Atempora Ltd

Privacy Policy

Effective

This policy explains how Atempora Ltd collects, uses, shares and retains personal data when you use the Atempora mobile application and the services provided through it.

1. Who we are

Atempora Ltd ("Atempora", "we", "us") is the controller of the personal data described in this policy.

Data controller: Atempora Ltd, a company registered in England and Wales with company number 17111915.

Registered office: 389 Queens Road, London SE14 5HD, United Kingdom.

ICO registration number:

Privacy contact: privacy@atempora.co.uk.

Data protection officer: privacy@atempora.co.uk

If you have a question about this policy or about how we handle your data, you can contact us using the details above.

2. Who can use the application

The application is available only to individuals aged 18 or over. It is not directed at, and we do not knowingly collect personal data from, anyone under 18. If we become aware that we have collected data from a person under 18, we will delete it.

3. The personal data we collect directly from you

3.1 Data you provide directly

- Account data, including the details you give when you register and manage your account.
- Contact information to enable us to get in touch with you such as email address or phone number.
- Self-reported contextual data, being your answers to questions presented in the application.
- Correspondence with us, including support requests.
- The amount of points you have received for contributing the data.
- The rewards you have redeemed from the points you have accumulated.
- A wallet address, if and when a token-based reward feature is made available and you choose to use it.

3.2 Data from your wearable devices and health platforms

Where you connect a device or health platform, we receive the data that connection makes available. Depending on the device, this may include:

- Sensor signals, such as electrocardiogram (ECG), photoplethysmogram (PPG), Electrodermal activity (EDA), electroencephalogram (EEG), your temperature, or the device accelerometer and gyroscope data.
- Computed and index data, such as heart-rate variability features, sleep duration, activity data, as well as trends in such data.

We may also create derived features produced by our own standardisation and decomposition processing.

3.3 Data generated by your use of the application

This may include:

- Device identifiers and technical information about the device you use.
- Application usage telemetry.
- Diagnostic and crash data, which may include device and user identifiers and fragments of application state.

3.4 Health and other special category data

Our questionnaire covers ten contextual areas and corresponding data types, including:

- sleep, circadian rhythm and recovery;
- diet, metabolic status and medication;
- physical activity, training and body composition;
- pathologies, illness and inflammation;
- stress, mental load and emotional state;
- hormonal health;
- cognitive performance and productivity;
- longevity interventions;
- environmental and contextual stressors; and
- social and relational context.
- Log data, which includes logged events.

Answers in these areas, together with the data received from your devices, include data concerning your health. Depending on the questions presented to you, they may also include data about your sex life or sexual orientation, and, where laboratory or epigenetic data is added as a further labelling layer, genetic data. Data of these kinds is treated as special category data and is processed only where you have given explicit consent. The data types concerned are listed in the second table in section 5.

4. Data received from other sources

We receive personal data from you directly, from the devices and platforms you choose to connect, and from the service providers that operate the application on our behalf. Current integrations include:

Source	What it provides
Apple Health / HealthKit	Health and fitness data held on your Apple device(s), where you grant permission.
Health Connect and / or the Google Health API	Health and fitness data from Android devices and connected Google and Fitbit accounts, where you grant permission.
Junction	Ingestion of data from other connected devices and accounts.
Wearables	Through direct wearable integration
Laboratory data	Laboratory data you upload through the App
Other data	Any test results you upload through the App

You control which devices and accounts are connected and can disconnect them at any time in the application or in the settings of the relevant platform. Disconnecting stops further data being received; it does not by itself delete data already received, which is dealt with in sections 9 and 10.

5. Why we use your data, and our legal basis

The first table below sets out, for each type of data we hold, why we use it, the legal basis we rely on, and whether it is shared outside Atempora. The second table lists the data types that are special category data (health data), which we process only with your explicit consent.

5.1 Data types processing information

Data type	Purpose	Legal basis (Article 6)	External sharing
Account and contact data (e.g. name, email, contact number)	Creating and administering your account, verifying eligibility, and communicating with you about the service	Performance of a contract with you (Article 6(1)(b))	Not shared, other than with the service providers listed in section 6.1
Self-reported contextual answers (questionnaire data)	Building structured datasets; training, tuning and testing models within our own infrastructure; selecting and tailoring the questions presented to you	Your consent (Article 6(1)(a))	Not shared
Wearable, sensor and computed device data	As above, and developing our standardisation, adaptation and decomposition algorithms.	Your consent (Article 6(1)(a))	Not shared

Data type	Purpose	Legal basis (Article 6)	External sharing
	Training of AI models for our partners within our own infrastructure.		
Derived features produced by our processing	Dataset construction, algorithm development and model training within our own infrastructure	Your consent (Article 6(1)(a))	Not shared
Features and Labels	The AI model uses recorded deviations from your baseline inputs, as well as self-reported data, to create aggregate bands of anonymised data which can then form labels that can indicate characteristics.		Shared as a population cohort reasoning (insight derivative), without the link to specific individuals, personal data, or raw data.
Device identifiers and technical data	Operating the application, security, fraud prevention and diagnostics	Our legitimate interests in keeping the application secure and working correctly (Article 6(1)(f))	Splunk (crash and diagnostic reporting) and our hosting provider, as processors
Application usage telemetry	Product improvement, aggregate analysis and service statistics	Our legitimate interests in understanding and improving how the application is used (Article 6(1)(f))	Our hosting provider, as processor
Points balance and redemption records	Operating the rewards programme and enabling redemption with partner brands	Performance of a contract with you (Article 6(1)(b))	N/A. We provide a code that you can redeem with one of our redemption partners.
Correspondence and support records	Responding to your enquiries and to requests you make about your data	Performance of a contract with you and compliance with our legal obligations (Articles 6(1)(b) and 6(1)(c))	Not shared, other than as described in section 6.4
Any of the above, where the law requires	Complying with legal and regulatory obligations, and establishing, exercising or defending legal claims	Compliance with a legal obligation (Article 6(1)(c)), and our legitimate interests in defending claims (Article 6(1)(f))	Regulators, courts, and our professional advisers, as described in section 6.4

Where we rely on legitimate interests, we have assessed those interests against your interests, rights and freedoms. You may ask us for information about that assessment, and you may object to processing on this basis as described in section 12.

5.2 Health and other special category data, and the consent we rely on

The data types below are, or may be, special category data under Article 9. We process each of them only where you have given your explicit consent under Article 9(2)(a), together with your consent under Article 6(1)(a). We do not rely on any other Article 9 condition for them, except that we may rely on the establishment, exercise or defence of legal claims (Article 9(2)(f)) where that becomes necessary.

Data type	What it may include	Category under Article 9
Sensor and computed device data	ECG, PPG, EEG, temperature, movement, heart-rate variability features, sleep, activity and recovery measures and trends	Health data
Sleep, circadian rhythm and recovery	Sleep timing, quality, disturbance and recovery status	Health data
Diet, metabolic status and medication	Dietary pattern, metabolic status, and prescription and non-prescription medication use	Health data
Physical activity, training and body composition	Training load, activity levels and body composition measures	Health data
Pathologies, illness and inflammation	Chronic condition status, diagnoses, medical history, acute illness and inflammatory markers	Health data
Stress, mental load and emotional state	Perceived stress, symptom severity, trauma response indicators and engagement with therapy or counselling	Health data
Hormonal health	Menstrual cycle and fertility context, contraception, and menopause status	Health data, and data concerning sex life where applicable
Cognitive performance and productivity	Self-assessed cognitive function, focus and fatigue	Health data
Longevity interventions	Supplements, therapies and other interventions you use	Health data
Environmental and contextual stressors	Environmental exposures and situational stressors	Health data (where applicable)
Social and relational context	Relationship context, social support, and perceived libido and sexual health	Health data, and data concerning sex life
Laboratory data	Blood and other laboratory results used as an additional labelling layer	Health data
Epigenetic data	Epigenetic and other genetic results used as an additional labelling layer	Genetic data

You are not required to answer any question, and you may answer some verticals and not others. Declining to answer means the relevant data is not collected, and the only consequence is that you cannot contribute or earn points for that data.

5.3 Consent and withdrawal

- We ask for your explicit consent before processing health and other special category data. Consent is sought separately from the general terms of use and, where the purposes differ materially, separately for each purpose.
- You may withdraw consent at any point in sharing specific data categories in the section of the App.
- You may withdraw consent at any time, in the application or by contacting us. Withdrawal does not affect the lawfulness of processing carried out before you withdrew.
- The effect of withdrawal on data already contributed to a dataset is described in section 10.
- Providing device data and answering questions is not a statutory or contractual requirement and you are not obliged to do either. If you choose not to, you will not be able to contribute data or earn points, and parts of the application will not be available to you.

6. How your data is used

To be clear, we do not sell your data, and we do not give anyone outside Atempora general access to it. Your data stays on our own systems. Companies come to us to build and improve artificial intelligence models. That work is done by us, on our systems, using the data we hold. The company does not receive your data. It cannot download it, browse it, or search through it.

Atempora develops AI solutions and helps to tune AI models only for health, wellness, and longevity companies.

What the company receives is the finished model and our report on how well the model performed. A model is built from the contributions of a great many people. It is not a way of looking up what any one person has recorded.

In the event where we share bio-contextual reasoning “insights” based on correlations of features and labels (which do not contain raw data), they are organized as a population cohort reasoning insights that are used to improve Agents and Large Language Models (LLM’s).

We do not pass your data to advertisers, data brokers or companies that resell information. That holds even if the data has been grouped together with other people's or had the identifying details taken out.

Inside Atempora, only the people who need your data in order to run the service can see it, and they are under confidentiality obligations.

There are a few situations where data does go outside Atempora. They are the companies that help us run the Application. Each is explained below.

6.1 Service providers acting on our instructions

We use service providers to host and operate the application. They act as processors on our instructions and under written terms. They are:

Provider	Function	Processing location
Google Cloud Platform	Cloud hosting and storage, and native usage analytics	United Kingdom, in the London region, for data at rest. Google support personnel outside the United Kingdom may access data when handling a support request, including in the USA.
Junction	Device and account data ingestion	European Union, in Belgium, where the EU region is selected and its US region stores data in the United States.
Splunk	Crash and diagnostic reporting	United Kingdom, in the London realm, where that realm is selected. Splunk personnel outside the United Kingdom may access data in support and engineering.
Lighthouse Development Studio	Application development and technical support	Ukraine

Selecting a United Kingdom region governs where data is stored. It does not by itself keep every support or engineering interaction in the United Kingdom. Access of that kind is dealt with as a transfer in section 7.

6.2 Reward redemption partners

Where you redeem points with a partner brand, we share a redemption code required to fulfil that redemption. You will be told which partner is involved before you complete a redemption, and you can choose not to proceed.

6.3 Other disclosures

We may be required to make additional disclosures of your personal data to other parties where necessary to comply with the law or to perform necessary operations. Such examples may include:

- professional advisers, auditors and insurers, where necessary and subject to confidentiality.
- a regulator, court or public authority where we are required to disclose by law, or where disclosure is necessary to establish, exercise or defend legal claims.
- a buyer or prospective buyer in connection with a sale, reorganisation or financing of our business, subject to confidentiality and to the protections in this policy continuing to apply.

7. International transfers

Our intention is that storage and processing take place in the United Kingdom by default. Personal data may nonetheless be transferred to, or accessed from, other countries in the circumstances set out below.

Recipient	Country or region	Transfer safeguard
Google Cloud Platform	United Kingdom for data at rest. Support access from Google	Google Cloud Data Processing Addendum, which incorporates the standard contractual clauses and addresses UK GDPR

Recipient	Country or region	Transfer safeguard
	personnel outside the United Kingdom	
Junction	European Union (Belgium) where the EU region is selected, otherwise the United States	Transfers to the EEA are permitted under the UK adequacy regulations. If the US region is used, the International Data Transfer Agreement or the UK Addendum to the EU standard contractual clauses is required
Splunk	United Kingdom where the London realm is selected. Support and engineering access from outside the United Kingdom	Splunk EMEA data processing addendum, which applies the EU standard contractual clauses subject to the UK Addendum
Anthropic	UK, USA	Standard Contractual Clauses, incorporating the UK International Data Transfer Addendum

We offer the application to users in the United Kingdom, the European Economic Area, the United States and Ukraine. Where you use the application from a country outside the United Kingdom, your data will be transferred to the United Kingdom for the purposes described in this policy.

You can ask us for a copy of the safeguards we rely on by contacting us using the details in section 1.

8. Platform requirements

Where data reaches us through a device platform, that platform imposes its own conditions on how the data may be used. The following statements apply in addition to the rest of this policy.

- Data received through Apple HealthKit is used only to provide the features described in this policy. It is not disclosed to third parties except as permitted by the applicable Apple terms, and it is not used for advertising or for any similar service.
- Data received from wearable devices may be subject to the provider’s terms and conditions and privacy notices.
- Data received through Health Connect and / or the Google Health API is used and transferred in accordance with the applicable Google policies, including the Limited Use requirements. We do not transfer or sell this data to third parties such as advertising platforms, data brokers or information resellers, including where it has been aggregated or anonymised.

9. How long we keep data

The table below uses the same data types as section 5. Where we have not fixed a period, we keep the data for as long as it is needed for the purpose it was collected for, and for any further period during which a claim could be brought or the law requires us to keep it.

Data	Retention
Account and contact data	For as long as your account is open, and deleted on closure of your account.
Self-reported contextual answers (questionnaire data), in identifiable form	For as long as your account is open, subject to section 10.
Wearable, sensor and computed device data, in identifiable form	For as long as your account is open, subject to section 10.
Derived features produced by our processing	For as long as your account is open, subject to section 10.
Questionnaire data, device data and derived features after account deletion	Retained in the dataset in unlinked form, as described in section 10.
Device identifiers and technical data	12 months
Application usage telemetry	12 months
Diagnostic and crash data	12 months
Points balance and redemption records	For as long as your account is open and deleted on closure. Points balance will be retained for seven (7) days post-account closure.
Correspondence and support records	Six (6) years post correspondence.
Records we are required to keep by law	For the period required by the relevant law.

10. Deleting your account

You can delete your account at any time. It is important that you understand what deletion does and does not do.

- We delete the personal information held in your account and permanently break the link between you and the data you have contributed.
- That break cannot be reversed, including if you register again later with the same details. We will not be able to restore your contribution history, your points balance or any unredeemed rewards.
- The device data and contextual answers you contributed remain in the dataset in unlinked form and continue to be used for the purposes described in section 5.

- All accumulated points are lost in the event of the deletion of the account and cannot later be restored.

Data retained in this form is no longer personal data and is fully anonymised. This data cannot be re-linked to an individual even if the same user re-registers to use the application.

11. Automated decision-making and profiling

The questions you are presented with may be selected on the basis of the data you have already contributed and the research requirements of our clients.

We do not make decisions producing legal effects concerning you, or similarly significantly affecting you, based solely on automated processing.

The application does not provide medical advice, diagnosis or treatment, and nothing shown to you in it should be relied on for that purpose.

12. Your rights

Subject to the conditions and exemptions in data protection law, you have the following rights:

Right	**What it means**
Access	To be told whether we hold personal data about you and to receive a copy of it.
Rectification	To have inaccurate data corrected and incomplete data completed.
Erasure	To ask us to delete your data in the circumstances the law allows. Section 10 explains what deletion involves in practice.
Restriction	To ask us to limit our use of your data in certain circumstances.
Portability	To receive data you have provided to us in a structured, commonly used and machine-readable format, and to have it transmitted to another controller where technically feasible.
Objection	To object to processing carried out on the basis of our legitimate interests.
Withdrawal of consent	To withdraw consent at any time, as described in section 5.3.
Complaint	To complain to us about how we have handled your data, and to complain to a supervisory authority. How to do both is set out below.

To exercise any of these rights, contact us using the details in section 1, or use the controls in the application. We will respond within one month, and will tell you if we need longer because the request is complex or because you have made a number of requests.

If you wish to complain about how we have handled your data or your request, contact us first at privacy@atempora.co.uk. We will acknowledge your complaint and respond substantively within one month.

If you are not satisfied with our response, you can complain to the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, or through ico.org.uk. If you are in

the European Economic Area, you may complain instead to the supervisory authority in the country where you live or work, or where you consider the issue arose. Complaining to us first does not affect your right to go to a supervisory authority at any point.

13. Security

We maintain technical and organisational measures appropriate to the risk presented by the data we hold, including access controls, encryption of data in transit and at rest, logging and monitoring, and periodic review of those measures. No system can be guaranteed to be secure, and we ask you to keep your account credentials confidential.

14. Changes to this policy

We may update this policy to reflect changes to the application, to the providers we use or to the law. Where a change is material, and in particular where it introduces a new recipient of your data or a new purpose, we will tell you through the application or by contacting you directly, and we will give you at least 10 days' notice before the change takes effect. Where the law requires it, we will ask for your consent before the change takes effect, and in that case the change will not apply to you unless you give that consent.

Minor changes that do not affect how we use your data, such as corrections and clarifications, take effect when the updated policy is published, and the date at the top of this policy will be amended.

15. Cookies and similar technologies

The application stores information on your device where that is needed for it to work, for example to keep you signed in, to hold your settings, and to keep data safely on the device until it can be sent to us. Storage of that kind is necessary to provide the service you have asked for.

If we introduce storage or a similar technology that is not strictly necessary, such as separate analytics or an advertising identifier, we will ask for your consent before it is used and you will be able to withdraw that consent. This is required by the Privacy and Electronic Communications Regulations, which apply in addition to data protection law.

Our website at atempora.co.uk uses cookies. Those are dealt with in a separate cookie policy, which explains what each cookie does, how long it lasts, and how to change your choices. That policy is separate from this one, and choices you make on the website do not change the settings in the application.

Data received from Apple, Google and other device platforms is covered by section 8 rather than by this section.

16. Contact

Questions about this policy can be sent to privacy@atempora.co.uk, or by post to Atempora Ltd, 389 Queens Road, London SE14 5HD, United Kingdom.