1 Data Privacy and Security Summary

This service is provided by Aseptika Ltd. Our services are developed and operated with a set of key principles which ensure the security and privacy of you and the family members that you care for using the functionality it provides under the legal basis of UK GDPR Article 6(1)(a), where Aseptika is the Data Controller.

1. We never access the data that you generate unless you have provided consent for us to do so. Usually this is so we can provide you with technical support or as part of a research project or clinical service to which you have previously provided your informed consent.
2. All data transmitted to and from our Apps (Active^{+}me REMOTE, Asthma^{+}me and Activ8rlives^{4} Health+Wellness App) and the Activ8rlives Cloud service, is encrypted to appropriate standards for your security.
3. Many other health Apps generate revenues by selling your anonymised data to advertisers. We have not and will never do this with your data. We do not generate revenue by selling advertising space to third-parties who use anonymised personal data to target advertisements for specific products to you. For this reason, some of our services are a subscription or are prescribed. This protects you and the data you collect.
4. We do not share, sell or give your data with any third-parties, other than trusted health and social care systems and only if this is with your informed consent.
5. Export to trusted health and social care systems, with your informed consent, can be enabled so that a specific care service may be provided to you. This will only be enabled with your informed consent and following the completion of an appropriate identification process. When you consent to share your data with trusted health and social care systems, Aseptika becomes the Data Processor on the legal basis of UK GDPR Article 6(1)(e). The operator of the trusted health and social care system becomes the Data Controller on the legal basis of UK GDPR Article 9(2)(h).

2 Information we receive and how it is used

2.1 Information we receive about you

When you use an Aseptika software product, we access, collect and use a number of different types of information about you, including:

- Your Data: “Your Data” is the information that is required when you sign-up for the use of our services through a website or mobile application, as well as the information you choose to share.

- Registration information: When you sign-up for our services, you may be required to provide your name, email address, gender, age, ethnicity and other information, such as weight, height, activity levels or NHS number (UK citizens only).

- Information you choose to share: Your information also includes the information you choose to share on our services, such as when you post a comment, upload a photo or comment on a group messaging system.

- Information we collect to provide service functionality to you: Depending on the service you use, this may include activity data, location data, health and fitness data and physiological data.

The data we collect is categorised as follows:

Data Type	Required	Stored	Shared with third parties	Reason
Personal information, such as name, email address and user IDs	Yes	Yes	Never	Account management, app functionality
Personal information, such as address, phone number and ethnicity	No	Yes	Never	Account management, app functionality
Location	No	No	Never	App functionality
Messages	No	Yes	Never	App functionality
Photos	No	Yes	Never	App functionality
Health information	No	Yes	Never	App functionality
Fitness information	No	Yes	Never	App functionality
App crash and diagnostic logs	Yes	No	Never	Analytics

It also includes the information you choose to share when you take an action, such as when you add data about yourself.

Your profile picture and nickname are treated just like information you choose to make public.

2.2 Other information we receive about you

Aseptika also receives other types of information about you:

- We may receive data about you whenever you interact with our services, such as when you look at another group's profile, send someone a message or purchase one of our products.

- When you post things like photos or videos on our services, we may receive additional related data (or metadata), such as the time, date and place you took the photo or video.

- We may receive data from the computer, mobile phone, tablet or another device you use to access our services. This may include your IP address, location, the type of browser you are using, Bluetooth devices you are connected to, type of smart device and operating system.

- We do not store credit card or customer financial details.

2.3 Public information

When Aseptika use the phrase “public information” (which we sometimes refer to as “Everyone information”), we mean the information you choose to make public, as well as information that is always publicly available.

2.4 Information you choose to make public

Our services also include a messaging system. This should be treated like any social media service. Any content you choose to post, including any personal information, is public to all members of the group and all future members of the group. This also includes the name and profile picture associated with your account.

Ensure you wish to post this content publicly before proceeding.

Any messages posted must abide by our Terms and Conditions of Use.

External Browsers cannot search user accounts on our service, so your information will not be public beyond those within our service that you have given permission to view your public information.

2.5 Deleting and deactivating your account

If you want to stop using your account, you can either deactivate or delete it by:

2.5.1 Deactivation

Deactivating your account puts your account on hold. Other users will no longer see your profile, but we do not delete any of your information. Deactivating an account is the same as you telling us not to delete any information because you might want to reactivate your account at some point in the future. You can deactivate your account by writing to us by email: support@aseptika.com

2.5.2 Deletion

When you delete an account, it is permanently deleted from our services. It typically takes around 48 hours for an account deletion request to be processed. You should only delete your account if you are sure you never want to reactivate it. You should be aware that some information about you may remain in the service if you have posted on the messaging system. You can delete your account by writing to us at: support@aseptika.com

You can also request deletion of your account direct from the app settings.

2.6 Public search engines

Our services cannot be searched by a public search engine. Neither your data or your groups are searchable with a public search engine.

2.7 Minors and safety

Aseptika take safety issues very seriously, especially with children and we encourage parents to teach their children about safe internet practices.

To protect minors, we may put special safeguards in place (such as placing restrictions on the ability of adults to share and connect with them), recognising this may provide minors a more limited experience on our services.

2.8 Responding to legal requests and preventing harm

We may share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United Kingdom, where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction and is consistent with internationally recognised standards. We may also share information when we have a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity, to protect ourselves and you from violations of our Rights and Responsibilities and to prevent death or imminent bodily harm.

2.9 Notifications and Other Messages

We may send you notifications and other messages using the contact information we have for you, like your email address. We never share your email address with any third-party.

2.10 Invitations

When you invite another person to join our services, we send a message on your behalf using your name and up to two reminders. The invitation will also give the other person the opportunity to opt out of receiving other invitations to join our service.

2.11 Memorialising accounts

Aseptika may memorialise the account of a deceased person. When we memorialise an account, we keep the profile on our services. You can report a deceased person's profile by writing to us by email at: deceased@aseptika.com. We also may close an account if we receive a formal request from the person's next of kin.

2.12 Service Providers

Aseptika may need to give your information to the people and organisations that help us provide the services we offer. For example, we may use outside vendors to help host our website, serve photos and videos, process payments, shipping or provide search results. In some cases, we provide the service jointly with another organisation, such as an eCommerce Marketplace. In all of these cases our partners must agree to only use your information consistent with the agreement we enter into with them, as well as this privacy policy.

2.13 Healthcare service provision

Aseptika typically acts as the Data Processor and Controller for your data when you sign up to use our services, under the legal basis of UK GDPR Article 6(1)(a). However, when you consent to share your data with a trusted health or social care provider, Aseptika becomes the Data Processor, under the

legal basis of UK GDPR Article 6(1)(e) and the operator of the health and social care provider becomes the Data Controller, under the legal basis of UK GDPR Article 9(2)(h).

2.14 NHS login

Please note that if you access our service using your NHS login details, the identity verification services are managed by NHS England. NHS England is the Data Controller for any personal information you provided to NHS England to get an NHS login account and verify your identity and uses that personal information solely for that single purpose. For this personal information, our role is a Data Processor only and we must act under the instructions provided by NHS England (as the Data Controller) when verifying your identity. To see NHS login's Privacy Notice and Terms and Conditions, please click here. This restriction does not apply to the personal information you provide to us separately.

2.15 Security

Our services are developed with a privacy first principle to ensure we maintain the best possible standards for keeping the data you choose to store with us secure.

All data in our platform is stored in the UK and never leaves the UK.

Aseptika maintains a Cyber Essentials Plus certification, is compliant with the NHS Digital Technology assessment Criteria (DTAC) and NHS Data Security and Protection Toolkit.

While we maintain our high standards of security, we appreciate your help with this by asking that you use our service responsibly.

2.16 Change of Ownership of Aseptika

If the ownership of our business changes, we may transfer your information to the new owner so they can continue to operate the service. But they will still have to honour the commitments we have made in this privacy policy.

2.17 Notice of Changes

If we make changes to this Privacy Policy, we will notify you by publication here and on the Activ8rlives site. If the changes are material, we will provide you additional prominent notice as appropriate under the circumstances.

3 References

ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection — Information security management systems
BS EN ISO/IEC 27701:2021	Information Security Techniques - Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management
ISO 27033-6 IEC/EN 2016	Information technology — Security techniques — Network security — Part 6: Securing wireless IP network access
WCAG 2.1	Web Content Accessibility Guidelines 5 June 2018
NHSx DTAC	Digital Technology Assessment Criteria

NHS	The Information Security Management: NHS Code of Practice April 2007
NHS DSPT	NHS Data Security & Protection Toolkit
Cyber Essential Plus	Cyber Essentials & Cyber Essentials Plus
ICO.org	Personal data breaches: Information Commissioners Office
ICO.org	The Information Commissioner's Office (ICO) Guide to Data Protection
MDCG 2019-16 Rev.1	Guidance on Cybersecurity for medical devices

4 Document History

Version	Date	Authors Initials	Reviewers Initials	Changes from Previous Version	Authorised by & date
1.1	24.07.2016	KAA		Needs review	
1.2	28.2.2018	KAA		Made public document	
1.3	03.05.2018	ETRA		Update to a new template and a new name of the document	
2.0	11/12/2018	ETRA	KAA, JAA, CB	Annual review and part of CC2018-0187	
3.0	02.12.2019	JA	MP	MDR Transition update, part of CC2019-057	KAA
4.0	23.11.2021	JA	GE	Annual review CC2021-075	Kevin A Auton 23.12.2021
5.0	07.03.2022	JA	GE	Change language CC2022-018	Kevin Auton 18.03.2022
6.0	28.10.2022	JA	GE	Migrate to AWS CC2022-063	KAA authorise JA 02.11.2022
7.0	14.08.2023	CB	MC	Update for NHS login CC2021-037	JA 14.08.2023
8.0	08.09.2023	JA	-	Additional clause CC2023-010	KAA authorise JA 08.09.2023
9.0	27.10.2023	JA	CB	Update for NHS login CC2023-034	KAA 27.10.2023
10.0	12.02.204	JA	SW	Update GDPR CC2024-004	KAA authorise JA 11.03.2024