



Vitaspan Privacy Notice

This Privacy Notice sets out how we use and protect your personal data. It is provided in a layered format so you can click through to the specific areas set out below.

[1. IMPORTANT INFORMATION AND WHO WE ARE](#)

[2. TYPES OF PERSONAL DATA WE COLLECT ABOUT YOU](#)

[3. HOW IS YOUR PERSONAL DATA COLLECTED?](#)

[4. HOW WE USE YOUR PERSONAL DATA](#)

[5. TO WHOM DO WE DISCLOSE YOUR PERSONAL DATA](#)

[6. INTERNATIONAL TRANSFERS](#)

[7. MARKETING](#)

[8. COOKIES](#)

[9. DATA SECURITY](#)

[10. DATA RETENTION](#)

[11. YOUR LEGAL RIGHTS](#)

[12. OUR CONTACT DETAILS](#)

[13. COMPLAINTS](#)

[14. CHANGES TO THE PRIVACY NOTICE AND YOUR DUTY TO INFORM US OF CHANGES](#)



1. Important information and who we are

Introduction

This Privacy Notice gives you information about how we, Vitaspan Limited, collect and use your personal data when you use this platform, including any data you may provide when you visit or interact with us in any way, including when you register with us or use any features on our platform.

Users of this platform must be over 16 years old. If you are under 16, only your parent or legal guardian can use this platform on your behalf.

The Vitaspan platform

Vitaspan is a platform that uses wellness data to deliver real time AI-driven insights and predictive analytics, to support clinical decision-making, improve healthcare outcomes, enable interoperability across healthcare providers, and to provide tailored patient experiences.

Our relationship with you

We work with healthcare providers (for ease, we'll call them **Healthcare Provider** from now on) and individuals giving them access to our platform and the services made available via it, to help provide proactive, personalised wellness care.

You could be interacting with us in one of two ways:

- 1) if your Healthcare Provider has invited you to use our platform, they're the ones in charge of your personal data. That means they decide what information is collected, why it's used and how its handled. We simply follow their instructions and help them manage your data, working like their assistant. In legal terms, your Healthcare Provider is the 'controller' of your personal data, and we act as their 'processor'. So, if you have any questions or concerns about how your personal data is being used, it's best to reach out directly to your Healthcare Provider. They are responsible for explaining everything and helping you with any issues.

OR

- 2) if you are using our platform on your own or you are a clinician or staff member working at a Healthcare Provider, then we are responsible for your personal data. That means we decide how your data is collected, used and protected. We handle your personal data in the way set out in this Privacy Notice, which explains everything, including what personal data we collect and how we keep it safe.

Data Protection Manager

We have appointed a Data Protection Manager to oversee data protection related queries. If you have concerns or questions, please reach out to our data protection manager at dpo@vitaspan.ai.



2. The types of personal data we collect about you

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 first name, last name, login data (e.g. username or similar identifier if you have an account with us), date of birth, biometric scans of parts of your body (if you choose to use those features), ID information (e.g. ID document type (e.g. passport or photo driving licence) and information included on it (e.g. issuing country, image)).
- **Contact Data** includes email address and telephone numbers.
- **Wellness and Medical Data** includes electronic health records, clinical notes, diagnostic imaging, lab results, treatment plans, prescriptions, wellness questionnaire answers, self-reported medical histories, lifestyle information, biometric measurements and outputs from clinically validated predictive algorithms used to assess risk and inform clinical decisions. See below for more information about this type of personal data.
- **Content Data** includes any personal data you choose to disclose whilst using any feature or functionality on our platform (including recordings between you and your Healthcare Provider).
- **Financial Data** includes bank account and payment card details.
- **Transaction Data** includes details about payments to and from you in connection with your use of the platform.
- **Usage Data** includes information about how you interact with and use our platform, and the content made available via it.
- **Marketing and Communications Data** includes your preferences in receiving marketing from us and our third party partners and your communication preferences.
- **Technical Data** includes internet protocol (IP) address, browser type and version, date, time and your activity on our platform, 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 platform.



Special Categories of Data

We will not collect, store and use the following “special categories” of more sensitive personal data regarding you:

- information about your political opinions; or
- information about your trade union memberships.

We may, however, collect:

- wellness and medical information about you (as described above)
- biometric information about you, for example, if you chose to provide a face scan or other live scan, to help us verify your identity or to use one of biometric scans to derive wellness related insights; and
- information about your ethnicity, race, sex life or sexual orientation, to the extent it informs your Wellness and Medical Data.

These types of personal data require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data. We may process special categories of personal data with your explicit consent. Less commonly, we may process this type of data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We will generally not collect, store and use any criminal records information in relation to you. If we do, we will let you know, at the time we collect it, on which basis we are relying to process that data.

Identity verification

To ensure the security of our platform and protect access to sensitive wellness-related services, we use a trusted third-party identity verification provider to verify your identity.

You will be asked for your consent to provide this personal data. The details of how your personal data is processed and the purpose for processing it will be outlined in the consent itself. If you choose not to consent, we cannot give you automatic access to the platform.

When you complete identity verification, your personal data (including photos, videos and an identity document, as well as the information derived from it) is submitted directly to our verification provider. We do not access, store, or process this data ourselves. We only receive a confirmation of your verification status (e.g., Approved, Resubmission needed or Declined).

We take this approach to safeguard your privacy and ensure that your wellness-related data remains protected. For more information, we encourage you to review the privacy notice of our identity verification provider Veriff, <https://www.veriff.com/privacy-notice>.



Anonymised and aggregated data

We may process your personal data to create anonymised and aggregated datasets. This means that any information that could identify you personally, such as your name, contact details, or wellness identifiers, is removed or irreversibly altered so that you cannot be identified, directly or indirectly from the resulting data.

We use these anonymised and aggregated datasets for:

- improving the quality, safety, and effectiveness of our services, including our algorithms
- conducting research and statistical analysis
- developing new products, tools, or service offerings
- sharing insights with academic, clinical or commercial partners
- commercial purposes, including licensing or selling anonymised datasets to third parties.

To be clear, these data sets are fully anonymised and do not contain information that could reasonably be used to identify you.

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 aggregate individuals' Usage Data to calculate the percentage of users accessing a specific platform feature in order to analyse general trends in how users are interacting with our platform to help improve the platform and our offering. We own all aggregated and anonymised data sets.

3. How is your personal data collected?

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

- **Your interactions with us.** You may give us your personal data by filling in our platform forms or by corresponding with us by post, phone, email or otherwise.

This includes personal data you provide when you:

- create an account on our platform;
 - interact with us via our platform
 - interact with functionality provided via our platform;
 - request marketing to be sent to you;
 - enter a competition, promotion or survey; or
 - give us feedback or contact us.
- **Other third parties or publicly available sources.** We will receive



personal data about you from various third parties and public sources as set out below:

Identity Data and Wellness and Medical Data may be collected and provided to us by our third party partners, including through your use of:

- wearable devices or other monitoring equipment and
- telemedicine or clinical AI platforms or services
that are linked to our platform.
- Technical Data is collected from the following parties: analytics providers such as Google; and search information providers.
- **Automated technologies or interactions.** As you interact with our platform, we will automatically collect Technical Data about your devices, browsing actions and patterns. We collect this personal data by using cookies and other similar technologies. We may also receive Technical Data about you if you visit other websites employing our cookies. Please see our Cookie Policy for information about the cookies we use.

Remember. If you access and use our platform via a Healthcare Provider, they may upload your Wellness and Medical Data and your other personal data to our platform to manage and help provide services to you. In that case, they are responsible for your personal data. Please see their privacy notice to understand how they collect, use and protect your personal data.

4. How we use your personal data

Legal basis

The law requires a controller to have a legal basis for collecting and using personal data.

Where we are acting as controller, we rely on one or more of the following legal bases:

- **Performance of a contract with you:** Where we need to perform a 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 patient 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.
- **Consent:** We rely on consent only where we have obtained your active agreement to use your personal data for a specified purpose, for example if



you choose to use a biometric scan that provides wellness related data or if you subscribe to an email newsletter.

Remember. If you have accessed this platform at the invitation of your Healthcare Provider, as they manage your personal data, they will set out the lawful basis on which they are collecting and using your personal data in their privacy notice. So please consult their notice for this information.

Purposes for which we will use your personal data

Where we are acting as controller of 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 verify you as a user or clinician before you are allowed to use our platform, register you as a user, and allow you to login to your account on the platform	(a) Identity (b) Contact	(a) Necessary for our legitimate interests (e.g. to ensure only authorised individuals are allowed to use the platform) (b) Performance of a contract with you or the Healthcare Provider that employs you
To allow you to use the platform's functionality	(a) Identity (b) Contact (c) Wellness and Medical Data (d) Financial (e) Content (f) Transaction	(a) Performance of a contract with you or the Healthcare Provider that employs you (b) Necessary for our legitimate interests (c) Consent (e.g. you consent to using the functionality provided)
To process and deliver your subscription to the platform or the purchase of any particular services including: (a) collecting money from you (b) managing payments, fees and charges	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Content	(a) Performance of a contract with you or the Healthcare Provider that employs you (b) Necessary for our legitimate interests (to recover debts due to us) (c) Necessary to comply with our legal obligations (e.g. to report to certain tax authorities)



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) Content	(a) Performance of a contract with you or the Healthcare Provider that employs 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 partake in a prize draw or competition	(a) Identity (b) Contact (c) Usage (d) Marketing and Communications	(a) Performance of a contract with you or the Healthcare Provider that employs you (b) Necessary for our legitimate interests (to study how users use our platform, to develop and grow our business)
To administer and protect our business and this platform (including identifying non-compliance with our Terms and policies, troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data To process your personal data to anonymise and aggregate it. This involves removing or altering any information that could identify you, so that you cannot be identified directly or indirectly from it.	(a) Identity (b) Contact (c) Technical (d) Content (a) Identity (b) Wellness and Medical Data (c) Content	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud, to ensure compliance with our policies, to handle complaints and in the context of a business reorganisation or group restructuring exercise) (b) Necessary to comply with a legal obligation Necessary for our legitimate interests (to help improve our services and develop new ones, to share insights and to license and sell anonymised and aggregated data sets).



To use data analytics to improve our platform, our offering, customer relationships and experiences and to measure the effectiveness of our communications and marketing	(a) Technical (b) Usage (c) Marketing and Communications	(a) Necessary for our legitimate interests (to define types of users for the services offered via our platform, to keep our platform 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 content that may be of interest to you	(a) Identity (b) Contact (c) Technical (d) Usage (e) Marketing and Communications	(a) Necessary for our legitimate interests (to carry out direct marketing, develop our products/services and grow our business) (b) Consent (e.g. consent to receive direct marketing communications)
To carry out market research through your voluntary participation in surveys or questionnaires	(a) Identity (b) Contact (c) Content (d) Usage	Necessary for our legitimate interests (to study how users use our platform and content and to help us improve and develop our business and offerings).

Where we are processing your personal data on the basis of your consent, you can withdraw your consent at any time by emailing dpo@vitaspan.ai. Please note however that the withdrawal of your consent will not affect any use of the personal data made before you withdrew your consent and we may still be entitled to hold and process the relevant

personal information to the extent that we are entitled to do so on bases other than your consent. Withdrawing consent may also have the same effect as not providing the information in the first place, for example we may no longer be able to provide certain services to you via the platform.

5. To whom do we disclose your personal data?

All organisations who we share data with are risk assessed and are required to ensure that all security measures and appropriate safeguards are put in place to protect your information and comply with data protection laws.

We share certain personal data about you with the following parties:

- **third party providers of wellness and medical services** made available via the platform. E.g. providers of biometric scan technology.
- **other service providers to our business:** payment processors, ID verification providers, administration and IT services and other service providers. Where you are providing your payment details, that personal data is hosted by our payment processors.



We do not store that personal data. As a result, the processing of that personal data is handled according to their privacy notice, not ours. You should read their privacy notice before you provide such personal data. Our payment provider Stripe's privacy notice is available [here](#).

- **advisors:** either advisors appointed by you, for example legal advisors, or advisors appointed by us.
- **purchasers of our business:** buyers or perspective buyers to whom we may sell or negotiate to sell our business.
- **the Government, government bodies or our regulators:** where we are required to do so by law or to assist with their investigations or initiatives, for example HM Revenue & Customs or the Information Commissioner's Office.
- **police, law enforcement and security services:** to assist with the investigation and prevention of crime and the protection of national security.

We do not disclose personal information to anyone else except as set out above unless we have your consent or we are legally obliged to do so. We do not sell, rent or trade your personal data.

6. International transfers

We are based in the UK and generally we will only hold your information in the UK.

However, sometimes we may share your personal information with other companies who provide certain services to us, for example companies that help us to look after our platform, or that provide certain functionality for our platform, that are based outside the UK. If we do, we make sure that your personal data is protected in a similar way as if it were still with us in the UK. This is done in a few different ways, for example:

- some countries to which we send your personal data are judged by the UK to have the same level of protection as the UK and are considered safe places for your personal data, for example countries in the EEA; or
- for other countries that are not judged to have the same level of protection, we put a contract in place with the recipients of your personal data to require the same level of protection as you would have under UK laws. These contracts may for example, be based on the UK's international data transfer agreement, the UK Addendum to the EU's standard contractual clauses or the UK Extension to the EU-US Data Privacy Framework.



7. Marketing

Direct marketing

During the registration process on our platform when your personal data is collected, you may be asked to indicate your preferences for receiving direct marketing communications from us via email, SMS, mobile. You will receive marketing communications from us if you

have requested information from us and you have not opted out of receiving the marketing.

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.

Opting out of marketing

You can ask us to stop sending you marketing communications at any time by logging into the platform and checking or unchecking relevant boxes to adjust your marketing preferences or by following the opt-out links within any marketing communication sent to you or by contacting us.

If you opt out of receiving marketing communications, you will still receive service-related communications that are essential for administrative purposes for example relating to updates to our terms or checking that your contact details are correct.

8. Cookies

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

9. Data security

We have put in place appropriate technical and organisational measures to protect your personal data against accidental loss, unauthorised access, use, alteration or disclosure.

In particular, personal data is protected using multiple layers of security, including:

- **Secure hosting.** Your data is hosted within Google Cloud Platform (GCP) data centres located in the geographic region selected by your Healthcare Provider. These facilities are designed and operated in accordance with internationally recognised security, privacy and compliance standards and are independently audited. Data is encrypted both in transit and at rest using industry-standard encryption technologies.
- **Access security.** Access to the Platform is protected using multi-factor authentication where appropriate, together with role-based access controls and audit logging to help ensure that only authorised users can access personal information.



- **Business continuity.** Data is securely backed up, and we maintain business continuity and disaster recovery procedures designed to support the availability and resilience of the Platform in the event of an unexpected disruption.
- **Restricted access.** Access to personal data is limited to employees, contractors, service providers and other authorised persons who require it to perform their duties. They process personal data only on our instructions and are subject to contractual and statutory confidentiality obligations.
- **Security monitoring.** We regularly review, monitor and test our security controls to help maintain the confidentiality, integrity and availability of personal information.

10. Data retention

How long do we keep your personal data for?

We will only retain your personal data for as long as you consent to us holding it, as required by law, to deal with a complaint or if we reasonably believe there is a prospect of litigation in respect of our relationship with you.

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 that may specify the periods for which we are required to hold your personal data.

Taking all of the above into account, we keep different types of your personal data for different periods in accordance with our Records Management Policy.

If you would like to know how long we keep a specific type of personal data for, please contact us at dpo@vitaspan.ai.

Where we have aggregated and anonymised your personal data so that it can no longer identify you (as described in section 2 above), we may use this information indefinitely as it is no longer considered personal data.

11. Your legal rights

You have a number of rights under data protection laws in relation to your personal data. Under certain circumstances, by law 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 at any time to the processing of your personal data for direct marketing purposes (see **OPTING OUT OF MARKETING** in section 7 for details of how to object to receiving direct marketing communications).
- 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 (see the table in section 4 for details of when we rely on your consent 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. Be aware, that if you withdraw your consent, we may not be able to provide certain services to you. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.
- 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 by emailing us at dpo@vitaspan.ai.

Where our platform uses biometric scans to derive wellness related insights about you, these insights do not result in automated decision making about you. All outputs from these scans are reviewed by qualified clinicians who apply their professional judgement to those outputs before any advice is given or action taken. This means that while we use technology to support analysis, final decisions are always made by humans, not algorithms.

Where our platform uses a third party ID verification provider, they may use automated systems to assist in the verification process. These processes may involve automated profiling, but no decisions with legal or similarly significant effects are made solely by automated means. A member of our third party ID verification provider team reviews any flagged cases and makes the final determination.

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.

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.

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.



12. Our 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: dpo@vitaspan.ai
- Address: 5th floor, 167-169 Great Portland Street, London, W1W 5PF, United Kingdom.

13. 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.

14. Changes to the privacy notice and your duty to inform us of changes

This Privacy Notice was last updated in August 2025. We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal data.

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 email address.