QUIXXS Privacy Policy

Privacy Policy

AMNEXIS HOLDING Ltd, trading as QUIXXS, ("**us**", "**we**", or "**our**") operate the QUIXXS app (the "**App**") and the QUIXXS web application, ("**Services**").

This privacy policy, ("**Privacy Policy**") together with our Terms of Use, https://amnexis.com/quixxslegals/, applies to your use of the App.

This Privacy Policy together with our Terms and Conditions, https://amnexis.com/quixxslegals/, applies to your use of the Services.

The App is made available for download onto your mobile telephone or handheld device ("**Device**") from the App Store – Apple, or the Google Play Store, ("**App Site**").

You can register to use the Services at https://QUIXXS.com, ("**Services Site**").

Please note:

All patient data (including their personal data) collected via your use of the App or Services is governed by your organisation's own privacy policy. Such patient data is processed by us pursuant to the Terms and Conditions entered into with your organization and in accordance with the provision of our data processing agreement, as your organisation's data processor. Patient data is not covered by the terms of this Privacy Policy.The App, the App Site and the Services Site are not intended for children and we do not knowingly collect data relating to children.

Please read the following carefully to understand our practices regarding your personal data and how we will treat it.

1. Data Controller

For the purposes of EU and UK data protection laws and any applicable national implementing laws, regulations and secondary legislation relating to the processing of personal data (together "**Data Protection Law**"), QUIXXS is the data controller of all data collected and processed when using the App pursuant to this Privacy Policy.

2. Data Protection Officer

We have appointed a data protection officer ("**DPO**") who is responsible for overseeing questions about this Privacy Policy who can be contacted as set out at the end of this Privacy Policy**.**

3. Personal data we may collect about you

We may collect, use, store and transfer different kinds of personal data about you as follows:

Description of categories of personal data

- **Identity Data**: first name, last name, username or similar identifier, marital status, title, date of birth, gender.
- **Contact Data**: work address, email address and telephone numbers.
- **Financial Data**: bank account and payment card details.
- **Transaction Data**: includes details about payments to and from you and details of in-App purchases.
- **Device Data:** includes the type of mobile device you use, a unique device identifier for example, your Device's IMEI number, the MAC address of the Device's wireless network

interface, or the mobile phone number used by the Device, mobile network information, your mobile operating system, the type of mobile browser you use and time zone setting.

- **Profile Data**: includes your username and password, in-App purchase history, your interests, preferences, feedback and survey responses.
- **Usage Data**: includes details of your use of the App, but not limited to, traffic data and other communication data, whether this is required for our own billing purposes or otherwise and the resources that you access.
- **Marketing and Communications Data**: includes your preferences in receiving marketing from us and our third parties and your communication preferences.
- **Location Data**: includes your current location disclosed by GPS technology.

We also collect, use and share Aggregated Data such as statistical or demographic data for any purpose. Aggregated Data could be derived from your personal data but is not considered personal data in law as this data will not directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific App feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this Privacy Policy.

We do not collect any special categories of personal data about you (this means details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health, and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

Like many apps, we may request permission to use or access features or hardware on your device. For example the use of your camera or files when you create your profile image. You may allow or remove these permissions at any time, however, you may not be able to use some portions of our App where these permissions are required.

4. How is your personal data collected?

We will collect and process the following data about you:

- **Information you give us.** This is information (including Identity, Contact, Financial, and Marketing and Communications Data) you consent to giving us about you by filling in any registration form on the App site and the Services site (together **Our Sites**), or by corresponding with us (for example, by email or chat). It includes information you provide when you register to use the App, download or register an App, subscribe to any of our Services, search for an App or Service, make an in-App purchase, enter a competition, promotion or survey, or when you report a problem with an App, our Services, or any of Our Sites. If you contact us, we will keep a record of that correspondence.
- **Information we collect about you and your Device.** Each time you visit one of Our Sites or use the App we will automatically collect personal data including Device, Content and Usage Data. We collect this data using cookies and other similar technologies. Please see our cookie policy https://amnexis.com/cookie-policy/ for further details.
- **Location Data.** We also use GPS technology to determine your current location. Some of our location-enabled services require your personal data for the feature to work. If you wish to use the particular feature, you will be asked to consent to your data being used for this purpose. You can withdraw your consent at any time by disabling Location Data in your settings.

5. If you fail to provide personal data

Where we need to collect personal data by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with goods or services). In this case, we

may have to cancel a product or service you have with us but we will notify you if this is the case at the time.

6. Information we receive from other sources

We work closely with the third parties set out in our Third Party Supplier List, https://amnexis.com/quixxslegals/, which includes, for example, business partners, sub-contractors in technical, payment and delivery services, advertising networks, analytics providers, search information providers, credit reference agencies and we may receive the following personal data about you from them:

- **Device Data:**
  from analytics providers, advertising networks and search information providers.

- **Contact, Transaction and Financial Data:**
  from providers of technical, payment and delivery services.

- **Identity and Contact Data:**
  from providers of chat/communication/helpdesk services with customers including via email.

- **Email Communications and Contact Data:**
  from providers of email communications service providers.

- **Business Contact and Financial Data:**
  from CRM service providers who manage contacts and keep a record of communications/ interactions with customers.

- **Contact Data and Financial Data:**
  from cloud accounting systems that store email and names of persons sent invoices by email.

7. Cookies

We use cookies and/or other tracking technologies to distinguish you from other users of the App or Our Sites and to remember your preferences. This helps us to provide you with a good experience when you use the App or browse any of Our Sites and also allows us to improve the App and Our Sites. For detailed information on the cookies we use, the purposes for which we use them and how you can exercise your choices regarding our use of your cookies, see our Cookie Policy., https://www.amnexis.com/cookie-policy/

You can set up your browser options, to stop your computer accepting cookies or to prompt you before accepting a cookie from the websites you visit. If you do not accept cookies, however, you may not be able to use the whole of Our Sites or all functionality of the Services.

To find out more about cookies, including how to see what cookies have been set and how to manage and delete them, visit www.allaboutcookies.org. To opt out of being tracked by Google Analytics across all websites visit http://tools.google.com/dlpage/gaoptout.

8. Pixel-Tags

We may use "pixel tags," which are small graphic files that allow us to monitor the use of the App and Our Sites. A pixel tag can collect information such as the IP (Internet Protocol) address of the computer that downloaded the page on which the tag appears; the URL (Uniform Resource Locator) of the page on which the pixel tag appears; the time the page containing the pixel tag was viewed; the type of browser that fetched the pixel tag; and the identification number of any cookie on the computer previously placed by that server. When corresponding with you via HTML capable e-mail, we may use "format sensing" technology, which allows pixel tags to let us know whether you received and opened our e-mail.

9. Web Beacons

Some of our web pages may contain electronic images known as web beacons (sometimes known as clear gifs) that allow us to count users who have visited these pages. Web beacons collect only limited information which includes a cookie number; time and date of a page view; and a description of the page on which the web beacon resides. We may also carry web beacons placed by third party advertisers. These web beacons do not carry any personal data and are only used to track the effectiveness of a particular campaign.

Do not track

We do not support Do Not Track ("**DNT**").

Do Not Track is a preference you can set in your web browser to inform websites that you do not want to be tracked. You can enable or disable Do Not Track by visiting the "Preferences" or "Settings" page of your web browser.

10. How we use your personal data

We will only use your personal data when the law allows us to do so. Most commonly we will use your personal data in the following circumstances:

- Where you have consented before the processing.
- Where we need to perform a contract we are about to enter or have entered with you.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where we need to comply with a legal or regulatory obligation.

We will only send you direct marketing communications by email or text if we have your consent. You have the right to withdraw that consent at any time by contacting us.

We will get your express opt-in consent before we share your personal data with any third party for marketing purposes.

Purposes for which we will use your personal data

Purpose/activity	**Type of data**	**Lawful basis for processing**
To install the App and register you as a new App user or customer	Identity Contact Financial Device	Your consent
To process your orders and deliver Services including managing payments and collecting money owed to us	Identity Contact Financial Transaction Device Marketing and Communications Location	Your consent Performance of a contract with you Necessary for our legitimate interests (to recover debts due to us)
To manage our relationship with you including notifying you of	Identity	Your consent

changes to the App, Services our Terms of Use, this Privacy Policy or our Terms and Conditions, dealing with your requests, complaints and queries.	Contact Financial Profile Marketing and Communications	Performance of a contract with you Necessary for our legitimate interests (to keep records updated and to analyse how customers use our products/ Services) Necessary to comply with legal obligations (to inform you of any changes to our terms and conditions)
To enable you to participate in a prize draw, competition or complete a survey	Identity Contact Device Profile Marketing and Communications	Your consent Performance of a contract with you Necessary for our legitimate interests (to analyse how you use our products/Services and to develop them and grow our business)
To administer and protect our business and this App or the Services, including troubleshooting, data analysis, testing, system maintenance, support updates, reporting and hosting of data.	Identity Contact Device	Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security)
To deliver relevant App and Services content and online advertisements to you. To make recommendations to you about goods or services which may interest you To measure and analyse the effectiveness of the advertising we serve you To monitor trends so we can improve the App. To use data analytics to improve our App and Services, customer relationships and experiences.	Identity Contact Device Content Profile Usage Marketing and Communications Location	Consent Necessary for our legitimate interests (to develop our products/Services and grow our business)

We will not sell or rent your personal data to anyone.

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original

purpose. If you wish to obtain an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

11. Disclosures of your personal data

Personal data we share with third parties

We may share your personal data where necessary with the third parties set out in our Third Party Supplier List, https://amnexis.com/quixxslegals/, for the purposes set out in the table above. Below is a summary of the types of third parties used:

- Any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.
- Business partners, suppliers and sub-contractors for the performance of any contract we enter into with them or you to provide services such as IT and system administration services, email communications, hosting services, backup services, credit card processing, research, development, marketing and customer support.
- Analytics and search engine providers that assist us in the improvement and optimisation of our App and Services.
- Professional advisors acting as service providers to us in relation to Our Sites or Services - including lawyers, bankers, auditors, and insurers who provide consultancy, banking, legal, insurance and accounting services.
- Tax authorities, regulators and other authorities who require reporting of processing activities in certain circumstances.
- Advertisers and advertising networks that require the data to select and serve relevant adverts to you and others. We do not disclose personal data about identifiable individuals to our advertisers, but we may provide them with Aggregated Data about our users. We may also use such Aggregated Data to help advertisers reach the kind of audience they want to target (for example, women living in London). We may make use of the personal data we have collected from you to enable us to comply with our advertisers' wishes by displaying their advertisement to that target audience.
- Credit reference agencies for the purpose of assessing your credit score where this is a condition of us entering into a contract with you.

Personal data we disclose to third parties

We may disclose your personal data where necessary to third parties:

- In the event that we sell or buy any business or assets, in which case we may disclose your personal data to the prospective seller or buyer of such business or assets.
- If we or a member of our group of companies or substantially all of their assets are acquired by a third party, in which case personal data held by them about their customers will be one of the transferred assets.
- If we are under a duty to disclose or share your personal data in order to comply with any legal obligation, or in order to enforce or apply our terms and conditions, terms of use and/or any other legal agreements; or to protect our rights, property, safety, our customers or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.
- Including Aggregated Data in the normal course of operating our business; for example, with other App or Services users, our customers or publicly to show trends or benchmark the general use of App and Services.

We require all third parties to respect the security of your personal data and to treat it in accordance with applicable law. We do not allow our third-party service providers to use your personal data for

their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

12. International Transfers

Some of our external third parties are based outside the UK so their processing of your personal data will involve a transfer of data outside the UK.

This may involve transferring personal data outside your country of residence to countries which have laws that do not provide the same level of data protection as your country of residence. When we share your personal data with our service providers, who are identified in our Third Party Supplier List, this will involve transferring your personal data to the country set out in the Third Party Supplier List for each service provider.

13. European Data

When we transfer UK, EU or Swiss personal data to countries whose laws do not provide the same level of data protection as the UK, the EU or Switzerland, we always ensure that a similar degree of protection is afforded to your data by ensuring that one of the following applicable safeguards is in place:

- We will only transfer UK personal data outside of the UK to: (i) countries deemed by the ICO to provide an adequate level of protection for UK personal data; or (ii) entities located outside of the UK with whom standard contractual terms approved for use in the UK which give the transferred personal data the same protection as it has in the UK have been entered into, for example the International Data Transfer Addendum, (IDTA) to the European Commission's standard contractual clauses for international data transfers or binding corporate rules (BCRs); or (iii) entities located in the USA certified under the UK Extension to the EU-U.S. DPF; or (iv) any entity located outside of the UK that is subject to any other transfer mechanism, bespoke contract, approved code of conduct or certification scheme approved by the ICO.

- We will only transfer EU personal data outside of the EEA to: (i) countries deemed by the European Commission to provide an adequate level of protection for EU personal data; or (ii) entities located outside of the EEA with whom standard contractual terms approved for use in the EU which give the transferred personal data the same protection as it has in the EU have been entered into, for example the European Commission's standard contractual clauses for international data transfers, (EU SCCs) or binding corporate rules (BCRs); or (iii) entities located in the USA certified under the EU-U.S. DPF; or (iv) any entity located outside of the EEA that is subject to any other transfer mechanism, bespoke contract, approved code of conduct or certification scheme approved by the European Commission.

- We will only transfer Swiss personal data outside of Switzerland to: (i) countries deemed by the Swiss Data Protection Authority to provide an adequate level of protection for Swiss personal data; or (ii) entities located outside of Switzerland with whom standard contractual terms approved for use in Switzerland which give the transferred personal data the same protection as it has in Switzerland have been entered into, for example the European Commission's standard contractual clauses for international data transfers, (EU SCCs) or binding corporate rules (BCRs); or (iii) entities located in the USA certified under the Swiss-U.S. DPF; or (iv) any entity located outside of Switzerland that is subject to any other transfer mechanism, bespoke contract, approved code of conduct or certification scheme approved by the Swiss Data Protection Authority.

14. Data security

All information you provide to us is stored on our secure servers. Any payment transactions carried out by us or our chosen third-party provider of payment processing services will be encrypted. Where we have given you (or where you have chosen) a password that enables you to access the App or certain parts of Our Sites, you are responsible for keeping this password confidential. We ask you not to share a password with anyone.

Once we have received your information, we will use strict procedures and security features to try to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way.

We will collect and store personal data on your Device using application data caches and browser web storage (including HTML5) and other technology.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator when we are legally required to do so.

15. Data retention

We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected if for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint, if we reasonably believe there is a prospect of litigation in respect of our relationship with you, to comply with law enforcement requests, maintain security, prevent fraud and abuse, resolve disputes, enforce our legal agreements, or fulfil your request to “unsubscribe” from further messages from us.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements. Usually this will be for as long as we provide access to the App or Our Site to you, your account with us remains open or any period set out in any relevant contract you have with us.

By law we have to keep basic information about our customers (including Contact Data, Identity Data, Financial Data and Transaction Data) for 6 years after they cease being customers for tax purposes.

In some circumstances we will anonymise your personal data (so that it can no longer be associated with your) after your account has been closed and we may use this for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

In some circumstances you can ask us to delete your data: see Your Legal Rights below for further information.

You may choose to delete your account at any time from your profile screen. We will archive your account for 30 days. Only during this period will it be possible to restore your account. After 30 days it is deleted forever.

In some circumstances we will anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

In the event that you do not use the App or Our Sites for a period of 12 months then we will treat the account as expired and your personal data may be deleted.

16. Your legal rights

You have a number of rights under Data Protection Law in relation to your personal data. You have the right to:

- Request access to your personal data (commonly known as a “subject access request”). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- Request rectification of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
- Request erasure of your personal data in certain circumstances. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have

processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

- Request restriction of the processing of your personal data. This enables you to ask us to suspend the processing of your personal data in one of the following scenarios: (i) if you want us to establish the data's accuracy; (ii) where our use of the data is unlawful but you do not want us to erase it; (iii) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (iv) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
- Object to the processing of your personal data where we are relying on a legitimate interest (or those of a third party) as the legal basis for that particular use of your data (including carrying out profiling based on our legitimate interests). In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your right to object.
- Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.
- Object any time to the processing of your personal data for direct marketing purposes.
- Withdraw consent at any time where we are relying on consent to process your personal data as the legal basis for using your data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

If you wish to exercise any of the above rights, please contact us as set out at the end of this Privacy Policy.

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

We will try to respond to all legitimate requests within 30 days and will deal with requests we receive from you, in accordance with the provisions of Data Protection Law. Occasionally it could take us longer, if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

17. Marketing Communications

We may use your Identity, Contact, Device, Usage and Profile Data to form a view on which products, services and offers may be of interest to you so that we can send you relevant marketing communications.

Direct marketing: You will receive marketing communications if you "opt in" to receive marketing communications from us when you registered on our App or Our Sites, or if you enquired about, or have purchased any of our goods or services and you have not opted out of receiving such marketing.

Third Party Marketing: We will obtain your express opt-in consent before we share your personal data with any third party for their own direct marketing purposes.

Opting out of Marketing: You can ask us to stop sending you marketing communications at any time by logging into the App or Our Sites and unchecking the relevant boxes to adjust your marketing

preferences or by following the “opt out” or “unsubscribe” links within any marketing communication sent to you.

Once you “opt out” or “unsubscribe”, you will no longer receive any marketing communications from us. You will however still received service related communications that are essential for administrative or customer service purposes, for example relating to orders, billing, updates, checking that your contact details are up to date and support issues.

Please note that where we send push notifications from time to time in order to update you about any service updates, events and promotions we may be running, if you no longer wish to receive these communications, please disable these in the settings on your device.

18. Complaints

Our intention is to meet the highest standards when collecting and using personal data. For this reason, we take complaints we receive very seriously. We encourage users to notify us if they think that our collection or use of personal data is unfair, misleading or inappropriate. If you have any complaints about our use of your personal data, please contact us as set out at the end of this Privacy Policy or you have the right to make a complaint to your local data protection supervisory authority.

For UK individuals:
The Information Commissioner’s Office at, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, England.

19. Age of Users

The App and Our Sites are not intended for and shall not be used by anyone under the age of 18.

20. Contact Us

If you have any questions about this Privacy Policy or about your personal data, please contact Dr. Marcus Fedder, our DPO using the details set out below.

- By post: Amnexis Holding Ltd (trading as QUIXXS), Guinness Enterprise Centre, Taylor’s Lane, Dublin 8, Ireland.
- By email: DPO@amnexis.com

21. Changes to this Privacy Policy and your duty to inform us of changes

We keep our Privacy Policy under regular review.

This version was last updated on 20th of November 2024. It may change and if it does, these changes will be posted on this page and, where appropriate, notified to you by SMS or by email or when you next start the App. The new Privacy Policy may be displayed on-screen and you may be required to read and accept the changes to continue your use of the App.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during our relationship with you.

22. Third Party Supplier List

Please refer to: https://amnexis.com/quixxslegals/