

# biq Privacy Policy

**Effective Date:** May 18, 2025

## Introduction

Your privacy is important to biq. This Privacy Policy explains **what information biq collects** from users of our app and related services, **how we use and share that information**, and the choices you have regarding your data. This Policy is part of biq's Terms of Service; by using the biq Service, you agree to the collection, use, and disclosure of your information as described in this Privacy Policy. If you do not agree with our practices, please **do not use the app or Service**.

biq (referred to as “**biq**”, “**we**”, “**us**”, or “**our**”) operates globally, but we are committed to handling your personal information in accordance with applicable laws, including, where relevant, the EU General Data Protection Regulation (GDPR) and other data protection laws. biq acts as the “data controller” for the personal information we collect (meaning we determine how and why that data is processed). If you have any questions about this Policy or our data practices, please contact us as outlined in the “Contact Us” section below.

## Information We Collect

We collect several types of information from and about users of the biq Service. This includes information that you provide directly, information collected automatically when you use the app, and information from device features like location sensors. The **categories of data** we collect include:

- **Account Information:** When you create or update a biq account, we collect personal information such as your **name or nickname** and **email address**. This information is necessary to set up your profile, communicate with you, and personalize your experience. We may also assign you a user ID or similar identifier internally.
- **Location Data:** A core feature of biq is verifying your real-world presence. With your permission, we collect **precise location data** from your mobile device to confirm your proximity to certain places or BLE beacons. This may involve GPS coordinates, Wi-Fi or Bluetooth signal information, device sensor data, and timestamps. We collect location data **only while you are actively using location-based features** (for example, when you check in or when the app is actively verifying presence), or as needed to maintain the Service's intended functionality. You can control the app's access to location services through your device settings; however, note that disabling location access will prevent

you from using biq's core features.

- **Device and Usage Information:** Like many apps, we automatically collect certain information about your device and how you interact with the Service. This may include:
  - **Device identifiers and hardware information** (e.g., your device model, operating system version, unique device ID, and mobile network).
  - **Log and usage data**, such as the dates and times you access the app, features you use, clicks and in-app actions, error logs, and so forth.
  - **IP address** and other device signals which may infer general location (e.g., city or country) when you use the app or website.
  - **Bluetooth data** relevant to the Service's functioning (e.g., detection of specific BLE beacon IDs to verify presence). (Note: We do *not* scan or collect data from your device's other apps or contents; we only use Bluetooth to detect relevant signals for presence verification.)
- **Cookies and Similar Technologies:** If biq has a web interface or if you visit our website, we may use cookies or similar tracking technologies to collect website usage data. This can include your website interactions, preferences, or authentication tokens. (Our primary Service is an app, so cookie use is minimal, but any website tracking will be disclosed in a separate cookie policy if applicable.)
- **Communications:** If you contact us directly (for example, via email support or an in-app help feature), we will collect the information you provide in your correspondence. This may include your name, contact information, and the content of your message. We will use this information to respond to you and improve our support services.

We do **not** collect any sensitive personal information such as government ID numbers, payment card details, or biometric data.

## How We Use Your Information

biq uses the information we collect for the following purposes, all in service of providing you with a functional and improving experience:

- **Providing and Improving the Service:** We use your personal information to **operate biq and deliver core features**. For example, we use your account info to recognize you as a user, and your location data to verify your presence at a given place in order to award digital badges or points. We also use data (like device and usage information) to **maintain and improve the Service's performance**, fix bugs, and develop new features

or enhancements.

- **Account Management and Communication:** Your email address and name are used to **create and manage your account**, and to communicate with you. We will send you service-related communications, such as verification emails (for account setup or password resets), notifications about badge awards or point updates, important security or support messages, and updates about changes to our Terms or Privacy Policy. We **may** also send you promotional communications or newsletters about biq features or events, but **only if you have opted in** to receive them (you can opt out at any time).
- **Location-Based Features:** We use your location data to **verify your IRL presence** and grant corresponding rewards (badges/points). We might also use location information to show you relevant content within the app, such as nearby events or opportunities to earn badges, or to prevent fraud (for example, ensuring that check-ins are genuine and not spoofed).
- **Analytics and Product Development:** We analyze usage and device data (in aggregated and anonymized forms wherever possible) to understand how our users interact with biq. This helps us identify trends, usage patterns, and areas of the Service that need improvement. Analytics also help us **measure the effectiveness** of any notifications or features we introduce, ensuring that biq continues to provide value to users.
- **Safety and Security:** We are committed to keeping biq safe and secure. We may use your information (including logs and certain personal data) to **monitor for and prevent fraud, unauthorized access, cheating, and other misuse** of the Service. For example, we might detect if multiple accounts are suspiciously trying to spoof location and take action under our Terms of Service. We also may use information to **investigate violations** of our Terms or applicable laws, and to cooperate with law enforcement when legally required.
- **Legal Compliance:** Where necessary, we will use and disclose personal information to **comply with our legal obligations**. For instance, to respond to lawful requests by public authorities, court orders, or to meet national security or law enforcement requirements. We may also use your data to enforce our agreements or protect the rights, property, or safety of biq, our users, or others (for example, disclosing information to prevent harm or in the context of an investigation of fraud or security issues).
- **Other Purposes (with Notice/Consent):** If we intend to use your personal information for a purpose that is not outlined in this Policy, we will provide you with specific notice and obtain your consent when required by law. For example, if in the future biq wants to use your data for a new feature or external program, we would let you know and, if necessary, give you the choice to participate.

# Legal Basis for Processing Personal Data (EU/UK Users)

For users in the European Economic Area (EEA), United Kingdom, or other jurisdictions that require a legal justification for processing personal data, biq relies on the following **legal bases**:

- **Consent:** In certain cases, we rely on your consent to process your personal information. For example, we ask for your consent to access precise **location data** via your device's permissions. We also would obtain your consent before sending any marketing or promotional emails. You have the right to withdraw your consent at any time (for example, by disabling location access in your device settings or unsubscribing from marketing communications), but note that withdrawing consent does not affect the lawfulness of processing based on consent before its withdrawal.
- **Performance of a Contract:** We process some personal data because it is **necessary to provide our Service under our contract with you** (the Terms of Service). When you create a biq account and agree to our Terms, a contract is formed. We need to process your data (like your email, name, and location verifications) to fulfill our obligations in that contract – for example, to authenticate you and deliver the features you expect (such as awarding badges for verified presence). Without this data, we couldn't provide the core functionality of biq.
- **Legitimate Interests:** We also process personal data as needed for **legitimate interests** pursued by biq or others, **balanced against your data protection rights**. Our legitimate interests include: maintaining the security of our platform (e.g., preventing fraud or misuse), improving and personalizing the user experience, performing analytics and research about how our Service is used, and communicating with you about product updates or features. When relying on legitimate interests, we ensure that our interests are not overridden by your privacy rights or freedoms – for instance, we might pseudonymize or aggregate data to reduce privacy impact, and you always have the right to object to processing based on legitimate interests (see "Your Rights" below).
- **Legal Obligation:** In some circumstances, we must process personal data to comply with a **legal obligation**. For example, applicable law might require us to retain certain data about your transactions or communications for a fixed period, or we might have to disclose information if compelled by a court order or regulatory authority. In such cases, the law is the basis for processing, and we will only process the data to the extent necessary to meet those obligations.

We will only use your personal data for the purposes for which we collected it (as described above), unless we reasonably consider that we need to use it for another reason that is compatible with the original purpose. If we need to use your personal data for an unrelated purpose, we will notify you and explain the legal basis that allows us to do so, or, if required, request your consent.

# How We Share and Disclose Information

We understand that your personal information is important, and we are careful about how we share it. biq does **not sell** your personal data to third parties for profit or for others' independent marketing purposes. We only share your data in the following circumstances:

- **Service Providers and Partners:** We may share your information with trusted third-party companies that perform services on our behalf, also known as “**data processors**”. These services may include: cloud hosting and data storage (to store and manage data securely), email delivery services (to send you verification or notification emails), analytics services (to help us understand app usage), and customer support tools. These providers are given access to your information only as needed to perform their functions and are contractually obligated to protect it and use it only for our purposes, consistent with this Policy.
- **Decentralized Network Verification:** biq operates as part of a decentralized physical infrastructure network (**DePIN**). This means that verifying your presence might involve interacting with **third-party devices or nodes** in the network (for example, independent BLE beacons or validators). To facilitate this, certain data points necessary for verification may be **broadcast or shared within the network. Importantly, this data is minimized to protect your privacy** – typically it would include anonymized or hashed identifiers and location proof (e.g., cryptographic attestations of your device's presence near a beacon at a certain time), without revealing personal details like your name or email. In simpler terms, other network participants might know that a user was present at X location at Y time (to validate the event), but they won't know it was you specifically, as no directly identifying information is shared. We design the system to prioritize your privacy while still allowing the network to function.
- **Aggregate or De-Identified Data:** We may aggregate or de-identify information so that it can no longer be linked to you personally, and share that aggregated or anonymized data with partners or the public. For example, we might publish statistics about total user participation in certain locations or the growth of the network. This information will **not** contain any personal data and is used to illustrate trends or performance in a privacy-preserving way.
- **Legal Requirements and Safety:** We may disclose your information if required to do so by law or in a good-faith belief that such action is necessary to **(i)** comply with a legal obligation, such as a subpoena, court order, or government demand; **(ii)** protect and defend the rights, property, or safety of biq, our users, or others; **(iii)** investigate or assist in preventing any violation of law or our Terms of Service, including fraud or security issues. If we receive a government or law enforcement request for your data, we will attempt to redirect the request to you or notify you (for example, via the email on your account), unless we are legally prohibited from doing so.

- **Business Transfers:** If biq is involved in a merger, acquisition, financing due diligence, reorganization, bankruptcy, receivership, sale of company assets, or transition of service to another provider, **your information may be transferred as part of such a transaction.** In such cases, we will ensure that the successor entity honors commitments in this Privacy Policy or inform you if any changes to handling of your personal data will occur, giving you the opportunity to opt-out if applicable.
- **With Your Consent:** In situations other than those above, if we want to share your information, we will ask for your consent. For instance, if we ever plan to share your details with a third-party for their own marketing purposes, we would obtain your opt-in consent. You have the right to decline such sharing.

We will never rent or sell your personal information to third-party advertisers or other companies for their independent use without your explicit consent. Any third parties with whom we share data are obligated to use that data in accordance with our instructions and applicable law, ensuring your personal information remains protected.

## Data Retention

biq retains your personal information only for as long as necessary to fulfill the purposes for which it was collected, as described in this Policy, and to comply with applicable legal requirements. This means:

- **Account Data:** We keep your account information (such as your name, email, and profile info, as well as your badge/point history and associated location check-ins) **for as long as your account is active.** If you decide to delete your account or if your account is terminated, we will initiate the process of deleting or anonymizing your personal data from our active databases. In general, account deletion will result in removal of personal identifiers and the dissociation of badges/points from your identity (although we may retain aggregate statistics).
- **Location Data:** Precise location records are kept only as long as needed for the Service. For example, when you verify your presence to earn a badge, we may store that you earned the badge at a certain place and time. However, we do not continuously track your location in the background, and we do not retain raw GPS logs of your every movement beyond what is necessary for the verification events. Historical verification events associated with your account are kept so that you (and we) have a record of your earned badges/points, but if you delete your account, those records will either be deleted or stripped of personal identifiers so they can no longer be linked to you.
- **Usage Data:** Log files and usage data are generally retained for a short period (e.g., a few months) for the purposes of analysis and security. In some cases, we may retain logs for a longer period if we believe it's necessary for security (e.g., investigating a

breach or abuse) or if required for legal reasons. When usage data is kept longer, we typically anonymize or aggregate it so it no longer identifies a user.

- **Communications:** If you contact support or otherwise communicate with us, we may retain those communications for a period of time to ensure we can follow up properly and improve our services (for example, keeping a history of support tickets to reference if you reach out again). These records will be deleted or anonymized when no longer needed.
- **Legal Requirements:** We may need to retain certain information for longer periods if required by law. For instance, if applicable law mandates that we keep certain data for a set time (such as tax or financial records, or data involved in an investigation), we will retain that data as required. Also, if we are in a legal dispute with a user, we may retain relevant information until the issue is resolved.

Once we have no ongoing legitimate business need or legal requirement to retain your personal information, we will delete it or anonymize it. If deletion is not immediately feasible (for example, because the data is stored in secure backups), we will ensure that your data is isolated from further use until deletion is possible.

## Data Security

We take **reasonable and appropriate security measures** to protect the personal information we hold from loss, misuse, unauthorized access, disclosure, alteration, or destruction. These measures include:

- **Encryption:** We use encryption technology to protect data during transmission. For example, any data exchanged between the biq app and our servers is protected using **SSL/TLS encryption**. Where possible, we also encrypt sensitive data at rest on our servers or databases.
- **Access Controls:** We limit access to personal data to authorized employees, contractors, and service providers who need to know that information in order to process it for us. These parties are subject to strict confidentiality obligations. User passwords are stored using strong cryptographic hash functions (we never store plain-text passwords). We also encourage users to choose strong passwords and keep their login credentials confidential.
- **Security Testing and Maintenance:** We regularly monitor our systems for possible vulnerabilities and attacks. Our development practices include security reviews and testing of our code and infrastructure. We may also periodically update you to newer versions of the app to address security updates and encourage you to install those updates promptly.

- **Anonymization/Pseudonymization:** Where feasible, we use techniques to pseudonymize or anonymize personal data, particularly for analytics or when sharing within the decentralized network, to minimize the risk to your privacy in case of any unauthorized access.
- **Incident Response:** In the event of a data breach or security incident, we have procedures in place to respond promptly. If a breach occurs that affects your personal information, we will notify you and the relevant authorities as required by law.

Despite our efforts, please note that **no security measure or modality of data transmission over the Internet is 100% secure**. We cannot guarantee absolute security of your data. It is important for you to also play a role in keeping your information safe. We urge you to **keep your account credentials confidential**, use unique and strong passwords, and notify us immediately if you suspect any unauthorized access to your account. We will not be responsible for breaches of security caused by an individual user's failure to securely safeguard their login credentials or other private information.

## International Data Transfers

biq is a global service. The information we collect from you may be **transferred to, stored in, and processed in** one or more countries outside of your home country, including the United States (where our main servers may be located) or other jurisdictions where our affiliates, service providers, or network participants operate. While data protection laws vary by jurisdiction, we take steps to ensure that your personal information is given **adequate protection** wherever it is processed.

If you are located in the EEA, UK, or other regions with laws governing data collection and use, please note that **your personal data may be transferred to countries which may not provide the same level of data protection as your home country**. In such cases, biq will transfer data only in accordance with applicable data protection law, for example by implementing **Standard Contractual Clauses (SCCs)** or relying on another lawful transfer mechanism (such as your consent or the necessity of the transfer for performing our contract with you).

By using biq, you understand that your information may be transferred to our facilities and those third parties with whom we share it as described in this Policy. We will always handle your personal data in accordance with this Privacy Policy, wherever it is processed.

If you would like more information about our transfer of data or the safeguards we have in place, please contact us (see Contact Us section). We will be happy to address any questions or concerns.

## Your Rights and Choices



You have certain rights and choices regarding your personal information. These rights may vary depending on your jurisdiction, but we are committed to providing you with control over your data. Below is a summary of **common rights** and how you can exercise them:

- **Access Your Information:** You have the right to request access to the personal data we hold about you. This means you can ask us to confirm if we are processing your personal data and request a copy of that data (often called a Subject Access Request).
- **Rectification (Correction):** If any of your personal information is inaccurate or incomplete, you have the right to request that we correct or update it. For example, if you change your email address or realize your name was misspelled, you can update some of this info in-app or ask us to update it.
- **Deletion (Right to be Forgotten):** You have the right to request the deletion of your personal data. If you no longer want biq to have your information, you may delete your account via the app (which triggers deletion of your personal data as described in Data Retention) or contact us to request deletion. We will delete your data unless we have a legal obligation or a compelling legitimate reason to keep it (we will inform you if that's the case). Please note that deleting your data means you will **lose your account, badges, points, and any associated records** permanently.
- **Withdraw Consent:** Where we rely on your consent to process data (e.g., for location services or marketing emails), you have the right to withdraw that consent at any time. You can disable location permissions for biq in your device settings to stop sharing precise location. You can also unsubscribe from marketing emails via the "unsubscribe" link in those emails or by contacting us. Keep in mind, withdrawing consent for location will limit or disable core features of biq (since verifying presence relies on it).
- **Objection to Processing:** You have the right to object to our processing of your personal data in certain circumstances, particularly if we are processing it based on **legitimate interests**. If you object, we will evaluate whether we have compelling legitimate grounds to continue processing (such as security or legal reasons) that override your rights, and we will inform you of our decision. You can also object at any time to the use of your personal data for direct marketing purposes, and we will honor that objection (we do not currently send third-party ads, but if we ever did, you can opt out).
- **Restriction of Processing:** You can ask us to suspend the processing of your personal information in certain scenarios, for example if you contest the accuracy of the data, or you have objected to processing (and we are evaluating the request), or if processing is unlawful and you prefer restriction over deletion. When processing is restricted, we will still store your data but not use it until the issue is resolved.

- **Data Portability:** In some cases, you have the right to request a copy of your personal data in a structured, commonly used, machine-readable format (for example, a CSV file) so that you can transfer it to another service. This generally applies to data you provided us directly and that we process by automated means based on your consent or our contract (such as account information and perhaps your check-in history). We will assist with such requests as required by law.
- **Automated Decision-Making:** biq does not typically make any decisions that have a legal or similarly significant effect on you solely by automated means (without human involvement). If that changes in the future, you would have the right not to be subject to such decisions without your consent or without an opportunity for human review.
- **California Privacy Rights:** If you are a resident of California (USA), you are protected by the California Consumer Privacy Act (CCPA) and subsequent amendments (such as CPRA). In accordance with CCPA, California users have the right to:
  - **Know** the categories of personal information we collect, the sources, and how we use and share it (this Privacy Policy is intended to provide that information). You also have the right to know the specific pieces of personal data we have collected about you (which is similar to the access right above).
  - **Request Deletion** of your personal information (with similar limitations and processes as the deletion right mentioned above).
  - **Opt-Out of Sale or Sharing** of personal information. Note: biq does **not sell** personal data, and we do not share personal data with third parties for cross-context behavioral advertising. If that ever changes, we will implement a formal opt-out mechanism and update this Policy.
  - **Non-Discrimination:** You have the right not to receive discriminatory treatment for exercising your CCPA rights. biq will not deny you service, charge you a different price, or provide a lesser experience because you exercised any of your privacy rights.  
 If you are a California resident and would like to exercise any of these rights, please contact us via the methods below. We will need to verify your identity (such as by confirming information associated with your account) before fulfilling certain requests.

To exercise any of your rights listed above, please **contact us** using the information provided in the Contact Us section. We will respond to your request as soon as reasonably possible, and in any event within any timeframes required by law (for example, under GDPR we generally have one month to respond, which can be extended in complex cases). Please note: for your protection, we may take steps to verify your identity before providing access to your personal

data or making corrections/deletions. This is to ensure that we do not grant rights to the wrong person.

Also, you have the **right to lodge a complaint** with a data protection authority if you believe that our processing of your personal information violates the law. For example, if you are in the European Union, you can contact the supervisory authority in your EU member state. We encourage you to contact us first, so we have an opportunity to address your concerns directly.

## Children's Privacy

As stated in our Terms of Service, biq is **not intended for children under the age of 13**. We do not knowingly collect or solicit personal information from anyone under 13. If you are under 13, please do not attempt to register for biq or send any personal information about yourself to us. If we learn that we have collected personal information from a child under 13, we will delete that information promptly and terminate the child's account.

If you are a parent or guardian and discover that your child under 13 has created an account or otherwise provided personal data to biq without your consent, please contact us immediately so that we can take appropriate action, including deleting the child's information from our systems.

For minors aged 13 to 17: We expect such users to only use biq with parental permission and under supervision, where required by law. Some countries have higher age thresholds (for example, 16 years in certain jurisdictions for consent to process personal data). We will adhere to those requirements as applicable. If you are under the age of majority in your region, you should review this Privacy Policy with your parent or guardian to make sure you both understand it, and you should only use the Service if you have their consent.

## Changes to This Privacy Policy

We may update or revise this Privacy Policy from time to time to reflect changes in our practices, technologies, legal requirements, or other factors. When we make changes, we will update the **"Effective Date"** at the top of this Policy. If we make any significant or material changes, we will take additional steps to notify you: for example, by sending a notice to the email address associated with your account, or by displaying an in-app notification or alerting you upon your next login.

We encourage you to **review this Privacy Policy periodically** to stay informed about how we are protecting your information. Your continued use of biq after any update to this Privacy Policy will constitute your acceptance of the changes, to the extent permitted by law. If you do not agree with any updates or changes, you should stop using the Service and, if applicable, delete your account.

## Contact Us

If you have any questions, concerns, or requests regarding this Privacy Policy or your personal data, please do not hesitate to contact us. We are here to help.

- **Email:** You can reach our team at **connect@biq.me**. This is the preferred and fastest way to reach us for privacy-related inquiries or to exercise your data rights.
- **In-App Support:** You may also find support contact options within the biq app under “Settings” or “Help” if available.

We will endeavor to respond to all legitimate requests or questions as promptly as possible, and at minimum within any timeframe required by applicable law. Your privacy and trust are important to us, and we will do our best to address any issues you have with how we handle your data.

Thank you for reading our Privacy Policy. By keeping you informed of our data practices, we hope to ensure you feel confident using biq and participating in our community, knowing that your personal information is respected and protected.