Quiba Privacy Policy

This privacy policy has been compiled to better serve those who are concerned with how their 'Personally Identifiable Information' (PII) is being used online. PII, as described in US privacy law and information security, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

In EU law it is defined as any information relating to an identified or identifiable natural person directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Please read our privacy policy carefully to get a clear understanding of how we collect, use, protect or otherwise handle your Personally Identifiable.

What personal information do we collect from the users of our app?

As a user, you need to have a Google or Apple account in order to buy the license and use our app. There is no further need to enter any other personal information directly into our app, as you do not log in to our app, nor our servers.

Quiba app allows the user to store bookmarks and notes locally on your device. We do not have access to your bookmarks and personal notes and we do not transfer any data you insert over internet and/or to our servers. Quiba app is not Cloud based.

Quiba app and its developers do not form and process any identifiable app user databases.

When contacting us through the app under the “contact” section user will be asked to enter your email address or other details to help you with your experience.

It is not excluded, that with the updates of the app user may be asked to enter email address or other details to help you with your experience when ordering or registering on our app.

Bookmarks and Personal notes

As described above, Quiba app allows the user to store bookmarks and notes. This information is only stored locally on the device and we cannot access them.

However, as bookmarks and notes can be considered as PII, especially in cases when the user of the app would put down in notes information about himself, patients and/or treatments, we stress that is important that the user of the app respects all legal requirements about personal data.

Under the EU law processing of personal data concerning one’s health may only be done if:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes,
it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services provided that those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy.

**How do we use your information?**
The app uses the information about your bookmarks to personalize your experience and to allow the app to deliver the type of content, which you chose is the most interested.

We use your email information to reply to you in order to service you in responding to your customer requests.

**How do we protect your information?**
We do not use vulnerability scanning and/or scanning to PCI standards.
We only provide information. We never ask for credit card numbers.
We use regular Malware Scanning.

In a case any of your personal information would be collected it will be contained behind secured networks and is only accessible by a limited number of persons who have special access rights to such systems, and are required to keep the information confidential. In addition, all sensitive/credit information you supply is encrypted via Secure Socket Layer (SSL) technology.

In a case any of your personal information would be collected we will implement a variety of security measures.

All transactions are processed through a gateway provider and are not stored or processed on our servers.

**Data protection by design and by default**
The controller shall implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of EU law users.

The controller shall to his best knowledge and with utmost care and resources implement appropriate technical and organisational measures for ensuring that, by default, only personal data, which are necessary for each specific purpose of the processing, are processed.

In case the app would store any other information or data about the user outside the scope of the Privacy policy disclosure, the request for consent shall be presented in a manner, which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language and the user shall have the right to withdraw his or her consent at any time. Prior to giving consent, the data subject shall be informed thereof.
Right to erasure (‘right to be forgotten’)
User shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;
- the personal data have been or still are unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation;
- other legal reasons as defined by EU or national law.

Do we use 'cookies’?
We do not use cookies for tracking purposes.

Third-party disclosure
We do not sell, trade, or otherwise transfer to outside parties any Personally Identifiable Information unless we provide users with advance notice.

However, non-personally identifiable visitor information may be provided to other parties for marketing, advertising, or other uses.

Third-party links
We do not include or offer third-party products or services on our website.

Google
We have not enabled Google AdSense on our app but we may do so in the future.

In case that happens Google’s advertising requirements can be summed up by Google’s Advertising Principles. They are put in place to provide a positive experience for users. https://support.google.com/adwordspolicy/answer/1316548?hl=en

California Online Privacy Protection Act
CalOPPA is the first state law in USA to require commercial websites and online services to post a privacy policy. The law’s reach stretches well beyond California to require any person or company in the United States (and conceivably the world) that operates websites collecting Personally Identifiable Information from California consumers to post a conspicuous privacy policy on its website stating exactly the information being collected and those individuals or companies with whom it is being shared. - See more at: http://consumercal.org/california-online-privacy-protection-act-caloppa/#sthash.0FdRbT51.dpuf

According to CalOPPA, we agree to the following:
Users can use our app anonymously – we do not have a database of our users as users pay the right to use the application trough Google Play or Apple App Store.

Our Privacy Policy link includes the word 'Privacy' and can easily be found on the “Information” tab in the app.
You will be notified of any Privacy Policy changes:
• On our Privacy Policy Page in in "Information" tab in the App

You can change your personal information that you disclosed to us:
• By emailing us

**How does our app handle Do Not Track signals?**
We honor Do Not Track signals and do not track, plant cookies, or use advertising when a Do Not Track (DNT) browser mechanism is in place.

**Does our app allow third-party behavioral tracking?**
We do not allow third-party behavioral tracking when using our app.

**COPPA (Children Online Privacy Protection Act)**
When it comes to the collection of personal information from children under the age of 13 years old, the Children's Online Privacy Protection Act (COPPA) puts parents in control. The Federal Trade Commission, United States' consumer protection agency, enforces the COPPA Rule, which spells out what operators of websites and online services must do to protect children's privacy and safety online.

We do not specifically market and/or service directly to children under the age of 13 years old.

**Fair Information Practices**
The Fair Information Practices Principles form the backbone of privacy law in the United States and the concepts they include have played a significant role in the development of data protection laws around the globe. Understanding the Fair Information Practice Principles and how they should be implemented is critical to comply with the various privacy laws that protect personal information.

**In order to be in line with Fair Information Practices we will take the following responsive action, should a data breach occur:**
- We will notify the users via in-app notification without undue delay and, where feasible, not later than 72 hours after having become aware of it.

We also agree to the Individual Redress Principle which requires that individuals have the right to legally pursue enforceable rights against data collectors and processors who fail to adhere to the law. This principle requires not only that individuals have enforceable rights against data users, but also that individuals have recourse to courts or government agencies to investigate and/or prosecute non-compliance by data processors.
**CAN SPAM Act**
The CAN-SPAM Act is a law that sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have emails stopped from being sent to them, and spells out tough penalties for violations.

**We store your email address in order to:**
- Send information, respond to inquiries, and/or other requests or questions

**To be in accordance with CANSPAM, we agree to the following:**
- Not use false or misleading subjects or email addresses.
- Identify the message as an advertisement in some reasonable way.
- Include the physical address of our business or site headquarters.
- Monitor third-party email marketing services for compliance, if one is used.
- Honor opt-out/unsubscribe requests quickly.
- Allow users to unsubscribe by using the link at the bottom of each email.

If at any time you would like to unsubscribe from receiving future emails, you can email us at quiba@transatlanticpharma.biz and we will promptly remove you from ALL correspondence.

**Contact Us**
If there are any questions regarding this privacy policy, you may contact us using the information below.

Quiba
Transatlantic Pharma Inc.
4216 Cravens Point Rd
Wilmington, NC 28409
United States
quiba@transatlanticpharma.biz