

Privacy Policy

Last modified: September 24, 2018.

On this page we inform you about our policy regarding the collection and use of personal data that we obtain in the context of the SMARD service.

Your personal data will only be used in formal scientific research projects where your participation in a project has been approved by you in advance. When you use the SMARD app, you agree to the collection and use of your personal data in accordance with the conditions in this document.

Data

The collection of personal data through your smartphone is an existing and frequently used means for various purposes used by various (market) parties. SMARD is also within this spectrum and is exclusively intended to support scientific studies on human behavior. SMARD will therefore only be installed and activated on your smartphone with your explicit consent and after you have been fully informed about the nature of this mobile application. Within scientific research projects, this process is also known as 'informed consent'.

SMARD collects various types of data, including: your answers and response to the tasks that you receive through the SMARD app. Each data is accompanied by additional information such as the date and time. We never store information regarding the content of your spoken and / or written messages. Identifying information about you or others within your knowledge circle (such as telephone numbers) will not be collected.

Cookies

Cookies are files with a small amount of data often consisting of unique serial numbers. SMARD does not use cookies.

Safety

The security of your personal data is very important to us, and although no method of digital processing and storage is completely invulnerable, we strive to ensure the safe storage of your data and thus your privacy through combinations of security measures.

- Basically no directly identifiable information (eg, data, etc.) about you is included in services that are part of SMARD. Participants are only represented in our systems by a unique serial number, this number can and will probably be included for registration in separate decentralized monitoring systems of care and / or scientific institutions.
- All measurement data collected by the mobile application is encrypted before it is saved on the device.

- After each successful synchronization of measurement data by the mobile application, it is deleted from the device. If your device is lost, you can report this to your study manager, who will re-initialize your account so that the mobile application on your existing device, if it is still online, will fully reset itself and all collected measurement data will be removed from the device.
- All digital communication flows to and from central components within the SMARD service take place over secure connections.
- The SMARD service is hosted on the Google Cloud Platform, this platform is built on a security model with 15 years of experience in protecting user data. The platform is HIPAA and ISO 27001 certified with which it also complies with European data protection rules. Finally, SMARD data is stored encrypted within this platform so that only authorized researchers within the team can access the data.

Our privacy policy will be subject to change over time. You will be informed by us of these changes. However, we encourage you to review the privacy policy from time to time for changes.

Contact

For questions about our privacy policy, please contact us via smard.psy@radboudumc.nl .