Assuric
Assisted Document

Privacy Notice (Users)

Organisation: Augmentia
Issue Date: Aug 3, 2025
Document Owner: Alex Radcliffe

Document Version Control

Version	Date	Description	Author	Approver

Privacy Notice

This Privacy Notice describes the organisation's policies and procedures on the collection, use and disclosure of personal data and informs users about privacy rights and how the law protects individual rights and freedoms.

Contents

Privacy Notice

This Privacy Notice gives you information about how Augmentia collects and uses your personal data through your use of our app and when you communicate with us in any way, including any data you may provide when you sign up and use our services.

Who we are and how to contact us

Augmentia is the controller and responsible for your personal data (collectively referred to as, "we", "us" or "our" in this Privacy Notice). Augmentiais a company registered in England and Wales with company number 15010967 with its registered office at 20 Wenlock Road London N1 7GU.
If you would like to contact us about anything in this Privacy Notice, or if you have any questions about how we use your information or if you would like to exercise any of your data subject rights, please contact us here:
dpo@augmentia.ai

The types of personal data we collect about all the users of our app

Personal data means any information about an individual from which that person can be identified.
We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

- **Identity Data** includes Email address, first name, last name, date of birth, gender, DIN, title.
- **Contact Data** includes phone numbers, email addresses, billing addresses, and telephone numbers..
- **Transaction Data** includes details about payments to and from you and other details of products and services you have purchased from us.
- **Technical Data** includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, device ID and other technology on the devices you use to access this website, as well as on the devices running our desktop client, which also includes session information and metadata (log in times & durations).
- **Profile Data** includes your username and password, purchases or orders made by you, your interests, preferences, feedback and survey responses.
- **Usage Data** includes information about how you interact with and use our website, products and services.
- **Marketing and Communications Data** includes your preferences in receiving marketing from us and our third parties and your communication preferences.
- **Health Data** includes any data about your health that you share with us when you express interest in, sign up for, and/or use our services.

We also collect, use and share **anonymised aggregated data** such as statistical or demographic data which is not personal data as it does not directly (or indirectly) reveal your identity. For example, we may use this anonymised data for the purposes of helping us build evidence to justify formal clinical trials and feasibility studies in a clinical setting, or for internal research and product development, including product development involving machine learning and big data analysis, or for future publications.

1.0 How is your personal data collected?

We use different methods to collect data from and about you including through:

- **Your interactions with us.** You may give us your personal data by signing up to use the app, filling in online forms or by corresponding with us by post, phone, email or otherwise. This includes personal data, you provide when you:
  - create an account to use the Augmentiaapp;
  - sign in to use the Augmentiaapp
  - subscribe to our newsletters or publications;
  - request marketing to be sent to you;
  - enter a competition, promotion or survey; or
  - give us feedback or contact us.
- **Automated technologies or interactions.** As you interact with our app, we will automatically collect Technical Data about your equipment, browsing actions and patterns.

2.0 How we use your personal data

2.1 Legal basis

The law requires us to have a legal basis for collecting and using your personal data. We rely on one or more of the following legal bases:

- **Performance of a contract with you:** Where we need to perform the contract we are about to enter into or have entered into with you.
- **Legitimate interests:** We may use your personal data where it is necessary to conduct our business and pursue our legitimate interests, for example to prevent fraud and enable us to give you the best and most secure customer experience. We make sure we consider and balance any potential impact on you and your rights (both positive and negative) before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law).
- **Legal obligation:** We may use your personal data where it is necessary for compliance with a legal obligation that we are subject to. We will identify the relevant legal obligation when we rely on this legal basis.
- **Consent:** We rely on consent only where we have obtained your active agreement to use your personal data for a specified purpose.

2.2 Purposes for which we will use your personal data

We have set out below, in a table format, a description of all the ways we plan to use the various categories of your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Purpose/Use	Type of data	Legal basis
To register you as a new user	(a) Identity (b) Contact	Performance of a contract with you
To identify the payments you have made to us, any refunds you may be due, and to identify the products or services you have purchased from us	(a) Transaction Data	Performance of a contract with you
To process and deliver our services to you: (b) Provide you with most accurate educational and supportive materials	(a) Identity	Performance of a contract with you
To manage our relationship with you which will include: (a) Notifying you about changes to our terms or Privacy Notice (b) Dealing with your requests, complaints and queries	(a) Identity (b) Contact (c) Profile (d) Marketing and Communications	(a) Performance of a contract with you (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our records updated and manage our relationship with you)
To enable you to complete a survey	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications	(a) Necessary for our legitimate interests (to study how customers use our products/services, to develop them and grow our business) (b) Consent
To administer and protect our business and this app (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise) (b) Necessary to comply with a legal obligation
To deliver relevant app content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications (f) Technical	Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)
To use data analytics to improve our website, products/services, customer relationships and experiences and to measure the effectiveness of our communications and marketing	(a) Technical (b) Usage	Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)
To send you relevant marketing communications and make personalised suggestions and recommendations to you about goods or services that may be of interest to you based on your Profile Data	(a) Identity (b) Contact (c) Technical (d) Usage (e) Profile (f) Marketing and Communications	Consent, having obtained your prior consent to receiving direct marketing communications
To carry out market research through your voluntary participation in surveys	(a) Identity (b) Contact (c) Technical (d) Usage (e) Profile	Necessary for our legitimate interests (to study how customers use our products/services and to help us improve and develop our products and services).
To provide you with a method of recording and reporting your symptoms whilst you are using our services	(a) Identity (b) Contact (c) Profile	(a) Performance of a contract with you
To provide you with the most relevant educational and informational content.	(a) Identity (b) Contact (c) Profile	(a) Performance of a contract with you

2.2.1 Augmentia as a data processor:

Augmentia acts as a data processor when processing user data which means we only process user data according to the instructions of the data controller – the organisations providing care, such as GP practices, PCNs. They maintain the overall responsibility for user data and the circumstances of any processing. As such, Augmentiais acting under the instructions of the user's organisation (the data controller they determine the lawful basis for processing. In most cases the organisation relies on:

- Article 6 (1) (e) of the GDPR, – processing personal information that is necessary to provide a service which is in the public interest

2.3 Direct marketing

We may use Your Personal Data to contact You with newsletters, marketing or promotional materials and other information that may be of interest to You. You may opt-out of receiving any, or all, of these communications from Us by following the unsubscribe link or instructions provided in any email We send or by contacting Us at dpo@augmentia.ai.

2.4 Third-party marketing

We will get your express consent before we share your personal data with any third party for their own direct marketing purposes.

2.5 Opting out of marketing

You can ask to stop sending you marketing communications at any time by following the opt-out links within any marketing communication sent to you or by contacting us at dpo@augmentia.ai.
If you opt out of receiving marketing communications, you will still receive service-related communications that are essential for administrative or customer service purposes.

2.6 Cookies

For more information about the cookies we use and how to change your cookie preferences, please see our Cookies Policy

3.0 Disclosures of your personal data

We may share your personal data where necessary with external third parties who provide services to us, e.g: cloud service providers and technology services, or clinical research organisations. We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We have Data Processing Agreements in place with these third party providers and 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. We do not sell your data to anyone and only share it with our contracted processors.
Augmentia processes personal data in the capacity of both a data controller and a data processor. When we are a processor of personal data, we are doing so purely on the instructions of another organisation or company as they are the controller.

3.1 Business Transactions

If the Company is involved in a merger, acquisition or asset sale, Your Personal Data may be transferred. Alternatively, we may seek to acquire other businesses or merge with them. We will provide notice before Your Personal Data is transferred and becomes subject to a different Privacy Policy.

3.2 Law enforcement

Under certain circumstances, the Company may be required to disclose Your Personal Data if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency).

3.3 Other legal requirements

The Company may disclose Your Personal Data in the good faith belief that such action is necessary to:

- Comply with a legal obligation
- Protect and defend the rights or property of the Company
- Prevent or investigate possible wrongdoing in connection with the Service
- Protect the personal safety of Users of the Service or the public
- Protect against legal liability

4.0 International transfers

We may transfer your personal data to service providers that carry out certain functions on our behalf. This may involve transferring personal data outside the UK or EEA to countries which have laws that do not provide the same level of data protection as the UK or EU law.
Whenever we transfer your personal data out of the UK or EEA to service providers, we ensure a similar degree of protection is afforded to it by ensuring that the following safeguards are in place:

- We will only transfer your personal data to countries that have been deemed by the UK or the EU to provide an adequate level of protection for personal data; or
- We may use specific standard contractual terms approved for use in the UK and/or EEA which give the transferred personal data the same protection as it has in the UK or EEA, or another transfer mechanism which has been approved by the relevant regulator in the UK and/or the EEA. To obtain a copy of these contractual safeguards, please contact us at dpo@augmentia.ai.

5.0 Data security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

6.0 Data retention

6.1 How long will you use my personal data for?

Your information is securely stored. Augmentiawill retain Your Personal Data only for as long as is necessary for the purposes set out in this Privacy Notice.
We will retain and use Your Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies. The Company will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of Our Service, or We are legally obligated to retain this data for longer time periods.
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.
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.

7.0 Protecting your sensitive data

Augmentia follows the information security values of

- confidentiality - making sure your information is always kept secret and private;
- integrity - we ensure the completeness, consistency, and accuracy of the data over its lifecycle; and
- availability - we ensure the right information is available to the right person at the right time.

We use the following techniques and best practices to protect your sensitive data:

7.1 People

To assure the data protection, we take the precautions as listed:

- Training - All staff receive regular appropriate training on data protection and security and their related duties to ensuring your personal data is secure;
- Minimised access: your personal data, can only be accessed on a strictly needs to know basis by our admin staff, or customer support as and when necessary, specifically as relates to your particular request for support;
- Security expertise: To design and operate our platform, we utilise qualified security professionals with recognised experience in technical security architecture as well as governance, risk, and compliance.

7.2 Cyber resiliency, business continuity, and disaster recovery

- Our web frontend(s) and parts of our backend are hosted on Cloudflare and make use of their secure platform.
- Our cloud and on-premise servers which may be in use from time to time are automatically kept up-to-date with the latest security patches and fixes.
- In addition, we commit to undertaking annual third-party security audits with certified security auditors including web, desktop and mobile application penetration tests to ensure comprehensive coverage.

7.3 Technology

We adopt principles of Secure by Design, including:

- Architecture in line with industry standards.
- This includes role based access controls.
- Our REST APIs utilise authentication and authorization to ensure data minimization and prevent unauthorised access to data.
- Our password quality validation for users ensures only strong passwords are allowed and are stored hashed using SHA-256.

We use encryption in all of the following scenarios:

- In transit using modern protocols (TLS only) and secure ciphers (both internally within the VPC and externally with users & applications)
- At rest using AES-256 encryption

Data centres:

- We host data in multiple availability zones/regions in order to maximise availability. All production environments are located within the UK and EEA.
- Where possible, deploy a High Availability (HA) architecture to ensure resilience with automated failover to provide uninterrupted service.

Development, security & operations:

- We operate a mature secure software development life cycle (SDLC), which includes but is not limited to:
  - Separation of keys for each environment and robust key management processes
  - Regular dependency and package management audits and remediation
  - Logical separation of production and development environments including isolated databases
  - Static code testing to ensure code is free from known vulnerabilities
  - Dynamic code testing to ensure applications do not expose vulnerabilities
  - Manual security testing (annual penetration test)

8.0 Your legal rights

You have a number of rights under data protection laws 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 **correction** 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.
- **Object to 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.
- You also have the absolute right to object any time to the processing of your personal data for direct marketing purposes.
- 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.
- Withdraw consent at any time where we are relying on consent to process your personal 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.
- Request restriction of 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:
  - If you want us to establish the data's accuracy;
  - Where our use of the data is unlawful but you do not want us to erase it;
  - 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
  - You have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
  - If you wish to exercise any of the rights set out above, please contact us dpo@augmentia.ai

Where Augmentia is the data processing (for example, if a GP practice or PCN is the controller,) to find out more about how your data is protected by them, or to exercise your rights under data protection law, you should contact them directly.

8.1 No fee usually required

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.

8.2 What we may need from you

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.

8.3 Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it could take us longer than a month 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.

9.0 Contact details

If you have any questions about this Privacy Notice or about the use of your personal data or you want to exercise your privacy rights, please contact us in the following ways:

- Email address: dpo@augmentia.ai

10.0 Complaints

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK regulator for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

11.0 Changes to the Privacy Notice and your duty to inform us of changes

We keep our Privacy Notice under regular review. This version was last updated in 15.07.2025.
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 your relationship with us, for example a new address or email address.

12.0 Third-party links

The website or the product may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the Privacy Notice of every website you visit.
We require all third parties to respect the security of your personal data and to treat it in accordance with the 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.

13.0 Payments

We may provide paid products and/or services within the Service. In that case, we may use third-party services for payment processing (e.g. payment processors). We will not store or collect Your payment card details. That information is provided directly to Our third-party payment processors whose use of Your personal information is governed by their Privacy Notice.

14.0 Children's Privacy

Our Service does not knowingly address anyone under the age of 18. We do not knowingly collect personally identifiable information from anyone under the age of 18. If You are a parent or guardian and You are aware that Your child has provided Us with Personal Data as user, please contact Us. If We become aware that We have collected Personal Data from anyone under the age of 18 without verification of parental consent, We take steps to remove that information from Our servers.
If We need to rely on consent as a legal basis for processing Your information and Your country requires consent from a parent, We may require Your parent's consent before We collect and use that information.