential:

Without this, anti-counterfeit verification cannot work.

3.7 SCAN BEHAVIOR INTELLIGENCE (Critical for AC)

Includes:

- Frequency of scans
- Device used for scan
- Time gap between scans
- Geographic spread of scan attempts
- Repeated scan attempts per code

Purpose:

- Detect fake codes
- Stop illegal duplication
- Prevent code sharing
- Catch counterfeiters copying labels

Examples of fraud detected:

- Same code scanned in 3 cities within minutes
- Code scanned 50 times in 1 day
- Code scanned from multiple devices

3.8 LOCATION DATA

Captured **only with permission**.

Includes:

- Approximate location (city-level)
- Precise location (GPS-level) — if allowed
- Region-based scan patterns
- Location of first scan
- Location of repeated scans

Purpose:

- Detect counterfeit distribution
- Identify mismatch between product region vs scan region
- Prevent misuse of region-restricted loyalty schemes
- Support brand recall or consumer safety alerts

3.9 DEVICE INFORMATION (Advanced Technical Layer)

Includes:

- Device model (e.g., Samsung A52)
- Operating system version
- Browser version
- Device fingerprint ID
- Screen resolution
- App version (if using app)
- Unique device signature

Purpose:

- Fraud detection
- Improve scanning accuracy
- Detect bots or automated systems
- Prevent multiple fake accounts from one device

3.10 NETWORK INFORMATION

Includes:

- IP address
- Network type (4G/5G/WiFi)
- Carrier name
- VPN detection

Purpose:

- Prevent location spoofing
- Detect fake claims
- Support investigation for counterfeit patterns

3.11 OTP AUTHENTICATION LOGS

Includes:

- Mobile number used
- Time of OTP request
- Number of attempts
- OTP verification logs
- Failed OTP attempts

Purpose:

- User identification
- Prevent brute-force misuse
- Detect account takeover attempts

3.12 USER ACTIVITY DATA

Includes:

- Login time
- Logout time
- Session duration
- Page navigation
- Actions taken in portal

Purpose:

- Improve user experience
- Detect abnormal patterns
- Support KYC & payout decisions

3.13 LOYALTY PROGRAM DATA (BL)

Includes:

- Points issued
- Points used
- Points pending approval
- Scheme rules applicable
- Eligibility status
- Transaction ledger
- Failed redemption attempts

Purpose:

- Maintain transparency
- Enable audit for brands
- Support dispute resolution

3.14 PAYOUT HISTORY (BL)

Includes:

- Cashback amount
- Payout transaction ID
- Payment mode
- Payment status
- Failed payout reasons
- Retry attempts

Purpose:

- Audit
- User support
- Fraud detection

3.15 CUSTOMER SUPPORT DATA

Includes:

- Photos of product
- Photos of packaging
- Photos of QR/Code
- User explanations
- Complaint history

Purpose:

- Resolve complaints
- Verify counterfeit claims
- Support brands in investigations

3.16 DOCUMENT UPLOAD DATA (BL/Support)

Includes:

- Photo ID
- Address proof
- Photo of product
- Invoice (if requested by brand)

3.17 NOTIFICATION DATA

Includes:

- Messages sent to user
- Delivery status
- Read/open rate (if applicable)

3.18 BEHAVIORAL ANALYTICS (System Improvement)

Includes:

- Time taken to scan
- Time between actions
- Drop-offs
- Error tendencies

Used ONLY for improving system performance.

3.19 ERROR & FAILURE LOGS

Includes:

- System crash logs
- QR read errors
- Browser errors
- Failed verifications

Used to improve platform quality.

3.20 AUTOMATED FRAUD SIGNALS

Includes:

- Duplicate identity matches
- Device correlation
- Multi-account mapping
- Suspicious geographical patterns
- Attack signals (bot detection)

Used ONLY for fraud prevention.

3.21 BRAND-INSTRUCTED FIELDS

Brands may ask for:

- Dealer ID
- Mechanic ID
- Shop name
- Route code
- Sales territory
- Vehicle number (auto rewards)

VCQRU collects them on brand's behalf.

3.22 COOKIES & TECHNICAL STORAGE

Used for:

- Maintaining session
- Improving performance
- Storing login state (optional)

We do NOT use cookies for advertising.

3.23 VOLUNTARY DATA

Any additional information voluntarily shared by the user.

3.24 ANONYMIZED DATA

Used only for analytics without identifiable information.

3.25 DATA NOT COLLECTED

The following data is **NEVER collected**:

❌ ATM PIN
❌ CVV
❌ Credit card details
❌ Banking passwords
❌ Personal photos unrelated to verification
❌ Contacts
❌ Microphone
❌ Stored files
❌ SMS inbox
❌ Social media accounts

SECTION 4 — HOW WE USE YOUR DATA

Below is a **full, legal-grade explanation**.

4.1 Anti-Counterfeit (AC) Verification

1. To verify product authenticity in real time

Your scan data is compared with encrypted brand records to confirm if the product is *genuine, invalid, duplicate, reused, or suspicious*.
This protects YOU from counterfeit products.

2. To detect duplicate, copied, or reused codes

If the same QR/security code is scanned in multiple cities, devices, or times quickly — the system flags it.
This helps brands identify fake product circulation.

3. To track first scan and scan history behavior

VCQRU records:

- First scan
- Second scan
- Location patterns
- Device signatures

This enables precise counterfeit detection.

4. To analyze the location of scans for counterfeit clusters

We use region patterns to find fake markets, such as:

- Multiple fake scans from one city
- Repeated duplicates in one retail area
- Industry-level duplication patterns

Brands rely on this for supply-chain investigations.

5. To compare printed product data with digital data

Mismatch analysis includes:

- Batch number differences
- MRP mismatch
- Expiry mismatch
- Manufacturing unit mismatch

Any mismatch produces a high-risk alert.

6. To provide real-time user warnings

If the product is counterfeit or suspicious, the system immediately shows warnings like:

- “Duplicate Scan”
- “Invalid Code”
- “Fake Product Suspected”

This protects consumer safety.

7. To enable brand recall decisions

If faulty batches or counterfeit items are identified, brands may take action.

8. To prevent sellers from misusing genuine codes

Scan behavior patterns identify sellers reusing genuine stickers.

9. To ensure each scan is authentic and not tampered

We verify:

- Browser integrity
- URL integrity
- QR link security
- Device integrity

This stops fake QR redirection.

10. To help brands perform supply chain analysis

Scan analytics show:

- Where fakes appear
- Which distributors might be leaking stock
- Region where more duplicates exist

11. To maintain product safety standards

Scan data helps brands decide:

- Which regions require awareness campaigns
- Where safety alerts are needed

12. To maintain historical verification logs

For audit, product tracing, and compliance.

4.2 Loyalty / Reward / Cashback Services (BL)

13. To create and maintain your reward account

We use your identity (name, mobile number) to create a secure loyalty profile.

14. To credit points after successful scans

Each verified scan triggers brand rules:

- Instant points
- Tiered benefits
- Slab-based rewards

15. To process cashback through UPI/NEFT

We use your UPI ID or bank details to route your payments via NPCI or banking partners.

16. To validate your KYC for high-value payouts

Some brands require KYC under government regulation.
We only process after brand approval.

17. To prevent duplicate claims

System checks if:

- Code already claimed
- User created multiple accounts
- Same UPI used for many accounts

18. To execute brand-specific scheme logic

Each brand has:

- Different reward rules
- Different point structures
- Different eligibility criteria
  We implement those safely.

19. To maintain a detailed reward ledger

Every earned & redeemed point is documented for transparency.

20. To provide reward notifications

We notify users about:

- Cashback status
- Reward credits
- Scheme eligibility
- Redemption success/failure

21. To resolve disputes with complete audit logs

Brands use this to verify:

- Why a reward was not given
- Why a scan was invalid
- Why cashback failed

22. To maintain scheme integrity

Stops channel partners from misusing schemes by scanning:

- Wrong products
- Old stock
- Fake labels

23. To comply with tax requirements (e.g., 194R)

PAN may be needed for TDS deduction on high-value rewards.

4.3 Identity & Account Security — 5 Use Cases

24. To authenticate the user with OTP

Ensures the account belongs to the correct person.

25. To detect unauthorized login attempts

Tracks suspicious patterns:

- Too many OTP attempts
- Multiple device changes
- Session hijacking

26. To link all actions to a single, verified identity

Prevents:

- Account duplication
- Fake UPI usage
- False reward claims

27. To secure user sessions

Maintains secure login tokens and session integrity.

28. To ensure compliance with legal and brand rules

Identity verification is needed for fairness and compliance.

4.4 Financial & Payout Processing — 5 Use Cases

29. To process UPI payouts

Your UPI ID is validated and used strictly for payout.

30. To process NEFT payouts

Used when brand rules require bank transfer.

31. To ensure money goes to the correct person

We verify:

- Beneficiary name
- Bank account mapping
- Scheme eligibility

32. To maintain complete transaction audit logs

Required for legal & financial compliance.

33. To handle payout failures & retries

If payout fails:

- System logs the reason
- Auto-retries

- Notifies user and brand

4.5 Fraud Detection & Prevention — 9 Use Cases

34. To detect duplicate scans

When the same code is used multiple times.

35. To detect geographic anomalies

e.g., code scanned in Delhi and Chennai within minutes.

36. To detect device misuse

VCQRU maps device signatures to stop multiple fake accounts.

37. To detect VPN or GPS spoofing

Prevents reward misuse.

38. To detect brute-force attempts

Multiple invalid codes from same device.

39. To detect multi-account fraud

Same UPI used across many accounts.

40. To block suspicious codes automatically

Counters mass duplication attacks.

41. To notify brand about counterfeit risks

So they can protect consumers.

42. To ensure loyalty scheme fairness

Fraud reduces genuine user benefits—VCQRU prevents this.

4.6 System Improvement & Analytics — 5 Use Cases

43. To improve verification accuracy

Data helps refine:

- AI-based scan patterns
- Counterfeit detection algorithms

44. To improve system performance

Logs help detect:

- Slow networks
- High-traffic issues

45. To improve user experience

User behavior helps identify:

- Confusing steps
- Error-prone fields

46. To identify technical issues

Crash logs help fix platform bugs.

47. To generate brand-level analytics

Used by brands to understand:

- Region performance
- Product authenticity trends
- User engagement

All analytics are **anonymous**.

4.7 Brand Compliance & Legal Requirements — 4 Use Cases

48. To comply with government KYC rules

For channel partners in cashback-based schemes.

49. To comply with taxation rules (Section 194R)

If reward value exceeds regulatory thresholds.

50. To comply with anti-counterfeit laws

Brand needs verification logs for enforcement.

51. To comply with legal investigations

In case of counterfeit markets or fraud cases.

4.8 Customer Support & Escalation

52. To resolve user complaints

Support teams use data to:

- Check scan history
- Validate points
- Investigate payout failures

53. To verify counterfeit product reports

User-submitted photos + scan data help investigations.

54. To provide region-specific support

Helps brands identify local issues.

55. To maintain a complete support history

Enables faster resolution of repeat issues.

SECTION 5 — DATA PROTECTION & SECURITY MEASURES

Below are **extremely detailed, enterprise-level** explanations for each protection mechanism.

5.1 Encryption of All Sensitive Data (AES-256 + TLS 1.2/1.3)

What we encrypt:

- UPI IDs
- Bank details
- KYC information
- Personal identification data
- Scan logs
- Authentication results
- Reward history

Encryption Standards:

- **Data at Rest:** AES-256 encryption
- **Data in Transit:** HTTPS + TLS 1.2/1.3
- **Database Encryption:** Field-level + table-level encryption
- **Hashing:** One-way hashing for sensitive fields (SHA-256/512)

Why this matters:

Even if someone gets unauthorized access, the data is **unreadable and unusable**.

5.2 Role-Based Access Control (RBAC)

Only authorized personnel with defined roles can access limited parts of the system.

Types of Access:

- System Admin
- Product Access
- Database Reader
- Reward Finance
- Brand-specific Access
- API Integration Teams

Rules:

- No single employee has complete access
- All access is logged
- Temporary access auto-expires
- Brand data is strictly siloed

5.3 Zero-Trust Architecture Principles

We apply “Never Trust, Always Verify” security model:

- Every request is authenticated
- Every device is verified
- No internal system is trusted by default
- Continuous authentication

5.4 Firewall, WAF & DDoS Protection

VCQRU uses:

- **Web Application Firewall (WAF)** against attacks (SQL injection, XSS, CSRF)
- **Layer 7 protections**
- **DDoS mitigation**
- **Intrusion detection systems (IDS)**
- **Intrusion prevention systems (IPS)**

All incoming traffic is filtered for threats.

5.5 Secure Cloud Infrastructure (ISO 27001-certified)

Our servers and databases are hosted only on:

✔️ ISO-27001 certified
✔️ SOC-2 compliant
✔️ PCI-DSS aligned (for payment intermediaries)

cloud providers such as AWS / Azure / GCP.

Benefits:

- Global-grade physical security
- 24/7 monitoring
- Automated failovers
- Redundant backups

5.6 Data Minimization (Collect Only What Is Needed)

VCQRU strictly collects:

- ONLY the data required to provide AC or BL service.
- No unnecessary or excessive personal data.

This reduces risk and enhances privacy.

5.7 Strict Data Segregation (Brand-Wise Separation)

Every brand has **isolated databases or logically separated tables**, ensuring:

- No crossover between brands
- No shared access
- No accidental mixing of loyalty data
- No brand visibility into another brand's user base

This protects confidentiality and prevents legal conflicts.

5.8 Access Logging & Audit Trails

Every system access is logged including:

- Who accessed
- When accessed
- What they viewed
- What changes they made

Audit logs are:

- Tamper-proof
- Stored securely
- Regularly reviewed

5.9 Secure Coding Practices (OWASP Top 10)

VCQRU follows OWASP guidelines to prevent:

- SQL Injection
- Broken Authentication
- Sensitive Data Exposure
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Server-Side Request Forgery (SSRF)

We conduct:

- Code reviews
- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)

5.10 Regular Vulnerability Scanning & Penetration Testing (VAPT)

Professional security audits include:

- Black-box testing
- White-box testing
- API penetration testing
- QR-code tampering simulations
- Fraud pattern stress testing

Performed quarterly or as required by brands.

5.11 Data Backup & Disaster Recovery (DR Policy)

VCQRU maintains:

- Daily incremental backups
- Weekly full backups
- Multi-region replication
- Disaster Recovery site
- 99.5%+ uptime

Backups are:

- Encrypted
- Version-controlled
- Automatically verified

5.12 NPCI & RBI-Compliant Payout Processing

For BL payouts:

- UPI validation
- NEFT/RBI compliance
- Payout encryption
- Audit-ready reconciliation

- No storage of banking passwords
- No auto-debit capability

Financial data is treated with **banking-grade security**.

5.13 Secure Session Management

Ensures:

- OTP tokens expire automatically
- Login sessions time out
- No one can hijack sessions
- Browser/device integrity checks

Mitigates unauthorized access.

5.14 Fraud & Abuse Detection Engine

We continuously monitor:

- Device fingerprinting
- Geo-anomalies
- Repeated code scans
- Duplicate UPI usage
- Location spoofing
- High-frequency suspicious behavior

This protects both user and brand rewards.

5.15 Data Masking for Sensitive Info

Sensitive data like:

- UPI
- PAN
- Bank account

is masked when displayed:

Example:
`test@upi → t***@upi`
`1234567890 → 1234****90`

5.16 Regular Compliance & Security Audits

VCQRU participates in:

- Third-party audits

- Brand security reviews
- Annual legal compliance checks

5.17 Controlled Third-Party Access

We DO NOT share user data with advertisers or external companies.

Data is only shared with:

- Brands you interact with
- NPCI/banking partners for payout
- Government authorities (legal mandate only)

All access is governed by:

- NDAs
- Data Processing Agreements
- Restricted and audited access

5.18 No Selling or Monetising User Data

VCQRU does not:

❌ Sell data
❌ Share with marketers
❌ Use for ads
❌ Build consumer profiles

Data is used **only** for service improvement & security.

5.19 Incident Detection & Response

If unusual or risky behavior is detected:

- Incident is logged
- Security team notified
- Immediate containment
- Root-cause analysis
- Fix deployed
- Brand notified (if needed)

5.20 Data Retention & Deletion Security

We store data only as long as:

- Brand requires
- Policy requires

- Law requires

Deletion logs are maintained, and KYC/financial data is securely purged after expiry.

SECTION 6 — DATA SHARING & DISCLOSURE (EXTREMELY DETAILED)

VCQRU follows a **strict, limited, purpose-only, minimum-necessary** data sharing policy.
Your data is NEVER sold, rented, traded, or exploited.

We ONLY share your data with entities that are essential for delivery of AC or BL services.

6.1 SHARING WITH BRAND PARTNERS (PRIMARY PURPOSE)

Brands are the manufacturers/owners of the product you scanned or the loyalty scheme you participate in.

✔️ **What data is shared with brands:**

- Scan data
- Authenticity results
- Duplicate or suspicious scan alerts
- User identity fields (mobile number, name, region)*
- Points/cashback eligibility
- Reward redemption logs
- KYC status (if applicable)
- Payout success/failure reports
- Fraud alerts detected by VCQRU

(*Address/email/photo only if BRAND requires for their program.)

✔️ **Why brands need this data:**

- To verify product authenticity
- To detect counterfeit activity
- To maintain audit logs for regulators
- To contact users in counterfeit/safety issues
- To approve or reject loyalty/cashback rewards
- To comply with taxation & KYC laws
- To investigate misuse or fraud

✔️ **What brands CANNOT do:**

❌ Cannot sell your data
❌ Cannot use it for unrelated marketing without consent

❌ Cannot share it with unauthorized third parties
❌ Cannot alter any data without leaving audit trails

VCQRU makes sure brands follow strict agreements.

6.2 SHARING WITH PAYMENT PROCESSORS (UPI/NEFT PURSUANT TO NPCI/RBI)

Cashbacks or rewards require payouts.

✔️ **With whom we share:**

- NPCI-authorized UPI payout partners
- RBI-regulated banks for NEFT transfers
- TDS processing systems (if required under 194R)

✔️ **What data is shared:**

- UPI ID
- Bank account number
- IFSC
- Beneficiary name
- Amount to be transferred
- Transaction ID
- Payout status

✔️ **Why:**

- To credit cashback
- To retry failed payouts
- To comply with government tax rules
- To maintain finance audit trails

✔️ **What they CANNOT access:**

❌ Your scan history
❌ Product data
❌ Loyalty points
❌ Personal files or photos
❌ KYC documents unless mandatory for banking law

These partners are legally bound under RBI/NPCI security standards.

6.3 SHARING WITH GOVERNMENT OR LAW ENFORCEMENT (ONLY WHEN REQUIRED)

VCQRU may share data ONLY under:

- Written legal request
- Court order
- Official law enforcement investigation
- Anti-counterfeit enforcement action
- Safety/citizen protection requirement

✔️ **What may be shared:**

- Scan data
- Counterfeit alerts
- Fraud indicators
- Transaction logs
- KYC data (ONLY IF law demands)

✔️ **When this happens:**

- Counterfeit scandal or illegal seller complaints
- Fraud cases with serious economic impact
- Regulatory audit
- Customs, FSSAI, Drug authorities checking for fake products
- Brand escalation to government agency

VCQRU NEVER voluntarily shares data with government bodies — ONLY under legal compulsion.

6.4 SHARING WITH VCQRU-INTERNAL SYSTEMS & SERVICE PROVIDERS

✔️ **Includes:**

- Cloud hosting (AWS, Azure, GCP)
- SMS/WhatsApp OTP service providers
- Email delivery providers
- Internal analytics systems

✔️ **What data they receive:**

- ONLY the minimum necessary operational data
- OTP delivery: mobile number
- Hosting: encrypted databases
- Email providers: email address (if brand uses email communication)

✔️ **Why it's necessary:**

- To deliver OTP
- To host your data securely

- To ensure system uptime
- To provide reliable notifications

✔️ **What they CANNOT do:**

❌ Cannot use your data for ads
❌ Cannot share with others
❌ Cannot access unencrypted personal data

These providers are under NDA + strict data protection agreements.

6.5 SHARING WITH FRAUD ANALYTICS OR SECURITY PARTNERS (IF USED)

Some brands require deeper fraud analysis.

✔️ **What may be shared:**

- Device ID hash
- Suspicious scan markers
- Fraud flags
- Payout misuse flags
- Duplicate KYC matches

✔️ **Why:**

- To catch organized counterfeiters
- To prevent repeated abuse of reward schemes
- To ensure user safety

✔️ **Restrictions:**

These partners DO NOT get:
❌ UPI
❌ Bank details
❌ Full KYC
❌ Private images
❌ User address

Only risk signals — not identifiable personal data — are shared.

6.6 SHARING WITH AUDITORS (BRAND OR LEGAL AUDIT)

✔️ **What they may access:**

- Encrypted logs
- Transaction history
- Scan records
- KYC approval logs
- Payout audit trails

✔️ **Why:**

- To comply with law
- To verify no manipulation or fraud
- To protect user rights
- To maintain trust for brands

Auditors do NOT get personal-level data unless legally necessary.

6.7 SHARING WITH YOU (THE USER)

You can request your own:

- Scan history
- Reward ledger
- Payout reports
- KYC status
- Account information

VCQRU supports full transparency with identity verification.

6.8 WHAT WE NEVER SHARE

VCQRU NEVER shares any of the following with ANYONE:

❌ ATM PIN
❌ CVV
❌ Card number
❌ Banking passwords
❌ UPI PIN
❌ Your contacts
❌ Your SMS inbox
❌ Your photos or gallery
❌ Your social media data
❌ Data with advertisers
❌ Data with unrelated brands

We do NOT monetize or trade data. Period.

6.9 DATA SHARING PRINCIPLES (Strict Legal Rules)

VCQRU follows these rules:

✔️ **Purpose Limitation**

Data shared ONLY for the specific service.

✔️ **Data Minimization**

Only minimum required fields are shared.

✔️ **Legal Compliance**

Sharing only as per DPDP Act, IT Rules, RBI/NPCI guidelines.

✔️ **Auditability**

Every sharing event is logged.

✔️ **NDA Binding**

Partners are under strict confidentiality.

SECTION 7 — USER RIGHTS

Users have full rights regarding their personal information, as described below.
Every right includes:

✔️ *What the right means*
✔️ *Why the right exists*
✔️ *How to exercise it*
✔️ *Limitations (legal or brand-specific)*
✔️ *How VCQRU protects the user*

7.1 RIGHT TO BE INFORMED

✔️ **What it means:**

You have the right to know **what data is collected**, **why it is collected**, **how it is used**, and **who it is shared with**.

✔️ **What VCQRU provides:**

- Transparent privacy policy
- Clear explanations on verification screens
- Details before OTP login
- Brand-specific disclaimers (if any)

✔️ **Why important:**

Ensures users are aware of the purpose and safety of their data.

7.2 RIGHT TO CONSENT & WITHDRAWAL OF CONSENT

✔️ **What it means:**

You choose whether to share personal data, and you may choose to withdraw that consent at any time.

✔️ **How VCQRU enables it:**

- Consent is taken before login
- Location permission is optional
- KYC is only requested when required
- You may stop using services anytime

✔️ **Limitations:**

Withdrawing consent may prevent access to:

- Anti-counterfeit results
- Loyalty points
- Cashback payout
- Verification history

7.3 RIGHT TO ACCESS YOUR PERSONAL DATA

✔️ **What it means:**

You can request a copy of all your data stored with VCQRU.

✔️ **Includes:**

- Personal profile details
- Scan history
- Reward history

- KYC status
- Payout logs

✔️ **How to request:**

You may contact VCQRU support or brand support.

✔️ **Purpose:**

Enables user transparency and trust.

7.4 RIGHT TO CORRECTION / RECTIFICATION

✔️ **What it means:**

You can request correction of incorrect or outdated information.

✔️ **Examples:**

- Wrong name
- Wrong mobile number
- Incorrect UPI ID
- Wrong bank details
- Typo in address

✔️ **Important:**

Corrections improve payout accuracy and prevent fraud.

✔️ **Limitations:**

Some data (like scan logs) cannot be altered as they are audit-protected.

7.5 RIGHT TO DELETION (RIGHT TO BE FORGOTTEN)

✔️ **What it means:**

You may request deletion of your data.

✔️ **What can be deleted:**

- Profile details
- Address
- Email

- Contact number (after account removal)
- Voluntary uploaded documents

✔️ **What CANNOT be deleted immediately:**

- Scan history (needed for anti-counterfeit audit)
- Reward transaction history (mandatory for brand audit)
- Government/KYC data (must follow legal retention period)
- Fraud investigation records

✔️ **Why limitations exist:**

To comply with brand policies and regulatory laws.

7.6 RIGHT TO DATA PORTABILITY

✔️ **What it means:**

You may request your data in a readable format (CSV/JSON/PDF) for transferring or reviewing.

✔️ **VCQRU provides:**

- Scan history
- Reward statements
- Payout ledger
- KYC status

✔️ **Benefit:**

Full transparency for the user.

7.7 RIGHT TO RESTRICT PROCESSING

✔️ **What it means:**

You can request that VCQRU stop using certain parts of your data.

✔️ **Example:**

- Stop using your address
- Stop using your email
- Disable notifications

✔️ **Limitations:**

Restricting some data may disable certain services (e.g., UPI payouts).

7.8 RIGHT TO OBJECT

✔️ **What it means:**

You may object to data processing if you believe it's unnecessary.

✔️ **Example:**

You may request that VCQRU stops processing your usage analytics.

✔️ **Limitations:**

VCQRU must still follow legal and brand obligations.

7.9 RIGHT AGAINST AUTOMATED DECISION-MAKING

✔️ **What it means:**

You have the right not to be judged by purely automated logic in cases involving risk or rejection.

✔️ **VCQRU ensures:**

- Human review is available for disputes
- Payout rejections are rechecked manually
- KYC failures are manually audited

7.10 RIGHT TO SAFE & FAIR PROCESSING

✔️ **What it means:**

Your data must be processed in:

- A safe manner
- A fair manner
- A non-discriminatory manner

✔️ **How VCQRU ensures fairness:**

- Same rules for all users

- Automated fraud checks apply equally to everyone
- Brands cannot reject legitimate rewards unfairly

7.11 RIGHT TO KNOW WHEN YOUR DATA WAS SHARED

You can request details on:

- Which entities accessed your data
- When the data was shared
- For what purpose
- What data was shared

This ensures full transparency.

7.12 RIGHT TO RAISE A COMPLAINT

Users can complain regarding:

- Data misuse
- Incorrect scan results
- Wrong reward rejection
- Failed payouts
- KYC issues
- Mishandling of counterfeit claims

✔️ **Where to raise complaints:**

- VCQRU Support
- Brand customer care
- Legal authorities (if needed)

7.13 RIGHT TO KNOW RETENTION PERIODS

Users can ask:

- How long data is stored
- Why retention is required
- Which data can be deleted earlier

7.14 RIGHT TO WITHDRAW FROM LOYALTY OR CASHBACK PROGRAM

Users may request complete removal from BL.

✔️ **Result:**

- No more points
- No future cashback

- Account closed
- Data retained only for audit/legal needs

7.15 RIGHT TO PRIVACY & ANONYMITY (Where possible)

You may verify products anonymously (AC verification does not always require login).
BL services require identity for payout, but AC does not.

SECTION 8 — USER RESPONSIBILITIES

To use VCQRU anti-counterfeit and loyalty services securely and fairly, users must follow the responsibilities below.
These responsibilities help prevent fraud, maintain system integrity, and protect all genuine users.

8.1 PROVIDE ACCURATE AND TRUTHFUL INFORMATION

✔️ **What this means:**

You agree to provide only correct, accurate, and updated information including:

- Name
- Mobile number
- UPI ID
- Bank details
- Address
- KYC documents

✔️ **Why important:**

Incorrect or misleading information may:

- Cause payout failures
- Lead to rejection of rewards
- Trigger fraud flags
- Block your account
- Slow down support resolution

✔️ **Examples of violations:**

- Using someone else's name
- Entering fake UPI IDs
- Providing wrong bank details to test payouts
- Uploading edited documents

This is strictly prohibited.

8.2 KEEP LOGIN CREDENTIALS & OTP CONFIDENTIAL

✔️ **What this means:**

- Never share your OTP with anyone
- Do not allow others to login using your mobile number
- Do not share your session or device with third parties

✔️ **Why important:**

OTP-sharing leads to:

- Unauthorized access
- Fraudulent reward redemption
- Wrongful payout attempts
- Misuse of scan data

VCQRU is NOT responsible for losses caused by user negligence.

8.3 DO NOT MISUSE QR CODES OR PRODUCT CODES

✔️ **Misuse includes:**

- Scanning the same code repeatedly to gain benefits
- Trying codes from the internet
- Scanning products you do not own
- Using photocopied or tampered labels
- Editing QR images
- Scanning codes from damaged or destroyed products

✔️ **Consequences:**

- Immediate disqualification
- Account suspension
- Loss of rewards
- Blacklisting
- Legal action (brand may initiate)

8.4 DO NOT ATTEMPT TO SELECTIVELY SCAN DIFFERENT PRODUCTS FOR BENEFITS

Users must scan only the legitimate products they purchased.
Trying random SKUs to “test if they give points” is considered abuse.

8.5 DO NOT USE FAKE, MANIPULATED, OR UNAUTHORIZED DEVICES/APPS

✔️ **Prohibited actions:**

- Using emulator apps
- Using rooted/jailbroken devices
- Using QR-altering software
- Using fake location apps
- Using VPNs to alter region
- Using hacking tools or scripts

✔️ **Why:**

These tools are commonly used for fraud in loyalty programs.

✔️ **Security Response:**

VCQRU automatically:

- Blocks sessions
- Blocks payouts
- Logs devices for investigation

8.6 FOLLOW ALL BRAND-SPECIFIC RULES & SCHEME TERMS

Each brand has:

- Unique eligibility
- Different reward structures
- Region restrictions
- Product restrictions
- MRP/batch requirements

User must comply with all such rules.
Violations may result in reward cancellation.

8.7 ENSURE UPI / BANK DETAILS ARE CORRECT & BELONG TO YOU

✔️ **You must ensure:**

- UPI is valid
- Bank account is correct
- Details belong to you (not a random person)
- Account is active

✔️ **Why:**

Wrong details cause:

- Permanent payout failures
- Fund loss (sometimes not recoverable)
- Payout rejection
- Fraud risk

Brands may deny payouts if ownership cannot be verified.

8.8 PROVIDE GENUINE KYC DOCUMENTS (IF REQUIRED)

✔️ **Documents must be:**

- Real
- Unedited
- Belonging to you
- Clear and readable

Uploading fake or edited KYC is a legal offense.

✔️ **Consequences:**

- KYC rejection
- Account block
- Permanent reward disqualification
- Legal action by brand

8.9 DO NOT CREATE MULTIPLE ACCOUNTS TO GAIN EXTRA BENEFITS

Fraud includes:

- Using multiple numbers
- Re-registering with new SIMs
- Creating accounts for family members for misuse
- Using different UPI IDs to claim additional benefits

VCQRU's system detects multi-account misuse automatically.

8.10 REPORT ANY FAKE PRODUCT OR SUSPICIOUS SCAN HONESTLY

If the system shows:

- Invalid Code
- Duplicate Scan
- Fake Product Suspected

You must:

- Not use the product
- Inform brand or VCQRU

- Not continue scanning it to exploit rewards

User safety comes first.

8.11 DON'T ATTEMPT TO REDEEM REWARDS ILLEGALLY

Fraud happens when:

- You try to redeem someone else's points
- You manipulate browser scripts
- You repeatedly request cashback for same product

This is strictly prohibited.

8.12 COMPLY WITH ALL LAWS AND REGULATIONS

You must comply with:

- Local laws
- Data privacy regulations
- Anti-counterfeit laws
- Taxation rules
- Identity verification rules

Violations may lead to legal consequences.

8.13 DO NOT TRY TO REVERSE-ENGINEER, HACK, OR DISABLE ANY VCQRU SYSTEMS

Prohibited actions include:

- Trying to bypass scan logic
- Intercepting network traffic
- Manipulating QR codes
- Attacking servers
- Running unauthorized penetration tests

VCQRU monitors all such activity.

8.14 RESPECT BRAND DECISIONS ON REWARD APPROVAL

The brand (not VCQRU) decides:

- Reward approval
- Point allocation
- Cashback eligibility
- Rejection reasons
- KYC requirements

User must respect these decisions.

8.15 RESPOND TRUTHFULLY TO CUSTOMER SUPPORT REQUESTS

Provide correct information when:

- Raising complaints
- Reporting counterfeit products
- Claiming missing rewards
- Submitting proof

False claims may lead to account suspension.

8.16 KEEP YOUR DEVICE SECURE & UPDATED

To ensure correct scanning:

- Maintain updated OS
- Allow camera permissions
- Ensure stable internet
- Avoid malware-infected devices

8.17 ENSURE SAFE USAGE OF SCANNED RESULTS

Users must use scan results responsibly and avoid spreading fake claims or misinformation.

8.18 USER IS RESPONSIBLE FOR ACTIVITY DONE THROUGH THEIR MOBILE NUMBER

All actions from your number are considered your responsibility unless proven otherwise.

8.19 READ AND UNDERSTAND ALL TERMS BEFORE USING THE SERVICE

Proceeding with OTP indicates full acceptance of all policies.

8.20 FOLLOW ALL INSTRUCTIONS SHOWN DURING SCAN OR LOGIN

These instructions help ensure security and proper functioning.

SECTION 9 — RESPONSIBILITY MATRIX (BRAND VS VCQRU)

This section clearly defines who is responsible for what, to ensure transparency and legal clarity.

We separate all responsibilities into:

- **Brand Responsibilities (What the Brand Owns)**
- **VCQRU Responsibilities (Technology & Platform Only)**

Let’s go deep.

9.1 WHAT THE BRAND IS FULLY RESPONSIBLE FOR

(Manufacturers / Product Owners / Principal Companies)

Brands have **complete ownership** of all business decisions.

Below are ALL areas that belong only to the brand:

9.1.1 PRODUCT QUALITY & SAFETY

The brand is solely responsible for:

- Manufacturing quality
- Product ingredients
- Product performance
- Safety & compliance
- Expiry and production dates
- Packaging quality
- MRP and labeling

VCQRU has **zero control** over product quality.

9.1.2 PRODUCT AUTHENTICITY & VALIDITY

VCQRU shows verification based on data provided by the brand.
The brand is responsible for:

- Authenticity records
- Batch mapping
- Ensuring secure QR/sticker usage
- Avoiding supply chain leakage
- Ensuring correct label print and placement

If wrong data is uploaded, the brand is responsible — not VCQRU.

9.1.3 REWARD, POINT & CASHBACK APPROVAL

The brand owns all decision-making about:

- How many points a user gets
- Who is eligible
- Reward structure
- Cashback amount
- Payout approval
- Scheme duration
- Conditions for qualifying
- Rejection of suspicious/red-flag claims

VCQRU only processes rewards based on brand rules.

9.1.4 KYC REQUIREMENTS & APPROVAL

Brand decides:

- Whether KYC is needed
- Which documents are acceptable
- Who is eligible based on KYC
- Whether to approve or reject KYC

VCQRU only verifies documents as per brand guidelines.

9.1.5 WARRANTY, RETURNS, & REPLACEMENTS

Brand owns:

- All warranty claims
- Return policies
- Replacement decisions
- Product malfunction issues
- Consumer complaints related to product performance

VCQRU is not involved in product refunds.

9.1.6 CUSTOMER SUPPORT FOR PRODUCT ISSUES

The brand is responsible for:

- Complaints about defects
- Customer dissatisfaction
- Damage or safety issues
- Replacement or refunds

VCQRU handles only **technical** queries related to the platform.

9.1.7 Payout Funding & Payment Settlement

The brand funds rewards.
The brand ensures:

- Wallet or cashback budget
- Payment approval
- Settlement of dues
- Handling failed transactions (final decision)

VCQRU does NOT pay any money from its own balance.

9.1.8 TAXATION & LEGAL COMPLIANCE (For Rewards)

Brand ensures:

- TDS deductions (under 194R)

- Filing returns
- Sending TDS certificates
- Reporting high-value transactions

VCQRU does not manage user tax records.

9.1.9 BRAND COMMUNICATION & TERMS

Brand is responsible for:

- All marketing material
- Program terms & conditions
- Privacy disclosures specific to product
- Customer care numbers & grievance redressal

VCQRU only displays what the brand provides.

9.1.10 APPROVALS FOR ACCOUNT BLOCK / UNBLOCK

Final decision to block/unblock users is always made by the brand.
VCQRU follows instructions.

9.2 WHAT VCQRU IS RESPONSIBLE FOR (TECHNOLOGY ONLY)

VCQRU owns only the **platform, backend engine, fraud detection, and payout processing infrastructure.**

Below are all responsibilities of VCQRU:

9.2.1 TECHNOLOGY PLATFORM OPERATION

VCQRU ensures 24/7 operation of:

- Anti-counterfeit system
- Loyalty portal
- Cashback engine
- KYC module
- Authentication system
- Scan analytics

9.2.2 STABLE & SECURE USER EXPERIENCE

VCQRU ensures:

- Smooth scanning
- Secure login
- Fast response
- Accurate results
- Zero downtime (best effort)

9.2.3 DATA SECURITY & PRIVACY PROTECTION

VCQRU is responsible for:

- Encryption
- Secure storage
- Access control
- Firewalls
- GDPR/DPDP compliance
- Zero data leak policy

9.2.4 FRAUD DETECTION & FLAGGING

VCQRU detects fraud using:

- Device intelligence
- Location mismatch
- Duplicate scan detection
- Multi-account mapping
- Suspicious UPI usage

VCQRU passes the final fraud decision to the brand.

9.2.5 PROCESSING OF REWARDS & PAYOUTS

VCQRU executes:

- UPI payouts
- NEFT payouts
- Reward ledger updates
- Cashback retries

Based on brand instructions.

9.2.6 VERIFICATION OF USER INPUTS

VCQRU checks:

- UPI validation
- Bank account validation
- Document clarity
- KYC matching

VCQRU does NOT approve — only verifies.

9.2.7 MAINTENANCE OF AUDIT LOGS

VCQRU maintains logs for:

- Scans

- Payouts
- KYC
- Login history
- Device fingerprint
- Fraud alerts

9.2.8 TECHNICAL CUSTOMER SUPPORT

VCQRU handles:

- Portal not loading
- OTP not received
- QR not scanning
- App/website errors
- Payout processing errors

But **NOT** product related issues.

9.2.9 BRAND-INSTRUCTED DATA PROCESSING

VCQRU processes data:

- Only on behalf of brand
- Only for intended purpose
- Only with user consent
- Only within defined limits

9.2.10 ZERO INVOLVEMENT IN PRODUCT DECISIONS

VCQRU has no role in:

- Product manufacturing
- Pricing
- Safety
- Quality
- Offline distribution
- Warranty claims
- Market launches

9.3 WHAT VCQRU IS NOT RESPONSIBLE FOR (LEGAL PROTECTION CLAUSES)

❌ **Product quality issues**

❌ **Product safety or failures**

❌ **Incorrect or missing rewards due to brand rules**

❌ **Returns, warranty, refunds**

❌ **Incorrect data uploaded by brands**

❌ **User-entered data mistakes (wrong UPI, wrong KYC)**

❌ **Network failures during payout**

❌ **Government actions or legal requirements**

❌ **User negligence (OTP sharing, multiple account misuse)**

These are critical clauses that protect VCQRU legally.

9.4 WHAT USER IS RESPONSIBLE FOR (SUMMARY OF SECTION 8)

Users must:

✔️ Provide correct information
✔️ Maintain OTP privacy
✔️ Use only authentic products
✔️ Avoid abusing schemes
✔️ Comply with brand rules
✔️ Use valid bank/UPI details
✔️ Submit genuine KYC

Violations may result in:

❗ account block
❗ reward cancellation
❗ legal action

SECTION 10 — SPECIAL CLAUSES & CONDITIONS

10.1 MULTIPLE ACCOUNT / MULTIPLE DEVICE FRAUD

✔️ **What it means:**

Creating multiple accounts using:

- Different mobile numbers
- Virtual numbers
- SIM cards
- Family numbers
- Repeated devices

to earn extra benefits is **strictly prohibited**.

✔️ **System Action:**

VCQRU will automatically:

- Map device fingerprint
- Detect duplicate UPI
- Identify suspicious patterns
- Block related accounts
- Reject payouts

✔️ **Brand Action:**

Brand may permanently disqualify the user from all future schemes.

10.2 QR CODE / SECURITY CODE DUPLICATION OR SHARING

Fraud includes:

- Sharing codes with others
- Posting codes online
- Forwarding photos of QR codes
- Scanning printed photocopies
- Scanning screenshots
- Scanning images from social media

System Action:

- Code flagged as abuse
- Points cancelled
- Account blocked
- Device blacklisted

10.3 LOCATION SPOOFING / VPN MISUSE

Using apps or tools to fake your GPS location to qualify for region-specific offers is not allowed.

VCQRU detects:

- Fake GPS apps

- VPN/Proxy networks
- IP mismatches
- Suspicious location jumps

Action:

- Automatic rejection
- Account suspension

10.4 MANIPULATION OF DEVICE OR BROWSER

Prohibited tools:

- Rooted phones
- Jailbroken iPhones
- Emulator/virtual device
- Script injections
- Browser tampering

Result:

- Scans rejected
- Account blocked
- Rewards cancelled

10.5 INCORRECT, FAKE, OR MISLEADING USER INFORMATION

Includes:

- Fake name
- Wrong UPI ID
- Someone else’s bank account
- Edited KYC
- Falsified photos
- Wrong address

Consequences:

- KYC failure
- Payout rejection
- Permanent blocking
- Brand may initiate legal action

10.6 WRONG UPI / BANK DETAILS ENTERED BY USER

Responsibility:

User is fully responsible for entering correct payout details.

If the user enters wrong UPI/bank details:

❌ reward cannot be reversed
❌ VCQRU is not liable
❌ brand will not re-issue payout

Why:

Banks do not refund misdirected UPI payouts.

10.7 WRONG PRODUCT SCANNED

If the user scans:

- Different SKU
- Expired product
- Old packaging
- Product from outside promo region

Brand may reject benefits.

10.8 BRAND HAS FINAL AUTHORITY OVER REWARD DECISIONS

VCQRU only processes.
Brand finalizes:

- Points
- Cashback
- Rejections
- Approvals
- Justifications

User agrees to accept brand decisions.

10.9 FAKE PRODUCT HANDLING CLAUSE

If a user scans and finds:

- “Fake Product Suspected”
- “Invalid Code”
- “Duplicate Code”

User must:

✔️ Stop using product
✔️ Contact brand support

✔️ Provide photos/videos
✔️ Provide purchase invoice (if asked)

VCQRU is **not responsible** for:

- Refunds
- Replacements
- Product damages
- Any physical or financial loss

These responsibilities belong to the brand.

10.10 DUPLICATE REWARD ATTEMPTS

Duplicate claims include:

- Scanning same product twice
- Trying to redeem same reward twice
- Trying different accounts for same product

VCQRU automatically prevents this.

Brand may:

- Cancel points
- Disable cashback
- Suspend the user

10.11 TAXATION CLAUSE (SECTION 194R / TDS)

For cashback/rewards above government threshold:

✔️ PAN required
✔️ TDS may be deducted
✔️ TDS certificate issued by brand
✔️ User responsible to submit correct PAN

VCQRU is not responsible for:

- TDS errors
- PAN mistakes
- Filing of tax returns
- Government notifications

10.12 REFUND & CANCELLATION CLAUSE

VCQRU does NOT:

❌ Provide refunds

❌ Reverse payouts

❌ Reverse points

❌ Adjust rewards

All financial decisions belong to the brand.

10.13 USER MISCONDUCT / ABUSE POLICY

The following actions can lead to **immediate, permanent suspension**:

- Abusive behavior with support
- Disrespectful language
- Threatening staff
- Misusing the platform
- Attempting to extort rewards
- Harassment of brand employees

Brand and VCQRU reserve right to block user.

10.14 BLACKLISTING CLAUSE

Users may be blacklisted across:

- All VCQRU platforms
- All brand schemes
- All future loyalty programs

If found guilty of:

- Fraud
- KYC forgery
- Multi-account abuse
- Payment misuse
- Fake complaints
- Code tampering

10.15 SCAN RESULT ACCURACY CLAUSE

Scan result depends on:

- Data from brand
- Proper label printing
- Product packaging
- Correct batch mappings

VCQRU is not responsible if:

- Brand uploads wrong data
- Distributor misuses genuine labels
- Retailer mixes batches

System displays results **based on brand data only**.

10.16 SYSTEM LIMITATIONS CLAUSE

Users understand that:

- OTP delays may occur
- Network issues may cause slow response
- Browser errors may occur
- Bank server outages may delay payouts

VCQRU is not liable for external system failures.

10.17 FORCE MAJEURE CLAUSE

VCQRU is not responsible for failures due to:

- Natural disasters
- Government restrictions
- Server downtime at bank/NPCI
- Telecom outages
- Pandemics
- Riots / strikes

SECTION 11 — USER CONSENT & DECLARATION

(This is a complete, legally strong, final statement)

11.1 CONSENT TO USE PERSONAL, FINANCIAL & SCAN DATA

By proceeding, logging in, scanning a product, submitting information, or using any feature of VCQRU's Anti-Counterfeit (AC) or Build Loyalty (BL) services, **you voluntarily give clear, informed, and unambiguous consent** for VCQRU Private Limited to:

1. Collect your personal details
2. Collect your financial information (UPI/Bank)
3. Process your scan history
4. Access device, network, and location data
5. Process your KYC (if required)
6. Use your information to deliver the AC & BL services
7. Use fraud detection & security systems
8. Share data with brands and payment partners as necessary

This is required for authentication, reward processing, counterfeit detection, and user safety.

11.2 CONSENT TO SHARE DATA WITH BRAND PARTNERS

You understand and agree that:

- VCQRU is only a technology provider
- The brand owns the product and the loyalty program
- VCQRU may share your scan history, KYC status, UPI/bank details (for payout), and fraud alerts with the brand
- The brand makes all final decisions on authenticity, rewards, cashback eligibility, KYC approval, disputes, taxation, and payouts

You consent to this data sharing for legitimate brand purposes.

11.3 CONSENT TO SHARE DATA WITH PAYMENT PARTNERS (NPCI/RBI)

By requesting any cashback or payout, you consent to share your:

- UPI ID
- Bank Account Number
- IFSC
- Beneficiary Name
- Payout logs

with NPCI-authorized payment gateways and RBI-regulated banks **strictly for processing payouts**.

No sensitive banking passwords / PINs are ever collected or shared.

11.4 CONSENT TO KYC COLLECTION & VERIFICATION

If a brand requires KYC:

You agree to submit valid, genuine documents such as PAN, Aadhaar, Voter ID, Driving License, etc., and consent to:

- Document verification
- Identity verification
- Facial or OCR verification
- Fraud checks
- Storage for compliance period

KYC is done only when mandated by the brand or by law.

11.5 CONSENT TO FRAUD DETECTION & SECURITY CHECKS

By using the service, you explicitly allow VCQRU to:

- Track device fingerprint

- Check location consistency
- Detect duplicate scans
- Flag repeated code misuse
- Identify VPN/GPS spoofing
- Map multi-account behavior
- Block suspicious accounts

You accept that such automated systems are essential for platform integrity.

11.6 CONSENT TO CONTACT FOR SERVICE UPDATES

You agree that VCQRU or the brand may contact you through:

- SMS
- WhatsApp
- Push notification
- Email
- In-app messages

for:

- OTP delivery
- Reward updates
- Payout status
- KYC issues
- Counterfeit alerts
- Safety information
- Scheme-related updates

No marketing is done without explicit brand permission.

11.7 ACKNOWLEDGEMENT OF BRAND RESPONSIBILITY

You acknowledge that:

- Product quality, warranty, safety, refunds, replacements, and commercial offers belong to the brand
- Reward approval, rejection, scheme eligibility, KYC rules, and tax deductions belong to the brand
- VCQRU does not manufacture, sell, distribute, or own any product
- VCQRU does not decide reward amounts or payout eligibility

VCQRU provides only the technical platform.

11.8 CONSENT TO DATA RETENTION & LEGAL COMPLIANCE

You agree that:

- Scan data may be stored for counterfeit prevention

- Reward transactions may be retained for audit
- KYC data may be retained for the legally mandated period
- Payout logs may be retained for financial compliance
- Fraud logs may be retained for investigation

Retention follows DPDP Act, IT Act, and brand compliance.

11.9 CONSENT TO LIMITATIONS & SYSTEM REQUIREMENTS

You understand that:

- UPI failures may occur due to bank/NPCI issues
- OTP delays may occur due to telecom networks
- Wrong UPI/bank details entered by you cannot be reversed
- Scan results depend on brand-provided data
- Device issues may impact QR scanning

VCQRU is not responsible for external system failures or user errors.

11.10 CONSENT TO TERMS OF USE & RESPONSIBLE BEHAVIOUR

By continuing, you confirm that you:

✔️ Will not misuse QR codes
✔️ Will not attempt fraud
✔️ Will not use fake location/VPN
✔️ Will not use multiple accounts
✔️ Will submit genuine KYC
✔️ Will use the platform ethically
✔️ Will follow brand rules
✔️ Will respect decisions taken by the brand

Violation may lead to account suspension or legal action.

11.11 BINDING AGREEMENT THROUGH OTP LOGIN

Entering the OTP or clicking "Continue" confirms that:

- You have read this policy
- You understand it clearly
- You voluntarily consent
- You agree to all terms
- You allow data processing as described
- You allow data sharing as required
- You confirm identity authenticity

- You accept all responsibilities

OTP = Legal Digital Signature
(Under IT Act, 2000 & DPDP Act, 2023)

11.12 CONTACT FOR CONSENT WITHDRAWAL OR QUESTIONS

You may request:

- Consent withdrawal
- Data access
- Data correction
- Account deletion (non-audit data)
- Complaint escalation

Through support or brand channels.

Withdrawal will disable loyalty, cashback, profile access, and verification history.