

PRIVACY POLICY

QRching

English version

Last updated: 4 August 2026

<https://qrching.com>

1. General information

This Privacy Policy explains how QRching UG (haftungsbeschränkt) ("QRching", "we") processes personal data when the website <https://qrching.com>, the web application and the QRching mobile application are used (together, the "Platform"). It provides the information required by Articles 12 to 14 of the General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR").

QRching is a technical platform for QR-code marketing and free giveaways. Users may participate in campaigns, while users aged 18 or over may create campaigns as Sponsors. QRching may also act as Sponsor for its own campaigns.

By using the Platform, you confirm that you have read this Policy. This does not mean that all processing is based on consent: the legal basis stated below applies to each purpose. Where consent is required for a particular activity, we request it separately; continued use of the Platform does not replace that consent.

2. Controller and contact details

QRching UG (haftungsbeschränkt), Bettina-von-Arnim-Straße 4, 92637 Weiden i.d.OPf., Germany.
Register court: Amtsgericht Weiden i.d.OPf.; commercial register: HRB 6622; VAT ID: DE348352084.

Privacy questions and data-subject requests may be sent to support@qrching.com or through the Platform contact form. If a data protection officer is appointed, their current contact details will be published in this section.

3. Who this Policy applies to

This Policy applies to website visitors, registered users, participants, Sponsors, winners, support correspondents and other persons whose data is processed in connection with the operation of the Platform, payments, payouts, claims or lawful requests.

4. Personal data we process

4.1. Account and registration. Selected language, nickname, email address, status and technical details of verification by one-time code, account identifier, date of birth where age verification is required, and the version, date and time of accepting legal documents or giving or withdrawing separate consent.

4.2. Sponsor and campaign. First and last name, date of birth where age verification is needed, gender, country, city, postal code, street and house number, time zone, Sponsor nickname, link to the page displaying the QR code for a public campaign, campaign type and format, dates, currency, prize fund, number and value of prizes, scanning rules and restrictions, and information on creation, payment, activation, completion or cancellation.

4.3. Participation and scans. Account identifier and nickname, campaign and QR-code number, date and time of an attempt, number and frequency of scans, participation status and result, prize and prize value, and internal indicators needed to prevent repeat participation, multiple accounts, circumvention of blocks and other abuse. Ordinary participation does not require a full name, postal address or payout details.

4.4. Winner verification and payout. First and last name, date of birth, country of residence and address or supporting documents; selected payout method; account holder, IBAN or account number,

BIC/SWIFT and bank details; PayPal email address; Bitcoin address where BTC payouts are supported; results of age, identity, sanctions, entitlement and fraud checks; and status of the claim, payout, refusal, disqualification or expiry. Providing details does not guarantee payout before verification has been completed.

4.5. Sponsor payments, refunds and financial records. Amount, currency, date, status and transaction identifier, payment or refund method, reason for a refusal or refund, and truncated payment-method information received from the provider. The Platform also creates campaign-related invoices, fund allocation certificates, fund claim lists, fund closure records, fund transfer records and other financial documents. Although users do not always provide this information directly, it is personal data where it relates to an identifiable Sponsor or winner. QRching normally does not receive full card details where they are entered directly with a payment provider.

4.6. Support and correspondence. Account email address, name if provided, subject, message, attachments, communication history and technical information needed to handle the request. A telephone number is processed only when voluntarily provided or necessary for a specific matter.

4.7. Automatically generated and collected data. A pseudonymous cryptographic device or installation identifier may be generated on installation or first use. It does not itself contain a name or contact details, but is personal data if it can be linked to an account, device or user activity. The Platform creates statistics on scans, participation, wins, and campaigns created and completed. We may also process IP address, device type, operating system, browser, app version, language, time zone, session data, push token, error and security logs and Platform events.

4.8. Location. If device permission is granted, the Platform may obtain approximate or precise location to determine country, city, postal code, time zone or availability of regional features. Where precise location is unnecessary, we use less precise information or manual input. Permission can be withdrawn in device settings. Location is not used for advertising without any separately required consent.

5. Sources of personal data

We obtain most data directly from users. Other data is generated during registration, scanning, winner selection, operation and financial closure of campaigns; obtained from devices and logs; payment and payout providers; a Sponsor or the public campaign resource; identity, age, sanctions or fraud-screening providers where actually used; and public authorities, courts, advisers and contractual partners where there is a lawful basis.

6. Purposes and legal bases

Article 6(1)(b) GDPR: creating and using an account, participation and scan records, creating and operating campaigns, selecting winners, verifying entitlement, making payouts, accepting payments, processing refunds and providing contractual support. The relevant feature may be unavailable without required data.

Article 6(1)(c) GDPR: compliance with accounting and tax retention duties and lawful requirements of courts and public authorities.

Article 6(1)(f) GDPR: Platform security and stability, prevention of fraud, multiple accounts and circumvention of blocks, enforcement of rules, fault analysis, dispute resolution and the establishment, exercise or defence of legal claims. We limit processing to what is necessary and balance our interests against users' rights.

Article 6(1)(a) GDPR: separate consent where required, for example for optional analytics, advertising, marketing communications or voluntary location functions. Consent may be withdrawn at any time with future effect.

7. Required information

Data marked as required is necessary to enter into or perform a contract, comply with law or prevent abuse. Without it, the relevant feature may be unavailable. For example, QRching cannot pay a prize without the required payout details and verification information. Optional information is identified separately.

8. Recipients

Where necessary, data may be received by providers of hosting, cloud infrastructure, backups, email and one-time codes, push notifications, support, error monitoring and security; payment providers, banks and international payout services, including Stripe, PayPal and the bank or service selected for payout; identity, age, sanctions or fraud-screening providers where used; accountants, tax advisers, auditors, lawyers, insurers, courts and competent authorities.

Processors are bound in accordance with Article 28 GDPR. Banks, app stores and some payment services may act as independent controllers for their own processing. In a business reorganisation, data may be disclosed to a buyer, investor or successor subject to confidentiality and law. As a rule, Sponsors do not receive a winner's real name, address, email address or payout details unless this is required for a specific campaign and was clearly disclosed in advance.

9. Public information

The public winners list may display a nickname, date or campaign details and prize value. Real names, addresses, email addresses, payout details, device identifiers and verification documents are not made public.

10. Cookies, local storage and app permissions

Strictly necessary cookies and local storage may be used for sessions, security, fraud prevention, language and technical settings. Access to information on a device without consent takes place only where permitted by section 25(2) TDDDG; the related processing of personal data is based on Article 6(1)(b) or (f) GDPR.

The camera is used to scan QR codes. Photo or file access is used to select a saved QR-code image; where the operating system provides selective access, the Platform receives only the selected file. Push notifications are sent after device permission and may be disabled in device settings. Optional analytics or advertising technologies are used only where the required consent has been given.

11. International transfers

We aim to process personal data within the European Economic Area. If data is transferred outside the EEA, we use safeguards provided for by law, such as an adequacy decision of the European Commission or Standard Contractual Clauses. Additional information about the safeguards used and how to obtain a copy may be requested at support@qrching.com.

12. Retention

Account data is retained while the account is active and then deleted or restricted unless another lawful purpose applies. Participation, scan and result data is retained until campaigns, claims and possible disputes are closed and then until applicable limitation periods expire. Winner data is retained until verification and payout or expiry of the 30-day period for providing information; evidence of decisions may be kept longer for legal claims.

Payment and accounting documents are retained according to their category and German law, generally for eight years for accounting vouchers and ten years for books, records and certain tax-relevant documents. Support matters are normally retained for up to three years after closure. Routine security logs are normally retained for up to 90 days, longer where an incident or investigation requires

it. Evidence of consent and withdrawal is retained while the relevant processing applies and then as long as needed to demonstrate compliance. Fraud-prevention and block identifiers are retained only while there is a material circumvention risk, subject to periodic review. Legal-claim records are kept until proceedings end and the applicable periods for bringing or defending claims expire. Data is then deleted or irreversibly anonymised.

13. Automated processing and abuse prevention

Algorithms automatically apply campaign rules, take account of scan frequency and sequence and determine winning events. In classic campaigns, winners may be selected automatically from eligible participants; in dynamic campaigns, the result depends on a winning scan number set in advance. Fraud systems may flag suspicious activity.

Where a solely automated decision produces legal or similarly significant effects, we apply Article 22 GDPR, including the right to request human intervention, express your point of view and contest the decision, unless the law provides otherwise. On request, a disputed disqualification or payout refusal based on a fraud signal is reviewed by a person. The minimum necessary pseudonymous identifiers and the reason and date of a block may be retained under Article 6(1)(f) GDPR. You may object to this processing under Article 21 GDPR.

14. Security

We use proportionate technical and organisational measures, including access controls, logging, encryption in transit, backups, data minimisation, vulnerability management and incident response. Absolute security cannot be guaranteed; measures are reviewed in light of risk and technological development.

15. Your rights

Where the legal requirements are met, individuals have rights to information and access (Articles 13–15 GDPR), rectification (Article 16), erasure (Article 17), restriction (Article 18), notification of recipients (Article 19), data portability (Article 20), objection to legitimate-interest processing and at any time to direct marketing (Article 21), safeguards for solely automated decisions (Article 22), withdrawal of consent for the future (Article 7(3)) and lodging a complaint with a supervisory authority (Article 77).

Requests may be sent to support@qrching.com. We may request reasonable proof of identity to protect personal data. We normally respond within one month; for complex requests the period may be extended by up to two further months with notice and reasons. Statutory retention duties and the rights of others may limit these rights.

16. Account and data deletion

Under Article 17 of the General Data Protection Regulation (GDPR), a user is entitled to request deletion of their account and the personal data associated with it where the statutory requirements are met.

A request to delete the account and personal data must be submitted exclusively by email to support@qrching.com. The request should be sent from the email address linked to the QRching account and should state the account email address and the username. If the request cannot be sent from the linked email address, QRching may request additional information necessary to verify the user's identity and authority over the account.

Partial deletion of individual data without deletion of the account is not available. The request covers deletion of the account as a whole and the personal data associated with it. After the request has been reviewed and confirmed, profile data, contact details, optional settings and other content associated with the account will be deleted or irreversibly anonymised unless further retention is necessary to comply with statutory obligations or for another lawful purpose.

Deletion of the account does not extend to data that QRching is required or permitted to retain temporarily. This may include, in particular, accounting and tax records, payment and payout information, records relating to unfinished campaigns, claims and disputes, evidence of consents given and actions taken, as well as the minimum identifiers required for fraud prevention and information concerning blocks. Processing of such data is restricted to the relevant purpose. The data is not used for incompatible purposes and is deleted or irreversibly anonymised after the retention periods specified in section 12 of this Privacy Policy have expired.

The request will be handled without undue delay and generally within one month after receipt and any required identity verification. Taking into account the complexity and number of requests, this period may be extended by up to two further months. In that event, the user will be informed of the extension and the reasons for it within one month after receipt of the request. QRching may request reasonable proof of identity to prevent an account and its data from being deleted at the request of an unauthorised third party.

17. Age restrictions

The Platform is intended for users aged 13 and over. Participation in individual giveaways and receipt of prizes are available from age 16. Only persons aged 18 or over may create giveaways and act as Sponsors.

18. Third-party resources

The Platform may link to Sponsor websites, pages and resources. Their operators are independently responsible for their processing. QRching may check a public resource supplied by a Sponsor only to the extent needed to confirm publication of the QR code and compliance with campaign rules.

19. Changes and supervisory authority

We update this Policy when the Platform, providers, processing or law changes. The current version and date are published at <https://qrching.com>. Material changes are communicated in advance where required by law; any required new consent is requested separately.

A complaint may be lodged with any competent supervisory authority, in particular the Bayerisches Landesamt für Datenschutzaufsicht (BayLDA), Promenade 18, 91522 Ansbach, Germany; postal address: Postfach 1349, 91504 Ansbach, Germany; <https://www.lida.bayern.de/de/beschwerde.html>.