This privacy policy contains important information on who we are and how and why we collect, store, use and share your personal data. It also explains your rights regarding your personal data and how to contact us or supervisory authorities in case of a complaint.

We collect, use and are responsible for certain personal data about you. When we do so we are subject to the UK General Data Protection Regulation (UK GDPR). We are also subject to the EU General Data Protection Regulation (EU GDPR) in relation to goods and services we offer to individuals and our wider operations in the European Economic Area (EEA).

Kardiaport Ltd acts as both the Controller and the Processor of your personal data. As the Controller, we determine the purposes and means of processing your personal data, such as for research purposes. As the Processor, we also carry out the processing activities, including data storage, analysis, and management. This privacy policy explains how we fulfill our responsibilities in both roles.

Key terms

It would be helpful to start by explaining some key terms used in this policy:

We, us, our	**Kardiaport Ltd**
Personal data	Any information relating to an identified or identifiable individual
Data subject	The individual who the personal data relates to

Personal data we collect about you

The personal data we collect about you depends on the specific type of research we conduct using your data. We will collect and use the following personal data about you:

- Name
- Email
- Address (including country)
- Phone number
- Communication preferences
- Sex
- Age
- Ethnicity
- Nicotine and alcohol use
- Health-related details including any medications you are taking or existing illnesses or medical conditions
- Health data including heart rate, activity levels, sleep patterns, calorie expenditure, step counts, and other biometric metrics, as well as any associated timestamps or contextual information

We collect and use this personal data for the purposes described in the section '**How and why we use your personal data**' below. If you do not provide personal data we ask for, it may delay or prevent us from making payment to you under our terms and conditions

Sometimes you can choose if you want to give us your personal data and let us use it. Where that is the case, we will tell you and give you the choice before you give the personal data to us. We will also tell you whether declining to share that personal data will have any effect on your privacy and the research we are conducting.

How your personal data is collected

We collect most of this personal data directly from you. However, we may also collect information from:

- Third party wearable devices. Where you choose to share your Fitbit history with us, we access that data through the Google Health API using your Google account. We only access the data you explicitly consent to share, we never receive your Google password, and you can withdraw our access at any time from your Google account security settings.

How and why we use your personal data

Under data protection law, we can only use your personal data if we have a proper reason, e.g.:

- where you have given consent;
- to comply with our legal and regulatory obligations;
- for the performance of a contract with you or to take steps at your request before entering into a contract; or
- for our legitimate interests or those of a third party.

A legitimate interest is when we have a business or commercial reason to use your personal data, so long as this is not overridden by your own rights and interests. We will carry out an assessment when relying on legitimate interests, to balance our interests against your own.

When we collect data from third-party wearable devices, we act as the Controller, determining the purposes and means of processing this data. We ensure that these devices comply with GDPR requirements and that your data is processed securely.

The table below explains what we use your personal data for and why.

What we use your personal data for	Our reasons
As part of our research	To develop predictive models to diagnose certain health conditions
Preventing and detecting fraud against you or us	For our legitimate interest, i.e. to minimise fraud that could be damaging for you and/or us
Conducting checks to identify our customers and verify their identity and eligibility to participate in the study	Depending on the circumstances: —to comply with our legal and regulatory obligations

Other activities necessary to comply with professional and legal regulations	—for our legitimate interests
To enforce legal rights or defend or undertake legal proceedings	Depending on the circumstances: —to comply with our legal and regulatory obligations; —in other cases, for our legitimate interests, ie to protect our business, interests and rights
Ensuring business policies are adhered to, eg policies covering security	For our legitimate interests, ie to make sure we are following our own internal procedures
Operational reasons, such as improving efficiency, training and quality control	For our legitimate interests, ie to be as efficient as we can
Ensuring the confidentiality of sensitive information	Depending on the circumstances: —for our legitimate interests, ie to protect commercially valuable information; —to comply with our legal and regulatory obligations
Statistical analysis to support our research and improve our services eg identifying patterns to enhance the quality and efficiency of our research	For our legitimate interests, ie to be as efficient as we can in conducting our research
Preventing unauthorised access and modifications to systems	Depending on the circumstances: —for our legitimate interests, ie to prevent and detect criminal activity that could be damaging for you and/or us; —to comply with our legal and regulatory obligations
Protecting the security of systems and data used to collect and process your data	To comply with our legal and regulatory obligations We may also use your personal data to ensure the security of systems and data to a standard that goes beyond our legal obligations, and in those cases our reasons are for our legitimate interests, ie to protect systems and data and to prevent and detect criminal activity that could be damaging for you and/or us
Updating and enhancing customer records	Depending on the circumstances:

	—to perform our contract with you or to take steps at your request before entering into a contract; —to comply with our legal and regulatory obligations; —for our legitimate interests, eg making sure that we can keep in touch with you about the study and any updates
Statutory returns	To comply with our legal and regulatory obligations
Ensuring safe working practices, staff administration and assessments	Depending on the circumstances: —to comply with our legal and regulatory obligations; —for our legitimate interests, eg to make sure we are following our own internal procedures and working efficiently so we can enhance the quality and efficiency of our research
External audits and quality checks, eg for ISO or Investors in People accreditation and the audit of our accounts to the extent not covered by 'activities necessary to comply with legal and regulatory obligations' above	Depending on the circumstances: —for our legitimate interests, ie to maintain our accreditations so we can demonstrate we operate at the highest standards; —to comply with our legal and regulatory obligations
To share your personal data with members of our group and third parties that will or may take control or ownership of some or all of our business (and professional advisors acting on our or their behalf) in connection with a significant corporate transaction or restructuring, including a merger, acquisition, asset sale, initial public offering or in the event of our insolvency In such cases information will be completely anonymised where possible and only shared where necessary	Depending on the circumstances: —to comply with our legal and regulatory obligations; —in other cases, for our legitimate interests, ie to protect, realise or grow the value in our business and assets

How and why we use your personal data—in more detail

More details about how we use your personal data and why are set out in the table below.

Purpose	Processing operation	Lawful basis relied on under the UK GDPR and EU GDPR	Relevant categories of personal data
Communications with you not related to marketing, including about changes to our terms or policies or changes to the services or other important notices (other than those addressed above)	Addressing and sending communications to you as required by data protection laws, ie: —the UK GDPR or Data Protection Act 2018; —the EU GDPR	Processing is necessary for compliance with a legal obligation to which we are subject (Article 6(1)(b))	—your name, address and contact information, including email address and telephone number;
	Addressing and sending communications to you about changes to our terms or policies or changes to the services or other important notices	Our legitimate interests (Article 6(1)(f)), which is to be as efficient as we can so we can deliver the best service to you	—your name, address and contact information, including email address and telephone number

How and why we use your personal data—Special category personal data

Certain personal data we collect is treated as a special category to which additional protections apply under data protection law:

- Personal data revealing racial or ethnic origin
- Biometric data (when used to uniquely identify an individual)
- Data concerning health

How and why we use your personal data—sharing

See '**Who we share your personal data with**' for further information on the steps we will take to protect your personal data where we need to share it with others.

Who we share your personal data with

We share your personal data with trusted third-party service providers to facilitate the secure operation of our research study. Specifically, we share personal data with:

Microsoft Azure: We use Microsoft Azure for secure data storage. Microsoft Azure provides robust baseline security measures, and we have implemented additional safeguards to ensure compliance with GDPR and the UK Data Protection Act 2018.

External auditors: For example, in relation to the audit of our accounts, in which case the recipient of the information will be bound by confidentiality obligations.

Professional advisors: Such as lawyers and other advisors, in which case the recipient of the information will be bound by confidentiality obligations.

Law enforcement agencies, courts, tribunals, and regulatory bodies: To comply with our legal and regulatory obligations.

Other parties: That have or may acquire control or ownership of our business (and our or their professional advisers) in connection with a significant corporate transaction or restructuring, including a merger, acquisition, asset sale, initial public offering, or in the event of our insolvency. Usually, information will be anonymised, but this may not always be possible. The recipient of any of your personal data will be bound by confidentiality obligations.

We only allow those organisations to handle your personal data if we are satisfied they take appropriate measures to protect your personal data.

We or the third parties mentioned above occasionally may also share personal data with:

- our external auditors, eg in relation to the audit of our accounts, in which case the recipient of the information will be bound by confidentiality obligations;
- our and their professional advisors (such as lawyers and other advisors), in which case the recipient of the information will be bound by confidentiality obligations;
- law enforcement agencies, courts, tribunals and regulatory bodies to comply with our legal and regulatory obligations;
- other parties that have or may acquire control or ownership of our business (and our or their professional advisers) in connection with a significant corporate transaction or restructuring, including a merger, acquisition, asset sale, initial public offering or in the event of our insolvency—usually, information will be anonymised but this may not always be possible. The recipient of any of your personal data will be bound by confidentiality obligations.

Who we share your personal data with—in more detail

More details about who we share your personal data with and why are set out in the table below. This will be updated once we decide to share your data with third parties.

More details about who we share your personal data with and why are set out in the table below. This will be updated as necessary if we decide to share your data with additional third parties.

Recipient	Processing Operation (Use) by Recipient	Relevant Categories of Personal Data Transferred to Recipient
Microsoft Azure	Secure storage of personal and health data	Anonymised and encrypted health data, participant identifiers
External auditors	Audit of accounts	Financial records, anonymised participant data
Professional advisors	Legal and regulatory advice	Anonymised participant data, legal documentation
Law enforcement agencies	Compliance with legal obligations	Personal data as required by law
Other parties (e.g., in corporate transactions)	Business restructuring or acquisition	Anonymised data, where possible

Microsoft Azure acts as a Sub-Processor, providing secure data storage services on our behalf. External auditors and professional advisors may act as independent Controllers when fulfilling their legal or professional obligations.

Who we share your personal data with—further information

If you would like more information about who we share our data with and why, please contact us (see '**How to contact us**' below).

Where your personal data is held

Personal data may be held at our offices and those of our service providers, if any, as described above (see above: '**Who we share your personal data with**').

Some of these third parties may be based outside the UK/EEA. For more information, including on how we safeguard your personal data when this happens, see below: '**Transferring your personal data out of the UK and EEA**'.

How long your personal data will be kept

We will not keep your personal data for longer than we need it for the purpose for which it is used. We will retain your personal data for 3 years unless a longer retention period is required by law or necessary for our legitimate interests. Anonymised data, which cannot be traced back to you, may be retained indefinitely for research and analysis purposes.

Different retention periods apply for different types of personal data. Further details on this will be made available in this section.

Transferring your personal data out of the UK and EEA

We process all personal data within the UK. However, as we may collect data from individuals located outside the UK and EEA (e.g., through advertising on platforms like Facebook and Reddit), we ensure that any data collected from these individuals is handled in compliance with applicable UK and EEA data protection laws.

We do not transfer your personal data to countries outside the UK or EEA for processing. All data collected, regardless of the participant's location, is securely processed and stored within the UK using Microsoft Azure, which complies with GDPR and UK Data Protection Act 2018 requirements.

In the event that it becomes necessary to transfer personal data outside the UK or EEA in the future, we will ensure that:

- The transfer is made to a country that the UK government or European Commission has determined provides an adequate level of protection for personal data (known as an 'adequacy regulation' or 'adequacy decision').
- Where no adequacy regulation or decision exists, appropriate safeguards are in place, such as legally-approved standard data protection clauses recognised under Article 46(2) of the UK GDPR and/or EU GDPR.
- Enforceable rights and effective legal remedies are available to you.

If we cannot rely on an adequacy regulation, decision, or appropriate safeguards, we will only transfer your personal data outside the UK/EEA where a specific exception applies under relevant data protection law.

We are committed to ensuring that your personal data is protected, regardless of where it originates, and will update this policy if our data transfer practices change in the future.

At present, we do not transfer your personal data outside the UK or EEA. If international transfers become necessary in the future, we will ensure that appropriate safeguards are in place, such as Standard Contractual Clauses or adequacy decisions, to protect your data.

Any changes to the destinations to which we send personal data or in the transfer mechanisms we rely on to transfer personal data internationally will be notified to you in accordance with the section on '**Changes to this privacy policy**' below.

At present, we do not transfer your personal data to countries outside the UK or EEA. All data is securely processed and stored within the UK using Microsoft Azure.

Should it become necessary to transfer your personal data outside the UK or EEA in the future, we will ensure that:

- The transfer is made to a country that the UK government or European Commission has determined provides an adequate level of protection for personal data (known as an 'adequacy regulation' or 'adequacy decision').
- Where no adequacy regulation or decision exists, appropriate safeguards are in place, such as legally-approved standard data protection clauses recognised under Article 46(2) of the UK GDPR and/or EU GDPR.
- Enforceable rights and effective legal remedies are available to you.

More details about the countries outside the UK and EEA to which your personal data may be transferred in the future will be set out in the table below, if applicable.

Recipient Country	Recipient	Processing Operation (Use) by Recipient	Lawful Safeguard
N/A	N/A	N/A	N/A

If you would like further information about data transferred outside the UK/EEA, please contact us (see 'How to Contact Us' below).

Your rights

You have the following rights, which you can exercise free of charge:

Access	The right to be provided with a copy of your personal data
Rectification	The right to require us to correct any mistakes in your personal data
Erasure (also known as the right to be forgotten)	The right to require us to delete your personal data—in certain situations
Restriction of processing	The right to require us to restrict processing of your personal data in certain circumstances, eg if you contest the accuracy of the data
Data portability	The right to receive the personal data you provided to us, in a structured, commonly used and machine-readable format and/or transmit that data to a third party—in certain situations
To object	The right to object: —at any time to your personal data being processed for direct marketing (including profiling); —in certain other situations to our continued processing of your personal data, eg processing carried out for the purpose of our legitimate interests unless there are compelling legitimate grounds for the processing to continue or the processing is required for the establishment, exercise or defence of legal claims
Not to be subject to automated individual decision making	The right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects concerning you or similarly significantly affects you
The right to withdraw consent	If you have provided us with a consent to use your personal data you have a right to withdraw that consent easily at any time You may withdraw consent by contacting us on contact@kardiaport.com

	Withdrawing consent will not affect the lawfulness of our use of your personal data in reliance on that consent before it was withdrawn

For more information on each of those rights, including the circumstances in which they apply, please contact us (see '**How to contact us**' below) or see the Guidance from the UK Information Commissioner's Office (ICO).

If you would like to exercise any of those rights, please:

- Email, call or write to us — see below: '**How to contact us**'; and
- provide enough information to identify yourself *(eg your full name, address and reference number)* and any additional identity information we may reasonably request from you;
- let us know what right you want to exercise and the information to which your request relates.

As the Controller, Kardiaport is responsible for responding to your requests to exercise your rights under data protection law. If you wish to exercise any of these rights, please contact us using the details provided in the 'How to Contact Us' section.

Keeping your personal data secure

We have appropriate security measures to prevent personal data from being lost accidentally, or used or accessed unlawfully. We limit access to your personal data to those who have a genuine business need to access it. Those processing your personal data will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

If you want detailed information on how to protect your personal data and other information and your computers and devices against fraud, identity theft, viruses and many other online problems, please visit www.getsafeonline.org. Get Safe Online is supported by HM Government and leading businesses.

Google user data:

Where you connect your Fitbit account, we receive activity, heart rate, sleep, weight and basic profile data from the Google Health API. This data is used solely for the cardiovascular research purposes described in this policy. It is stored securely in Microsoft Azure within the UK, and is not sold, transferred for advertising, or used to build user profiles for any purpose unrelated to this research. You may request deletion of your data at any time by contacting us at contact@kardiaport.com.

Kardiaport's use and transfer of information received from Google APIs to any other app will adhere to the Google API Services User Data Policy, including the Limited Use requirements.

How to complain

Please contact us if you have any queries or concerns about our use of your personal data (see below '**How to contact us**'). We hope we will be able to resolve any issues you may have.

You may also have the right to lodge a complaint with the Information Commissioner (the UK data protection regulator).

Changes to this privacy policy

This privacy notice was published on 21st March 2026 and last updated on 17th August 2026.

We may change this privacy notice from time to time—when we do we will inform you via other means of contact such as email.

Updating your personal data

We take reasonable steps to ensure your personal data remains accurate and up to date. To help us with this, please let us know if any of the personal data you have provided to us has changed, eg your surname or address—see below '**How to contact us**'. You can also update your personal data yourself via an email to our team.

How to contact us

Individuals in the UK

You can contact us by email or if you have any questions about this privacy policy or the information we hold about you, to exercise a right under data protection law or to make a complaint.

Our contact details are shown below:

Our contact details
contact@kardiaport.com

Individuals in the EEA

We have appointed Freeman Harris Solicitors to be our data protection representative within the EEA. Their contact details are contact@freemanharris.co.uk.

Individuals within the EEA can contact us direct (see above) or contact our European representative.

Do you need extra help?

If you would like this notice in another format (for example audio, large print, braille) please contact us (see 'How to contact us' above).