

QR2Connect Privacy Policy

Last updated: 22 April 2025

Your privacy is important to QR2Connect (“QR2Connect,” “we,” “us,” “our”). QR2Connect has created this Privacy Policy (“Privacy Policy”) to demonstrate the commitment to protecting your privacy and to explain the personal data QR2Connect processes, how QR2Connect processes it, and for what purposes. It also describes the choices available to you regarding our use of your personal information and how you can access and update this information.

1. GENERAL

QR2Connect is a mobile and desktop software program utilized by individuals and businesses. QR2Connect allows users to share information on mobile devices and computers for the purposes of anonymously communicating with others. QR2Connect utilizes sophisticated encryption software in order to ensure that all information shared between users remains secure, thereby driving meaningful interactions, relationships and creating better outcomes for individuals, professionals and businesses.

2. INFORMATION WE PROCESS

QR2Connect collects personal information about you as you use QR2Connect, through your interactions with us, as well as from previous owners and data controllers. “Personal information” is any information that relates to an identifiable individual and may include name, address, email address, phone number, login information (account number, password), social media account information, or payment card number.

We collect the following personal information:

Your account information. We collect limited personal information from users who register with our services including your first and last name and your contact details (such as your email address or your phone number).

Address book information. When you access and use our services, you may elect to share the data stored in the address book on the device from which you are accessing and using the service (the “Address Book Data”). If you decide to share this data with us, we will see the Address Book Data only in hashed/anonymized form (i.e., in a manner in which we cannot read the data) and we will not store your Address Book Data for non-QR2Connect users. We will use Address Book Data only to provide you with our services and to help you connect with people on QR2Connect that you have listed in your address book via their email address and/or phone number. If you would like to invite one of your friends to QR2Connect, we will send them an invitation to our service (eg, via SMS or email) and then delete that data as soon as the invitation is sent.

Device and connection information. When you download and use our services, we automatically collect information on the type of device you use, operating system version, a randomly-generated device identifier, system performance information, and IP address.

Location information. We collect your general location, such as your country from your device settings and based on your IP address. We do not at any time collect your precise location.

Usage, event and log information. We process certain log and contact data and other related information, such as your unique QR2Connect user ID and service-related, diagnostic, event and performance information (e.g., subscription status and connection information), in order to provide the service to you. For example, so the recipient of your message will know who has sent them the message. We do not store the contents of your messages or the recipients of your communications.

INTERNAL

Custom support and other communications. When you contact us for customer support or otherwise communicate with us, you may provide us with information related to your use of our products that you deem helpful. For example, information relating to app performance or other issues.

Billing information. If you decide to subscribe to our service directly via our website, we may collect credit card information which is tokenized and used for payment processing, but not stored. In all other circumstances, you will be directed to the appropriate app store, which may require you to provide certain payment and billing information. In the event you subscribe to our services via an app store, we will not store your billing information.

Your Messages on QR2Connect

When you use our services to send and/or receive encrypted messages, we store your message(s) in encrypted form. We do **not** have access to your messages at any time. Similarly, we do **not** have the ability to decrypt or read your encrypted messages.

3. HOW WE USE PERSONAL INFORMATION

In addition to the purposes described above, we may use the information we collect for a variety of purposes, such as the following:

Service delivery and Customer support

- Maintaining or servicing accounts, providing customer service, operation our website and mobile applications; processing or fulfilling orders and transactions, verifying user information, processing payments;
- Communicating about the products and Services we offer, and responding to requests, inquiries, comments, and suggestions.

Service improvement

- Conducting statistical analyses or other research activities to optimize our features and provide you with new ones;
- Understanding and evaluating how our Services and features perform with our users;
- Uncovering insights about usage in order to improve the Services and provide customers with enhanced features as well as inform our development of new features and products.

Profiling

- **Measuring our advertising and marketing activity** (e.g., measuring how a user was acquired).
- **Troubleshooting**
- Ensuring the quality and the proper functioning of our Services by analyzing, preventing, and correcting failures and bugs, and to prevent the illicit use or misuse of the Service.
- **Targeted advertising and marketing**
- Understanding our customer in order to more effectively market our Services
- Serving relevant advertisements, if applicable.
- **Quality and Safety Maintenance and Verification**

- activities related to improving the quality of the Services we provide, including upgrade or enhancement of the Services;
- verification or maintenance of the quality or safety of Services;
- Tracking and responding to quality and safety matters;
- Protecting our rights and property.

Compliance with legal obligations

- Complying with our legal obligations, including requests from public authorities, and proving that we have complied with them, such as in the event of a request from a public authority.

Defense

- Establishing, exercising, or defending our rights and those of our employees, and to carry out corporate transactions or operations. For example, your data may be processed in the event of bankruptcy, merger, acquisition, reorganization, and sale of assets or assignments, and the due diligence related to any such transactions.
- To perform the above functions, we may match information collected from you through different means or at different times, including both personal information and Automated Information, and use such information along with information obtained from other sources. We may also aggregate and/or de-identify any information that we collect, such that the information no longer identifies any specific individual. We may use, disclose and otherwise process such information for our own legitimate business purposes – including historical and statistical analysis and business planning – pursuant to this Privacy Policy and applicable privacy laws.

4. DATA SHARING

Your personal data may be transmitted to trusted and reliable third parties. This happens only when there are lawful grounds for the transmission. We don't sell your data, including your images, to third parties under any circumstances.

The types of third parties to which your data may be transmitted are as follows:

- Third parties that carry out activities related to our business and operations. Such parties can operate either on our behalf as data processors (for example, IT or storage service providers) or as autonomous data controllers (for example, professional advisors providing advice or otherwise protecting and managing our business interests).
- Third parties that collect personal data about you to show personalized advertising.
- Advisors and new owners, in the event that we carry out a corporate transaction or operation such as a merger, acquisition, reorganization, sale of assets or assignments, and as a part of the associated due diligence.
- Public, judicial, or police authorities, within the limits established by applicable laws.
- Other parties as necessary (for example, competent authorities), if we have reason to believe that your actions are inconsistent with our user agreements or policies or that you've violated the law, or if it's necessary to protect our rights, property, and safety or that of our users, the public, or others.

Additionally, we may share your personal data if it's required for the fulfillment of a legal obligation, or if you give us your consent to do so.

5. SOCIAL MEDIA AND OTHER COMMUNICATIONS

We maintain a presence on several social networking and blogging platforms, such as Facebook, Instagram, Google, LinkedIn, Twitter, Snap, TikTok and Pinterest. We may incorporate some third-party social networking features into our Services (including, allowing users to interact with others and share certain content and information

INTERNAL

on social media platforms) or utilize third-party provided platforms to publish or manage the Services or portions thereof. Through these platforms and features, we receive or may share information about you, and this Privacy Policy applies to that information as well. In addition, some providers of third-party social media or blogging platforms we utilize have their own privacy policies which explain how the third parties that provide them may collect, use and protect your information (e.g., if you establish an account with such platform providers directly). By using social features, you agree to those third parties' privacy policies and terms of use.

If you choose to communicate with us or another user through social features available on our websites or mobile applications or through our social media pages, or other similar communication or messaging features or services, such information may be made publicly available. **For security purposes, please do not include any password, social security number, payment card or other sensitive information via these features.** We have the right, but not the obligation to monitor messages and communications between and among users for security and training purposes. We may, but are not obligated to, remove any content we deem inappropriate.

6. LEGAL BASIS FOR PROCESSING DATA

In this section, we identify the legal grounds on which we rely to process personal information.

In some cases, we have a legitimate interest to process the personal information that we collect, such as to develop, administer and support our products and services; to operate, evaluate and improve our business; to facilitate and manage engagement programs; to promote research; to support our recruitment activities; to facilitate a Corporate Transaction (including a sale of assets or merger or acquisition); or to fulfill our contracts with business partners, such as third parties that distribute our products.

It may also be necessary for us to process personal information to establish, exercise or defend against fraud, illegal activity, and claims and other liabilities, including by enforcing the terms and conditions that govern the services we provide.

We may also process personal information as specifically permitted by applicable legal requirements.

If we rely on consent for the processing of your personal information, we will seek such consent at the time we collect your personal information.

7. DATA RETENTION

We retain personal data used for defense purposes for a maximum of ten (10) years from your most recent interaction with the app, or from the expiration of your subscription. If you access the app after your subscription has expired, the retention period starts from this most recent interaction. Specific legal obligations might require different retention periods and, in such cases, those different periods will apply. Upon the expiry of the retention period, the data is either deleted or anonymized.

We retain personal data used for the purpose of compliance with legal obligations for a maximum of five (5) years from your most recent interaction with the app, or from the expiration of your subscription. If you access the app after your subscription has expired, the retention period starts from this most recent interaction. Specific legal obligations might require different retention periods and, in such cases, those different periods will apply. Upon the expiry of the retention period, the data is either deleted or anonymized.

We retain the personal data for a maximum of three (3) years from your most recent interaction with the app, or from the expiration of your subscription. If you access the app after your subscription has expired, the retention period starts from this most recent interaction. After this period, unless any legal obligations require that the data is retained for longer, the data is either deleted or anonymized.

8. INTERNATIONAL DATA TRANSFERS

We may transfer your personal information to countries other than the country in which the data was originally collected for the purposes described in this Privacy Notice. For example, if you are located outside of the United

INTERNAL

States, we may transfer your personal information to the United States. The countries to which we transfer personal information may not have the same data protection laws as the country in which you initially provided the information. When we transfer personal information across borders, we consider a variety of requirements that may apply to such transfers.

Specifically, we may transfer personal information from the European Economic Area to:

- Countries that the European Commissions has deemed to adequately safeguard personal information,
- Pursuant to the recipient's compliance with standard contractual clauses (also known as Model Clauses), or Binding Corporate Rules,
- Pursuant to the consent of the individual to whom the personal information pertains, or
- As otherwise permitted by applicable EEA requirements.

9. YOUR CHOICES AND RIGHTS

You have the following rights in relation to how we use your personal information:

- **Access**: you may request access to your personal information and receive copies of it;
- **Correction**: you may have inaccurate/incomplete personal information corrected and updated;
- **Object to, or Limit or Restrict, Use of Data**: you can ask us to stop using all or some of your personal information or to limit our use of it;
- **Deletion**: in certain circumstances, you can request a right "to be forgotten" (this is a right to have your information deleted or our use of your data restricted). We will honor such requests unless we have to retain this information to comply with a legal obligation or unless we have an overriding interest to retain it;
- **Portability**: in certain circumstances, exercise the right to data portability (this is a right to obtain a transferable version of your personal information to transfer to another provider); and
- **Consent Management**: where we rely on consent to process your personal data, you may withdraw consent at any time. You do not have to provide a reason for your withdrawal where processing is based on consent.

For your protection, we may require proof of identity and verification before we can answer your requests.

You also have the right to complain before the competent national data protection authority, or any other applicable regulator in the jurisdiction where you reside, in the event that you think we've violated the applicable privacy laws and we haven't addressed your request.

10. INFORMATION FOR RESIDENTS OF CALIFORNIA: YOUR CALIFORNIA PRIVACY RIGHTS

If you are a California resident, the California Consumer Privacy Act ("CCPA") may provide you with rights that are in addition to those set forth elsewhere in this Privacy Policy regarding our use of your personal information. The CCPA Notice applies to "Consumers" as defined by the law. This section describes your CCPA rights as a California Consumer and explains how to exercise those rights. See Sections 1 - 4 above to learn what information we collected from you and how it is collected, used and shared.

Access Rights

No more than twice in a twelve-month period, you may request the right to know what personal information we have collected about you, including the categories of personal information, specific pieces of personal information, categories of sources from which we collected your personal information, business or commercial purposes for our collection or sale of your personal information, and categories of third parties to whom we've disclosed your personal information.

Data Correction Rights

You may request to have inaccurate personal information corrected and updated.

Data Deletion Rights

Except to the extent we have a basis for retention under CCPA, you may request that we delete your personal information that we have collected directly from you and are maintaining. Note also that we are not required to delete your personal information that we did not collect directly from you.

Exercising Your Rights

To make a request for access, correction, or deletion according to your rights under CCPA, send your request to privacy@bendingspoons.com. Consumers may exercise these rights via an authorized agent. We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm that the personal information relates to you. Any request you submit to us is subject to an identification and residency verification process ("Verifiable Consumer Request").

The Verifiable Consumer Request must provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative; and describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

Some personal information we maintain about Consumers is not sufficiently associated with enough personal information about the Consumer for us to be able to verify that it is a particular Consumer's personal information (e.g., clickstream data tied only to a pseudonymous browser ID). In accordance with the CCPA, we do not include that personal information in response to Verifiable Consumer Requests. If we cannot comply with a request, we will explain the reasons in our response.

We will make commercially reasonable efforts to identify Consumer personal information that we collect, process, store, disclose, and otherwise use and to respond to your California Consumer privacy rights requests. We will typically not charge a fee to fully respond to your requests, but we may charge a reasonable fee, or refuse to act upon a request, if your request is excessive, repetitive, unfounded, or overly burdensome.

Opt-Out

To make a request to opt-out of sale under CCPA, email admin@qrcode2connect.com.

We will not discriminate against you in a manner prohibited by the CCPA because you exercise your CCPA rights. However, we may charge a different price or rate, or offer a different level or quality of good or service, to the extent that doing so is reasonably related to the value of the applicable data. In addition, we may offer you financial incentives for the collection, sale and retention and use of your personal information as permitted by the CCPA that can, without limitation, result in reasonably different prices, rates, or quality levels. The material aspects of any financial incentive will be explained and described in its program terms. We may add or change incentive programs and/or their terms by posting notice on the program descriptions and terms linked to above so check them regularly.

California's "Shine the Light" law, Civil Code section 1798.83, requires certain businesses to respond to requests from California customers asking about the businesses' practices related to disclosing personal information to third parties for the third parties' direct marketing purposes. Alternately, such businesses may have in place a policy not to disclose personal information of customers to third parties for the third parties' direct marketing purposes if the customer has exercised an option to opt-out of such information-sharing. As discussed above, if we share Personal Information with third parties for their marketing purposes you will be able to elect for us not to do so by submitting your request to admin@QRCode2Connect.com (please include your name, mailing address, and email address).

11. ONLINE PRIVACY CHOICES AND RIGHTS

Device permissions

Mobile platforms have permission systems for specific types of device data and notifications, such as camera and microphone as well as push notifications. Where applicable, you can change your settings on your device to either

INTERNAL

consent or oppose the collection of the corresponding information or the display of the corresponding notifications. Of course, if you do that, certain services may lose full functionality.

Uninstall

You can stop all information collection by the app by disabling call forwarding and deactivating your account by following the instructions on the Service's Settings screen and then uninstalling the app using the standard uninstall process for your device. If you uninstall the app from your mobile device, the unique identifier associated with your device will continue to be stored. If you re-install the application on the same mobile device, we will be able to re-associate this identifier to your previous transactions and activities.

Email

If you receive commercial email from us, you may unsubscribe at any time by following the instructions contained within the email. You may also opt-out from receiving commercial email from us, and any other promotional communications that we may send to you from time to time, by sending a request to admin@QRCode2Connect.com. Please be aware that if you opt-out of receiving commercial email from us or otherwise modify the nature or frequency of promotional communications you receive from us, it may take up to ten business days for us to process your request, and you may receive promotional communications from us that you have opted-out from during that period. Additionally, even after you opt-out from receiving commercial messages from us, you will continue to receive transactional or administrative messages from us regarding the Services.

Location information

If you choose to opt-in, some of our apps may collect your device's precise real-time location, and in such cases, you may be able to opt out from further allowing us to have access to such location data by managing your location preferences in the app and/or on your device.

Notice to Nevada users

We do not sell covered information, as defined under Chapter 603A of the Nevada Revised Statutes, and we do not have plans to sell this information. However, if you would like to be notified if we decide in the future to sell personal information covered by the Act, please contact us at admin@QRCode2Connect.com. You are responsible for updating any change in your email address by the same method and we are not obligated to cross-reference other emails you may have otherwise provided us for other purposes. We will maintain this information and contact you if our practices change.

New Privacy Laws

We understand that privacy laws are constantly evolving. New US state laws and new international privacy laws are consistently emerging, developing and being enacted. We will respect all applicable privacy laws.

Advertising Opt-Outs

You may choose whether to receive some Interest-based Advertising by submitting opt-outs. Some of the advertisers and Service Providers that perform advertising-related services for us and third parties may participate in the Digital Advertising Alliance's ("DAA") Self-Regulatory Program for Online Behavioral Advertising. To learn more about how you can exercise certain choices regarding Interest-based Advertising, including use of Cross-device Data for serving ads, visit <http://www.aboutads.info/choices/>, and <http://www.aboutads.info/appchoices/> for information on the DAA's opt-out program specifically for mobile apps (including use of precise location for third party ads). Some of these companies may also be members of the Network Advertising Initiative ("NAI"). To learn more about the NAI and your opt-out options for their members, see <http://www.networkadvertising.org/choices/>. Please be aware that, even if you are able to opt out of certain kinds of Interest-based Advertising, you may continue to receive other types of ads. Opting out only means that those selected members should no longer deliver certain Interest-based Advertising to you but does not mean you will no longer receive any targeted content and/or ads (e.g., from other ad networks). Also, if your browsers are configured to reject cookies when you visit these opt-

out webpages, or you subsequently erase your cookies, use a different device or web browser or use a non-browser-based method of access (e.g., mobile app), your NAI / DAA browser-based opt-out may not, or may no longer, be effective.

When you allow Notifications, we may send you offers and promotions related to our products and features. You may opt-out of these through the Settings menu on your device.

12. HOW WE PROTECT PERSONAL INFORMATION

We use various efforts intended to safeguard the security and integrity of personal information collected through our Services. Despite these measures, however, we cannot and do not guarantee that information will be absolutely safe from interception or intrusion during transmission or while stored on our system, or otherwise, and you provide information to us at your own risk.

If you correspond with us by email or using Web forms like a "contact us" feature available through our Services, you should be aware that your transmission might not be secure from access by unauthorized parties. We have no liability for disclosure of your information due to errors or unauthorized acts of third parties during or after transmission. If you create an **account** as part of using our Services, you are responsible for maintaining the confidentiality of your account password and for any activity that occurs under your account. Please notify us of any unauthorized use of your password or account.

If we believe that the security of your personal information in our care may have been compromised, we may seek to notify you. If we have your email address, we may notify you by email to the most recent email address you have provided us in your account profile. Please keep your email address in your account up to date. You can change that email address anytime in your account profile. If you receive a notice from us, you can print it to retain a copy of it. To receive these notices, you must check your email account using your computer or mobile device and email application software. We may also post a conspicuous notice on our site or notify you through the mobile application.

13. LINKS TO WEBSITES AND THIRD-PARTY CONTENT

For your convenience and information, we may provide links to websites and other third-party content that is not owned or operated by us. The websites and third-party content to which we link may have separate privacy notices or policies. We are not responsible for the privacy practices of any entity that we do not own or control. We encourage you to review the privacy policies of such third parties before providing them with any personal information.

14. INFORMATION RELATING TO CHILDREN

We do not knowingly collect information from children under the age of 16 years old (or older if required in an applicable jurisdiction to comply with applicable laws). If you are not over 16 years old (or older if required in an applicable jurisdiction to comply with applicable laws) then **DO NOT DOWNLOAD OR USE THE SERVICES**. If you are a parent or legal guardian and believe that we may have personal information from or about your child under the age of 16 years old, please contact us at admin@QRCode2Connect.com. Note that we'll attempt to delete the account of any child under the age of 16 that's reported to us as soon as possible. You are responsible for any and all account activity conducted by a minor on your account.

15. IN-APP TRACKING TECHNOLOGIES

When we refer to "tracking technology" or "tracking technologies" in this policy, we mean any technology that stores or accesses information on the user's device, including SDKs, tracking pixels, HTML5 local storage, local shared objects, and fingerprinting techniques.

Tracking technologies are usually classified by purpose (technical, analytics, profiling) and by publisher (first-party, third-party). The legal requirements vary based on these classifications.

The tracking technology classifications and some practical examples now follow.

By purpose

Technical tracking technologies

These are used to transmit messages over an electronic communication network or to provide a service specifically requested by the user. Therefore, they're necessary for the app to function correctly, and for providing the service requested by and offered to the user.

For example, technical tracking technologies can be used to monitor sessions, store specific server access information related to the user configuration, facilitate the use of online content, keep track of items in a shopping cart, or keep track of information used to fill in a form.

As technical tracking technologies are necessary, they don't need your consent.

Analytics tracking technologies

These are used to assess the effectiveness of an information society service provided by a publisher, evaluate and improve the design of an app, or help measure traffic. In other words, they serve to track the traffic and performance of an app by collecting aggregate data on the number of users and how they interact with the app, which helps to improve its services.

For example, analytics tracking technologies may collect information about how users access an app, including the number of users and potentially grouped by geographical area, time zone, how long they stay on the app, which parts of the app they interact with, and the number of users who used a particular feature.

Normally, analytics tracking technologies are used only with your explicit consent. However, in the following cases they're treated like technical trackers, so don't need your consent:

- When they're used only to produce aggregated statistics that are performed through the controller's own resources and that don't turn into activities that go beyond statistical counting and assisting business-related decision-making
- When the third parties don't match the analytics trackers' data with any other information, and don't send any data gathered to other third parties

Profiling tracking technologies

These are used to evaluate some personal aspects of certain users, and to trace specific actions or recurring behavioral patterns in the use of the app in relation to specific, identified or identifiable individuals, so they can be grouped within homogeneous, multi-sized clusters. This enables the company to analyze and predict personal elements, provide users with customized services beyond what's strictly necessary for the delivery of the service, and sending targeted advertising messages in line with the preferences they express during their in-app activities. These serve to convey behavioral advertising, measure the effectiveness of ads, and customize the services offered in line with the user's monitored behavior.

For example, profiling tracking technologies can be used for the following activities:

- To create user profiles and offer content in line with the user's interests
- To send targeted ads or messages
- To conduct statistical analysis or other research activities to improve our products and services and measure the effectiveness of our campaigns

Profiling tracking technologies are used only with your explicit consent.

By publisher

First-party tracking technologies

These are installed and managed directly by the owner of the app (in this case, QRCode2Connect S.p.A). As the owner, we process the collected data for our own purposes.

Third-party tracking technologies

These are installed and managed by different apps or developers, either for our purposes or for those of the third party.

The data collected by the third parties for their own purposes is governed by their specific privacy policies and terms and conditions. For further information about these data processing activities, you can directly refer to the privacy policy of the relevant third parties as indicated in the subsection [Types of tracking technologies used by the app](#).

Third-party tracking technologies need your consent, unless they're anonymized and only used for analytical purposes. You can manage consent at any time from within the app's privacy settings.

Types of tracking technologies used in the app

This app uses the following types of tracking technologies:

Name & Purpose	Retention period	Type of publisher & Description	Description
QR2Connect SDK (technical) Technical	3 years	First-party	Our internal software development kit (SDK). It's necessary for the app to function correctly.
QR2Connect SDK (statistical analytics) Technical	3 years	First-party	Our internal software development kit (SDK). It allows us to produce aggregated statistics.
Google Sign In Technical	Defined by the Third Party	Third-party https://policies.google.com/privacy	Thanks to this SDK developed by Google we can provide you with a secure, fast, and easy way to log in into our app using Google.
Zendesk Chat SDK Technical	Defined by the Third Party	Third-party https://www.zendesk.com/it/company/agreements-and-terms/privacy-notice/#	Thanks to this SDK we can easily integrate customer support features within our app.
Facebook SDK Technical	Defined by the Third Party	Third-party https://www.facebook.com/privacy/policy/?entry_point=facebook_page_footer	Thanks to this SDK developed by Meta we can provide you with a secure, fast, and easy way to log in into our app using Facebook. If you like, you'll also be able to share your workouts on Facebook in an easy way.
Firebase Crashlytics	3 years	Third-party https://policies.google.com/privacy	A tool provided by Google that's necessary for the app to correctly

Name & Purpose	Retention period	Type of publisher & Description	Description
Technical			interact with the backend and provide you with key features.
Firebase Dynamic Links	3 years	Third-party https://policies.google.com/privacy	A tool provided by Google that's necessary for the app to correctly interact with the backend and provide you with key features.
Technical			
FirebaseAuth	3 years	Third-party https://policies.google.com/privacy	A tool provided by Google that's necessary for the app to correctly interact with the backend and provide you with key features.
Technical			
Firebase Analytics	3 years	Third-party https://policies.google.com/privacy	A tool provided by Google that's necessary for the app to work properly. When analytics features are enabled, it can help us to improve app traffic and performance.
QR2Connect SDK (profiling)	3 years	First-party	Our internal profiling software development kit (SDK). It allows us to provide customized services.
Profiling			
Firebase Profiling	3 years	Third-party https://policies.google.com/privacy	Firebase is a tool provided by Google which is essential for the app to work properly. When profiling features are enabled, it can help us to measure the effectiveness of our ads.

Tracking technologies settings

You can turn on or turn off—in whole or in part—profiling and third-party analytics tracking technologies at any time through the app's privacy settings. As for Meta Audience Network SDK, if you're an Android user, you can manage your choices directly on Meta's website.

When you withdraw consent, your data will no longer be collected through those trackers. However, we'll continue processing the data collected before the withdrawal.

You can't turn off first-party analytics tracking technologies—they're treated like technical trackers, so aren't contingent on consent. However, you can opt out of the further processing of your data that's been collected via these trackers. To do so, contact us at admin@QRCode2Connect.com.

With regards to your rights under applicable Data Protection Laws, please refer to the section [Your choices and rights](#).

16. UPDATES TO OUR PRIVACY POLICY

We reserve the right to update this Privacy Policy to reflect changes in our practices and services. When we post changes to this Privacy Policy, we will update the date of this Privacy Policy. Continued use of the Services after such date constitutes acceptance of such updates. When required by applicable law, we may inform you by additional means, such as through a notification on the website or in our mobile applications if we make material changes to how your personal information is collected, accessed or otherwise used as a result of your use of the

Services or if your rights under this Privacy Policy are materially impacted by changes to our privacy practices. We recommend that you check this page from time to time to inform yourself of any changes in this Privacy Policy.

17. HOW TO CONTACT US

If you want to submit a request by email or if you have any other questions about privacy or data protection at QRCode2Connect, you can contact us at admin@QRCode2Connect.com

Help

For product support

[Support center](#)

For partnership inquiries^{SEP}

partnerships@QRCode2Connect.com

For press inquiries

press@QRCode2Connect.com

INTERNAL