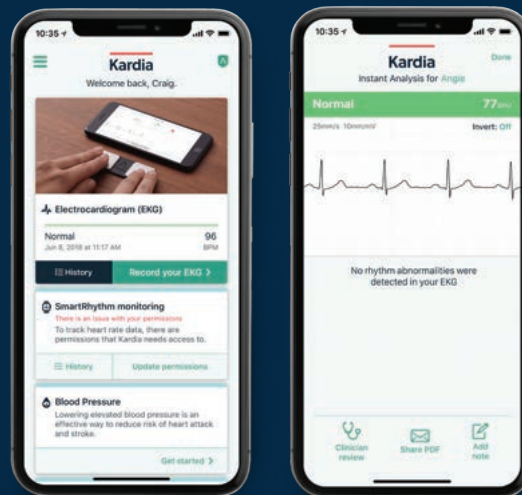


GDPR Consumer FAQ Sheet



AliveCor is committed to protecting our customers by achieving a high standard of data security and compliance in line with GDPR (General Data Protection Regulation) requirements. As our organisation scales, we continue to evolve and adapt our data governance and protection strategies, and strive to provide secure technology services to our customers.

This document is provided as a quick reference to frequently asked questions on how AliveCor handles your data and is not a replacement for AliveCor's official privacy policy, which can be found at alivecor.co.uk/privacy.

How does AliveCor handle my personal information and what are my rights?

Individuals located in the European Economic Area (EEA) have several enumerated rights in how AliveCor handles your personal information. AliveCor acts as Data Controller of your information with very few exceptions (e.g., your healthcare provider generates your Kardia account and provides you access credentials). You should contact AliveCor directly for all requests to exercise your rights under GDPR and for any other concerns you may have about the privacy of your personal information, including:

- The right of access to your personal data;
- The right to correct or rectify any inaccurate personal data;
- The right to restrict or oppose processing of personal data;
- The right to erase your personal data; and
- The right to personal data portability.



To contact an AliveCor Data Controller Representative please email privacy@alivecor.com.

How is my data stored within the EU?



- All data for EEA users are stored securely in the EU (Amazon Web Services in Germany)
- All data is fully encrypted at rest and in transmission
- No data stored in EU data servers will be transmitted to countries outside the EU*
- In standard / premium / KardiaCare mode data is stored in the app locally on the phone and in a secure cloud
- Device and cloud storage can be switched off in the app for users that have additional privacy concerns, where the data will not be stored/backed up in the cloud or locally on your device.

**When you make a request for support, the data you include in that request is sent to AliveCor support staff in the US and used for the sole purpose of providing the support you requested.*

How is my data used?



We rely on user consent as a lawful basis processing personal data for the following purposes:

1. Initial collection of personal data through the Service
2. If users opt-in, providing users with marketing or promotional communications. Users may opt out of such communications at any time by clicking the "unsubscribe" link found within the communications and changing their contact preferences.

Data of European users will not be used for any purpose such as studies or product development.

If you would like to find out more about our privacy and security policy please visit alivecor.co.uk/privacy

AliveCor®