



Data Protection Overview (UK)

To assist BetterPoint's Clients better understand how the BetterPoints Application uses the personal data of subscribers, we have prepared this overview. The information provided is drawn from the BetterPoints Application Data Protection Impact Assessment. If you have further questions, contact your BetterPoints representative.

SECTION 1: OVERVIEW

<p>What are the primary and secondary purpose of the BetterPoints Application?</p>	<p>The BetterPoints Application (App) encourages individuals to choose healthier and more sustainable behaviours. This is achieved through the use of behaviour change techniques within the App, including informing participants (“Subscribers”) about their activities; providing sources of knowledge and information needed to engage with and use support services; rewarding participants for engaging in healthy activities; and switching to sustainable transport modes.</p> <p>BetterPoints develops discrete challenges and activities delivered by the App with the aim of attaining specific outcomes (“programmes”). Metadata derived from the App is used to inform the development of individual programmes, promote programmes, and understand the success of programmes for internal and external (client) reporting. It is also used to segment and target users with personalised programmes of content and rewards.</p>
<p>What personal data is used?</p>	<p>This is recorded in a separate Record of Processing Activity (“RoPA”) and is further detailed in the BetterPoints privacy statement: https://www.betterpoints.ltd/privacy-app/</p>
<p>Who is the data controller?</p>	<p>BetterPoints Limited</p> <p>Whilst BetterPoints may be contracted to design and host programmes to provide desired outcomes that are defined by its Clients, BetterPoints exclusively determines the purposes and means of the processing of the personal data of subscribers to the App.</p> <p>Accordingly, BetterPoints is the data controller. BetterPoints does not process personal data on behalf of Clients.</p>

PROCESSING OVERVIEW STARTS ON THE NEXT PAGE

Processing Overview

How does the BetterPoint Application work and how is personal data is collected and used?

Overview

The App combines:

- (a) location tracking and motion & fitness sensing through (i) activation of sensors on a Subscriber's mobile device, and (ii) Subscriber interaction;

with

- (b) processing through sophisticated server-side algorithms to track and record subscriber journey activities and journey characteristics.

The personal data collected and created by the App, together with insight data created from further analysis of data collected by the App, is collated to:

- provide Subscribers with details of their activities and journeys;
- calculate rewards for Subscribers participating in Challenges; and
- tailor messaging and rewards;

Anonymised metadata derived from this data is also used for:

- research, system and product development; and
- to provide the sponsor of individual Challenges ("**Client**") with an analysis of the impact of Challenges.

Account Creation Stage

Potential Subscribers download and install the App from the Google Play Store (Android) or the Apple App Store (iOS).

Notifications:

The Subscriber is given the option to receive notifications via a prompt, where "Do Not Allow" is an option as well as "Allow". Either selection may be made. It is not a condition of the App to receive notifications.

Profile data:

The potential Subscriber is then prompted to provide the following data elements:

- First Name
- Last Name
- Gender
- Year of birth
- Email address

The Subscriber is provided with a link that explains in further detail why this data is needed to register for the App.

All the data requested must be provided (the gender field includes a “prefer not to say” response) before the Subscriber can move to the next step. However, this personal data is **not** transmitted to BetterPoints until the Subscriber submits it by selecting “JOIN NOW” on the final screen.

Additional data elements are able to be provided by the Subscriber in their profile at their option:

- Username
- Profile image (which may be any image uploaded by the Subscriber)

These optional data elements can be added after the account creation process has been completed.

Postcode

The Subscriber is then asked to provide their postcode. This is used to identify applicability for enrolment to specific programs or challenges.

Password creation and joining:

At this stage, a password is created by the Subscriber, with an eight (8) character minimum requirement, including 1 letter and disabling the use of the word “password” or use of the user’s email address in the password. The password is sent to BetterPoints before “JOIN NOW” is selected to verify that the password rules described above have been met. No other information is sent to BetterPoints until “JOIN NOW” is selected.

Users are asked to agree to the terms and conditions of the app, which are available to read via the (?) icon,

Users are asked to acknowledge the privacy policy (<https://www.betterpoints.ltd/privacy-app/>), which are available to read via the (?) icon.

Once “JOIN NOW” has been selected, an email verification will be sent to the email address provided by the Subscriber as part of their profile data (see above). If the email verification process is not completed within seven days (by the Subscriber clicking on the link provided in the verification email) the subscriber will become ‘Unconfirmed’ and logged out of the App. After 30 days (from date of account creation), ‘Unconfirmed’ accounts will be deleted.

Location tracking

“Location services“ (iOS, Android) is off by default.

Motion and Fitness tracking

“Motion & Fitness” (iOS) / Physical Activity/Body (Android) tracking is off by default.

Enabling Location and Motion & Fitness (Physical Activity) permissions

The first time the tracking toggle (at the top right corner of the app) is turned on, the user is asked for permission for the App to access the Location and Motion & Fitness permissions. As described in the Overview above, the App uses location data to be able to collate data about the Subscriber’s journey activities. The Subscriber is prompted to allow BetterPoints to process the location data for these purposes. At each step the reasons for the permission request are explained.

The App uses motion and fitness sensors to improve the accuracy of the Subscriber’s journey activities. The Subscriber is prompted to allow access to this function for this purpose. The reasons for this permission request is explained.

Email and notification preferences:

Subscribers will receive email and in-app notifications relating to their participation in BetterPoints. Subscribers who do not want to receive notifications by the App can disable this via the device settings, and can de-select the option to receive any emails from BetterPoints from within the App, via the Profile page.

App Engagement Stage:

Once the Account Creation Stage has been completed, the Subscriber can start interacting with the App, join Challenges, receive messages, earn rewards in the form of BetterPoints and BetterTickets, redeem points for vouchers in the in-app rewards catalogue or donate points to charity. BetterTickets automatically enter users into prize draws and they are informed of prizes via the in-App timeline or by email.

Tracking Toggle

If the Subscriber has not taken an action to toggle “On” the “Tracking” toggle in the top right corner of the App, neither the “Location services” nor the “Motion & Fitness” sensors are activated on the Subscriber’s device.

Challenge cycles

Challenge cycles comprise messaging (through the App), gamification of activity, tracking of App-engagement and participation in rewards (“**BetterPoints rewards**”). BetterPoints will design and implement challenge cycles that promote intended behaviours, or which otherwise support the Client’s transportation, health, or engagement objectives.

While challenge cycles can also be targeted and promoted by BetterPoints’ Clients, Subscribers remain data subjects in respect of whom BetterPoints is the data controller.

Baseline surveys

Before participating in a challenge, Subscribers are encouraged to complete a **baseline survey**. The purpose of this survey is to collect baseline data that supports the assessment of the success of a Challenge in attaining prescribed transportation, health, or engagement objectives. No special category data is collected as part of baseline surveys (such as health data).

RESPONSIBILITIES LINKED TO THE PROCESSING STARTS ON THE NEXT PAGE

Responsibilities linked to the processing

Who is the data controller?	BetterPoints Limited (“ BetterPoints ”)
Who are the data processors?	<p>This record is maintained as a part of the RoPA. The current data processors are:</p> <ul style="list-style-type: none"> • Microsoft Operations Ireland Limited (Azure Platform as a Service) • Cloudflare Inc (Cloudflare Web Application Firewall) • D.E.S. Computer Services Ltd (providing development and maintenance work for the App which may include access to personal data) • Google Firebase (enabling push notifications) • Google Workspace, Gmail (enabling relay service for sending email notifications to Subscribers via Google’s Gmail servers – back up service only) • ZenDesk (Client care support provider)

SECTION 2 (DATA PROCESSES AND SUPPORTING ASSETS) STARTS ON THE NEXT PAGE

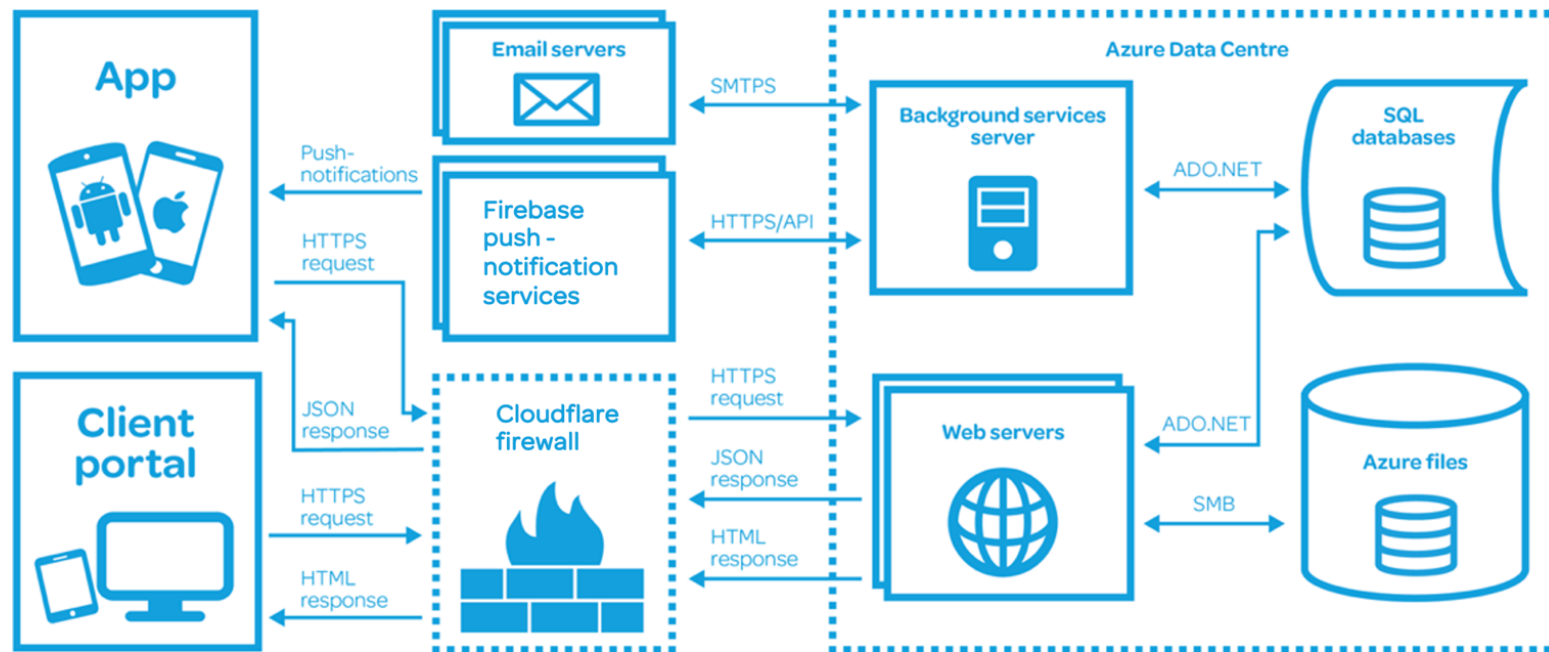
SECTION 2: DATA, PROCESSES AND SUPPORTING ASSETS

What categories of personal data are being processed?	See https://www.betterpoints.ltd/privacy-app/
Restrictions or prohibitions in respect of the processing of the personal data categories	<u>Generally</u> Processing of the personal data must meet the requirements of the UK GDPR and the Data Protection Act 2018 (each, as amended).

“HOW THE LIFE CYCLE OF DATA AND PROCESSES WORKS” STARTS ON THE NEXT PAGE

How the life cycle of data and processes work

Data flow overview



	Detailed Description of Process	Risks	Mitigations
What are the principal data flows?	<p>Generally See data flow diagram above.</p> <p>Overview Personal data is collected by BetterPoints both directly from individuals and indirectly from information location services and motion and fitness sensors on Subscriber devices collected through the Subscriber's device through the App.</p> <p>The personal data collected is transmitted by the Subscriber's device through third party networks and servers ("Network") to BetterPoints' Azure environment (the "BetterPoints Environment"), which hosts the application server and database.</p> <p>Account Creation Stage: Subscribers create an account and later log into the App using email and password credentials.</p> <p><u>Location services tracking</u> Location services tracking is disabled by default.</p> <p>Where Location services are enabled, the App collects "precise" location data and associated activity data (activity date, time, duration, route, likely mode of transport) ("Geolocation Data") using third party software embedded into the Application.</p>	<p>See specific risks identified below.</p> <p><u>Location services Tracking</u> Precise location data is highly sensitive data, despite not being special category data under Article 9 of the UK GDPR. For example, tracking precise location can reveal home location as well as travel sensitive locations, including places of religious or political exercise or locations where a particular type of health or medical care is made available (e.g., abortion clinics, HIV treatment centres, mental health treatment facilities, or other</p>	<p><u>Location services tracking</u></p> <ul style="list-style-type: none"> • BetterPoint's privacy statement clearly sets out the purposes for which personal data, including Geolocation Data, is used. This enables the Subscriber to make informed decisions as to whether or not they want to enable tracking.

	Detailed Description of Process	Risks	Mitigations
	<p>This is presented directly to the user through the App through and transmitted directly to BetterPoints (as described above).</p> <p>It is not collected or processed on BetterPoints' behalf by any third party.</p> <p><u>Motion & Fitness Activity Tracking</u> Motion and Fitness Activity tracking is disabled by default.</p> <p>The Subscriber is prompted to turn this on via native prompts of the operating system (iOS, Android text may vary).</p> <p><u>Analysis</u> BetterPoints analyses activity and Geolocation data within the BetterPoints environment.</p> <p><u>Notifications</u> Notifications and messages to Subscribers are issued from the BetterPoints Environment directly to the App through the network using Google Firebase.</p>	<p>highly sensitive health conditions or care).</p> <p>This collection may persist whether or not the Subscriber is using the App if "Always" is selected. The combination of these data elements with First Name, Last Name, Email, and Username elevates the risk.</p> <p><u>Motion & Fitness Activity Tracking</u> Motion & Fitness Activity is highly sensitive data which can also reveal disability status in the case of an individual with a disability with physical manifestation. Combined with the other identifying data elements like First Name, Last Name, email and username, this data heightens in sensitivity.</p>	<ul style="list-style-type: none"> • Location services tracking is disabled by default. • When tracking is enabled, this is clearly visible within the App through an icon which displays whether tracking is "on" or "off". <p><u>Motion & Fitness Activity Tracking</u> Training protocols for staff with access to Motion and Fitness Activity establishing the procedures for accessing the data to ensure it is not used in a way that infers health or disability.</p>

	Detailed Description of Process	Risks	Mitigations
Collection	<p><u>Account Creation Stage</u> Subscribers create accounts directly through the App, which can be downloaded from the Google Play Store or the Apple App Store.</p> <p>For additional information about the Account Creation Stage, see above.</p>	<p><u>Account Creation Stage</u> Over-collection of personal data (more personal data is collected than is necessary for the purposes it is to be used for).</p> <p>Data subjects are not provided with sufficient information on the uses of the personal data (transparency) at the point of collection.</p>	<p><u>Account Creation Stage</u> A detailed analysis of the necessity of collecting the categories of personal data sought has been completed, together with the lawful basis for that collection and associated processing (see Processing Review). In the context of the purposes of the App, the risks of over-collection are considered adequately mitigated.</p> <p>Personal data provided as part of the enrolment process is not actually collected until the potential subscriber finally creates the account. The enrolment process (and so collection of the personal data) is not completed until the account has been verified through the verification email.</p> <p>A privacy statement meeting the requirements of Articles 12 and 13 of the GDPR is made available to Subscribers. A link to this statement is available: on the BetterPoints website (https://www.betterpoints.ltd/privacy-app/); on the App page on Play Store and App Store; and from within the App itself.</p>

	Detailed Description of Process	Risks	Mitigations
	<p><u>Programme participation</u> When a subscriber participates in a programme, their account is associated with that programme to facilitate participation.</p> <p><u>Activity tracking</u> The App collects details of subscriber activities and journeys:</p> <ul style="list-style-type: none"> • Activity date • Duration of activity • Route of activity (geo-location data) • Mode of transport (where a journey), including location information and waypoints <p><u>Surveys</u> BetterPoints will conduct in-app surveys. These surveys are used for research, analytical, modelling, planning and statistical purposes. They are also used for user classification/segmentation and personalisation of content and rewards in the App. Surveys are collected through the App. Participation in surveys is always on a voluntary basis.</p>	<p><u>Programme participation</u> Data subjects are not provided with sufficient choice as to whether or not to provide personal data.</p> <p><u>Activity tracking</u></p> <ul style="list-style-type: none"> (i) Over-collection (ii) Lack of Transparency (iii) Lack of Choice <p><u>Surveys</u> See risks already identified in this section.</p>	<p>Pop-up summary privacy statements are provided at each data collection point to identify the purposes for which personal data provided as part of the subscription process is used. The verification email also includes a link to the privacy statements.</p> <p><u>Programme participations</u> Subscribers are not compelled to use the App.</p> <p><u>Activity tracking</u> See enrolment above. See also sections on necessity, proportionality, and effectiveness below.</p> <p><u>Surveys</u> See risk responses already identified in this section.</p> <p>Surveys that process special category data are reviewed by BetterPoints' independent Data Protection Officer to ensure specific risks associated with the survey are identified and managed.</p>

	Detailed Description of Process	Risks	Mitigations
Transportation	Data is transported between the App and the BetterPoints' environment through the network.	Interception of data during transportation	The network is supported by HTTPS certification. Data in transit is secured by encryption using Transport Layer Security.
Interrogation / Analysis	<p>BetterPoints interrogates and analyses personal data within the BetterPoints environment to:</p> <ul style="list-style-type: none"> • provide Subscribers information concerning their activities; • target functionality and challenges; • provide Subscribers rewards or recognition in respect of their activities in the context of specific programmes; • discover information in the form of metadata which is provided to Clients to inform conclusions and support decision making • perform analysis that informs future design and development of programmes, challenges, the BetterPoints application, administrators system and dashboards. 	<p>Interception of data during transportation.</p> <p>Failure to be transparent in respect of the processing operation.</p> <p>Presentation of personal data of one subscriber to another subscriber.</p> <p>Inaccurate or incorrect information provided to Subscriber.</p>	<p>See mitigations above.</p> <p>See mitigations above.</p> <p>Logical separation is based on User ID; log-in based on unique user credentials; and all information is queried on the application database using the user ID. BetterPoints allocates a unique (sequential) User ID against a unique (not previously registered) email address.</p> <p>The App can occasionally incorrectly attribute journey types to activity (e.g. a train journey is mis-identified as a bus journey). However, the user has the opportunity to override the inaccurate information.</p> <p>The development process includes testing of beta versions of the application by an internal testing group.</p>

	Detailed Description of Process	Risks	Mitigations
		<p>Incorrect allocation of Rewards.</p> <p>Failure to limit analysis to the purposes identified.</p>	<p>For each major application release, specifications will be shared with the Data Protection Officer to identify failures in privacy or information security.</p> <p>The App identifies who a user is. The activity is associated with the user (by way of the unique ID), allowing the system to allocate the reward to the user based on the activity associated with that user's unique ID. Where a user believes there has been an incorrect calculation or allocation of Rewards, BetterPoints can review and make manual adjustments where required.</p> <p>BetterPoints maintains a log of authorised purposes for analysis in central training documentation for members of the analysis team. Any updates are included in team-wide communications, along with a documented procedure for requesting authorisation of a new purpose</p>
Storage	The personal data is stored by BetterPoints in device (and in that respect is subject to the device security) and the Azure environment.	<p>Unauthorised access to stored personal data.</p> <p>Unauthorised or unintended breaches of data integrity.</p>	<p>See information security risk measures below.</p> <p>See information security risk measures below</p>

	Detailed Description of Process	Risks	Mitigations
		Data retained for a period longer than is necessary for the processing purposes.	Determined by the Subscriber. The Subscriber's personal data is deleted (or anonymised) once the account is closed. Subscribers can close their account by emailing BetterPoints or within the App itself (Profile > Edit Profile).
Deletion	Deletion is Subscriber managed by closing the account.	<p>Full deletes are not completed.</p> <p>Back-up data is not deleted and is recovered into live data.</p>	<p>Deletion is effected by removing identifiers from the relevant account record (email, password, gender, postal code, name, address (where provided), location, etc). Once the identifiers have been removed it is not possible to recreate the identifiers or associate the sanitised record with an individual.</p> <p>A procedure documenting the means and process for deleting personal data collected and processed by the application addresses the deletion of the account and/or requests from Subscribers to delete activities.</p>

Assets used in the data processing activities

	Description	Risks	Risk Mitigation <i>(state whether actual, planned or recommended)</i>
Assets	See the data flow diagram above. The Service is hosted entirely on the Microsoft Azure environment (Azure).	<ul style="list-style-type: none"> (i) Environment availability (uptime/failover). (ii) Loss of data on environment (back-up). (iii) Transfer of personal data outside the UK or countries with an adequacy decision. (iv) Environment security. 	<p>Azure operates a shared responsibility model under which clients (i.e. BetterPoints) are responsible for protecting the security of data and identities, on-premise resources, and the cloud components it controls (which varies by service type). This will always include: data; endpoints; account; and access management.</p> <p><u>Environment availability</u> Application server and database availability is maintained by Azure under an SLA, which provides for a 99.95% uptime. Currently, BetterPoints has determined in the context of the services it offers and the SLA provided by Azure, a redundancy environment is not required to allow for 100% availability.</p> <p><u>Loss of data</u> Back-ups have been enabled which provide a full back-up every 24 hours, plus an hourly log files back up.</p>

	Description	Risks	Risk Mitigation <i>(state whether actual, planned or recommended)</i>
			<p><u>Transfer of personal data</u> All personal data is hosted in the EEA.</p> <p><u>Unlawful access & Environment Security</u> Microsoft Azure benefits from STAR Level One and STAR Level Two certification and is a Cloud Security Alliance Trusted Cloud Provider. The Azure Consensus Assessments Initiative Questionnaire is available from the CSA website (and has been captured by BetterPoints).</p>

PROPORTIONALITY AND NECESSITY OF PROCESSING STARTS ON THE NEXT PAGE

SECTION 3: PROPORTIONALITY AND NECESSITY

Are the processing purposes specified, explicit and legitimate?

Processing purpose(s)	<p>Overall BetterPoints' technology and approach to behavioural change in the context of travel, health and sustainability is based on scientific research and analysis of factors that most influence individuals' decisions and long-term behaviours. These are reflected in the App and the programmes hosted by the app, in respect of which Subscribers are encouraged to participate. These are designed to inform Subscribers of their travel, health and climate impacting behaviours, interact with them in a way that stimulates greater consideration by Subscribers of their choices, provide challenges to change those behaviours, offer rewards for participation, and monitor change to track programme performance and outcomes.</p> <p>The App has been designed to (a) minimise the personal data collected; and (b) ensure Subscribers have complete choice as to the extent to which they participate in the programme in the context of transparency of how personal data is used.</p>	
	App functions or information use	Personal information collected and used
	Account creation and maintenance:	First Name, Last Name, email address, and unique password created by Subscriber, unique username created by Subscriber, photo of Subscriber (optional)
	Targeting app functionality (including access to the app) to specific groups or Subscribers: Attribute information to specific groups or Subscribers for research, analytical, modelling, planning, and statistical purposes:	Year of birth, gender, country, and postal code.

	Sending notifications (not marketing notifications) to Subscribers, including account set-up verification and messages about your interaction with the application:	First Name, email address.
	In-app surveys and collation and use of responses for research, analytical, modelling, planning, and statistical purposes:	BetterPoints may invite Subscribers to participate in surveys. Subscribers are not required to participate but if they do they may be providing additional details.
	Delivering activity related rewards or prizes:	First Name, Last Name, email address, postal address.
	Providing Subscribers with details of their activities and journeys:	(A) Activity date, time, duration, journey route on map. (B) Length of journey/activity; route of journey/activity; modes of transport (including location information and waypoints, provided through the tracking function of the app). (C) Precise Location
	Participation in challenges and prize draws:	
	Reviewing your activities for research, analytical, modelling, planning, and statistical purposes (information analysis):	
	Maintenance of BetterPoints	User account details and BetterPoints balances.

	Necessity	Effectiveness	Proportionality
Proportionality	<p>Overall Under UK law, personal data may only be collected and used (processed) if one or more of the lawful bases of processing set out in the UK GDPR and Data Protection Act 2018 applies.</p> <p>Utilising the App and participating in its programmes is entirely at Subscriber's discretion. In the context of the purpose of the programmes, the personal data collected is necessary to ensure the programme aims can be met.</p>	<p>BetterPoints designs behaviour change programmes which are delivered via the App.</p> <p>The effectiveness of the programmes are monitored continuously by reviewing self-report and tracked data which has been collected in the App.</p> <p>Using these data points, interventions may be adapted over the course of the programme to ensure the programme is delivering the aims which have been agreed with the client. These intervention updates may be rolled out programme-wide, or targeted at specific users/user groups who are not demonstrating behaviour change.</p> <p>All programme undergo an end-of-challenge evaluation by BetterPoints which measures the effectiveness of each programme. These evaluations are delivered to the client.</p> <p>Case studies and various industry presentations are on record to demonstrate the effectiveness of BetterPoints programmes.</p>	<p>In the context of the purpose of the App and its programmes, as well as the means required to deliver the outcomes, the personal data collected and processed is considered to be proportionate to its aims.</p>

		An 80% programme renewal rate demonstrates the effectiveness of the programmes at delivering client aims.	
--	--	---	--

THE LEGAL BASIS MAKING THE PROCESSING LAWFUL APPEARS ON THE NEXT PAGE

The legal basis making the processing lawful

	Lawful basis adopted (or not required)
What is the lawful basis of processing?	See https://www.betterpoints.ltd/privacy-app/

Is the personal data collected adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed?

Personal data category:	Why the personal data is required	Controls in place to minimise the personal data used
Account creation and maintenance: Name, email address, unique password	This is the minimum personal data required to associate an account with a specific user and ensure the security of the account for that user.	The application's use of personal data has been assessed in the context of the purposes of the application and the functionality it provides. All future changes to the application are required to be assessed by the independent Data Protection Officer to ensure the changes align with the requirements of the UK GDPR, the Data Protection Act 2018 and all other relevant standards.
Targeting app functionality (including access to the app) to specific groups or users: Age, gender, location and postal code	This personal data is required to ensure Subscribers are associated with the correct programmes. Programmes are designed and managed to deliver specific outcomes for clients and can be demographic, behaviour/ health status and geographic specific.	See "Account creation and maintenance" above.

Personal data category:	Why the personal data is required	Controls in place to minimise the personal data used
<p>Attribute information to specific groups or users for research, analytical, modelling, planning, and statistical purposes: Age, gender, location, and postal code</p>	<p>BetterPoints creates important metadata points from the activities of Subscribers and their interactions with programmes. This provides information to clients in respect of the programme and its attainment of the outcomes sought. It also informs BetterPoints on the success of programmes and factors (including demographic and geographic) that influence outcomes.</p>	<p>See “Account creation and maintenance” above.</p>
<p>Sending notifications to Subscribers: First Name, email address</p>	<p>This is the minimum personal data required to send notifications to Subscribers by email.</p>	<p>See “Account creation and maintenance” above.</p>
<p>In-app surveys and collation and use of responses for research, analytical, modelling, planning, and statistical purposes: Responses to questions specifically developed for a particular survey (survey data)</p>	<p>This will be survey specific. However, surveys are designed so that they provide specific information to BetterPoints and its clients in respect of the programme and its attainment of the outcomes sought.</p>	<p>See “Account creation and maintenance” above.</p>

Personal data category:	Why the personal data is required	Controls in place to minimise the personal data used
<p>Providing Subscribers with details of their activities and journeys; participation in challenges and prize draws; and reviewing activities for research, analytical, etc, purposes:</p> <p>A: Activity date, time, duration, journey route on map.</p> <p>B: Length of journey/activity; route of journey/activity; modes of transport (including location information and waypoints, provided through the tracking function of the app)</p> <p>(together, “activity data”)</p> <p>C. Precise Location</p>	<p>This personal data is fundamental to the operation of the App and is required for the specific purposes identified.</p>	<p>See “Account creation and maintenance” above.</p>

Is the data accurate and kept up to date?

Personal data category:	How accuracy of personal data is assured	How accuracy of personal data is maintained
<p>First Name, Last Name, gender, username, photo (optional)</p>	<p>Data subjects provide the personal data in the first instance.</p>	<p>Subscribers may modify the profile information by the Edit Profile option in Settings.</p>

Personal data category:	How accuracy of personal data is assured	How accuracy of personal data is maintained
Email address	Data subjects provide the personal data in the first instance. Emails are verified through the initial email verification.	The personal data is not amended other than at the request of the data subject.
Country and postal code	Data subjects provide the personal data in the first instance.	The personal data is not amended other than at the request of the data subject.
Activity data	Classifiers on phone, accelerometer and speed data are all used to classify mode of travel. Bus and train route data from open street map and transport operators are also used to verify transport mode.	The personal data is not amended. However, Subscribers are able to change the mode of transport for any specified journey in the event the application incorrectly assigns the mode of transport.
Precise Location data	Precise Location is activated at the Subscriber's option. The location services sensor on the Subscriber's device ensures accuracy, though in different geographies the accuracy could vary.	The individual would not be able to modify the location, as the location services would either be off or on.
Survey data	Data subjects provide personal data directly and is intended to be representative at the point of initial collection.	Not applicable.

Personal data category:	How accuracy of personal data is assured	How accuracy of personal data is maintained
BetterPoints data (reward points)	BetterPoints (etc) are allocated to users based on their completion of activities. BetterPoints are aggregated in a virtual wallet unique to the user. These “Activity Rewards” (ARs) can be for a range of activities including tracked physical activity or more static activities such as checking into a clinic or class. Reward points can also be won in prize draws, usually in pots of points worth between £5 and £100.	

What is the retention period for the data?

Personal data category and type	Retention period and deletion method
	All personal data as identified in the preceding sections is retained until the account is closed by the data subject. This allows the data subject to retain a record of all their interactions with the app whilst they maintain their account. Unconfirmed accounts are deleted 30 days from their creation date. Subscribers can also close their accounts directly through the application or request this through BetterPoints.

SECTION 4 (CONTROLS TO PROTECT THE PERSONAL RIGHTS OF DATA SUBJECTS) STARTS ON THE NEXT PAGE

SECTION 4: CONTROLS TO PROTECT THE PERSONAL RIGHTS OF DATA SUBJECTS

How data subjects are informed about the processing?

Description of methodology
<p>A privacy statement meeting the requirements of Articles 12 and 13 of the GDPR is made available to Subscribers. A link to this statement is available: on the BetterPoints website (https://www.betterpoints.ltd/privacy-app/); on the App page on Play Store and App Store; from within the App itself, and through links available in the verification email.</p> <p>Pop-up summary privacy statements are provided at each data collection point to identify the purposes for which personal data provided as part of the subscription process is used.</p> <p>A link to the privacy statement is included in the Personal Info section of the App.</p>

How is the consent of data subjects obtained?

Description of consent mechanism
<p>Consent is the lawful basis of processing in respect of the capturing of activities and journeys through the tracking function. See above in respect of turning tracking on, and off.</p>

How can data subjects exercise their rights?

Personal data right	Description of system
Rights of access	Data subjects can currently access much of their personal data directly from within the App. They can make a request for other personal data via email.
Rectification	Data subjects can modify their personal data Edit Profile option in Settings where available and otherwise via request to the support team.
Erasure	See above.
Restrict processing	At this time, the user sends an email to BetterPoints to exercise this right. The request would be handled by the Data Protection Officer.
Object to processing	At this time, the user sends an email to BetterPoints to exercise this right. The request would be handled by the Data Protection Officer.

In the case of data transfers outside the jurisdiction of origination, how is that data transfer lawfully made?

Personal data category / data set	Jurisdiction transferred to	Mechanism for lawful transfer
Personal data processed as part of the web application firewall (headers, payload of request)	Cloudflare Inc (United States)	EU-US Data Privacy Framework and the UK extension to the EU-US Data Privacy Framework.
Personal data processed as part of Client support	Zendesk, Inc (United States)	EU-US Data Privacy Framework and the UK extension to the EU-US Data Privacy Framework.
Personal data incidentally processed as part of the provider's support services	D.E.S. Computer Services Limited (United Kingdom)	Adequacy

SUMMARY OF INFORMATION SECURITY RISK CONTROL MEASURES APPEARS ON THE NEXT PAGE

SECTION 5: SUMMARY OF INFORMATION SECURITY RISK CONTROL MEASURES

Control	Summary
Information Security Management System	BetterPoints operates an Information Security Management System meeting the requirements of IS 27001:2022, and has been assessed against that standard.
Encryption	<p><u>In transit</u> Data is transmitted over the network using TLS 1.2 or above (TLS 1.1 has been disabled in the Cloudflare application firewall).</p> <p><u>At rest</u> Data stored on Azure is encrypted at rest by default, using an Azure encryption key. Azure has established and implemented procedures to enforce segregation of key management and key usage duties. Azure key management encompasses the entire life cycle of cryptographic keys and has identified a method for establishing and managing keys in each management phase from generation, installation, storage, rotation and destruction. Azure's cryptographic controls are reviewed and verified by external auditors in ISO27001, SOC and etc.</p> <p><u>Device encryption</u> Device specific and in control of the user. Encrypted in transit for the Web Application log-in TLS 1.2 and above.</p>
Anonymisation	<p>Personal data is not anonymised until it is deleted in the database.</p> <p>For data exports a pseudonymisation key is deployed, replacing data that can be used to identify an individual (such as Client ID and postal code) with a random string or sequential number meaning that no personal data is made available to the recipient of the data export.</p> <p>Passwords are stored on the Azure database using hash/salt key.</p>
Data partitioning	Separate virtual machines for the web servers and work services use a common database for the relevant BetterPoints application, but segregated to process the data and run individual databases. The application segregates data based on the unique, sequential, User ID (which is not repeated or re-used). The User ID associates all data on the database with the individual to whom it is assigned. If a user ID is not associated with a data element or object, then the element or object is not recoverable.

Control	Summary
Logical access control	<p><u>Azure databases</u> Direct access to the databases is limited to the BetterPoints administration team. Direct access to the databases is IP address restricted and requires two factor authentication (locked down to static IP address of the system admin team). This is repeated for access to the application server controls.</p> <p><u>Web portal</u> RR28 - Unique log-ins are required to access the administration portals (requiring a unique email address and password). Currently, there is no TFA/MFA (only username/password – password rule is 8 letter/number characters). There is no periodic force change.</p> <p>There are no IP access controls.</p>
Traceability (logging)	Full web logs (historic style IIS logging style; Azure web logs (30 days); and database call logs are available. Date exports are specifically logged, including parameters used and who completed the export.
Integrity monitoring	Azure Defender has been implemented.
Operating security	Microsoft Azure benefits from STAR Level One and STAR Level Two certification and is a Cloud Security Alliance Trusted Cloud Provider. The Azure Consensus Assessments Initiative Questionnaire is available from the CSA website (and has been captured by BetterPoints).
Clamping down on malicious software	<p><u>Azure</u> Connections to Azure servers are limited and “closed”. Cloudflare is deployed to filter requests before they are sent to the Azure servers and is IP locked to communicate with Azure over a TLS link. Microsoft Azure benefits from STAR Level One and STAR Level Two certification and is a Cloud Security Alliance Trusted Cloud Provider. The Azure Consensus Assessments Initiative Questionnaire is available from the CSA website (and has been captured by BetterPoints).</p> <p><u>Staff machines with access to BetterPoints web application portal</u> Staff machines are all independent, with no central control or centrally deployed protections.</p>

Control	Summary
Website security	End users are not directly accessing the websites – no link to database from public URL.
Back ups	Back-ups have been enabled which provide a full back-up every 24 hours, plus an hourly log files back up
Security of networks	Internal Azure controls – only accepts connections from webserver and BP office.
Physical access control	Microsoft Azure benefits from STAR Level One and STAR Level Two certification and is a Cloud Security Alliance Trusted Cloud Provider. The Azure Consensus Assessments Initiative Questionnaire is available from the CSA website (and has been captured by BetterPoints).
Hardware security	Microsoft Azure benefits from STAR Level One and STAR Level Two certification and is a Cloud Security Alliance Trusted Cloud Provider. The Azure Consensus Assessments Initiative Questionnaire is available from the CSA website (and has been captured by BetterPoints).
Avoiding sources of risk	Microsoft Azure benefits from STAR Level One and STAR Level Two certification and is a Cloud Security Alliance Trusted Cloud Provider. The Azure Consensus Assessments Initiative Questionnaire is available from the CSA website (and has been captured by BetterPoints).
Protecting against non-human sources of risks	Microsoft Azure benefits from STAR Level One and STAR Level Two certification and is a Cloud Security Alliance Trusted Cloud Provider. The Azure Consensus Assessments Initiative Questionnaire is available from the CSA website (and has been captured by BetterPoints).
Pen Testing	Periodic pen testing not yet fully implemented, but provided for clients on demand.

For further information, please contact privacy@betterpoints.uk