mindsampler

Data Security and Privacy

Information for Institutional Review Board

1. Summary

MindSampler is a mobile application designed for secure and user-friendly experience-sampling data collection. As devoted researchers, we are committed to the highest ethical standards. The following comprehensive guide explains how MindSampler manages data, emphasizing our robust security, compliance with regulations, and meticulous privacy measures.

2. Purpose & Platform

MindSampler, available across both iPhone and Android devices, offers a streamlined interface for participants to respond to studies designed by researchers.

The core mission of the app is to foster efficient and secure data collection, always respecting participant privacy.

3. Data Protection Measures

Encryption and Security Protocols

MindSampler utilizes Transport Layer Security (TLS) encryption for transmitted data and follows stringent firewall protection measures. Regular audits and reviews are conducted to ensure persistent compliance with GDPR and HIPAA guidelines.

Hosting by Google Cloud Platform (GCP)

MindSampler's services are hosted by Google Cloud Platform (GCP), with servers located specifically in Europe. This ensures compliance with the General Data Protection Regulation (GDPR), aligning with the region's robust privacy and security standards. Google Cloud is renowned for its secure infrastructure, meeting the demands of security-conscious organizations, and adhering to global standards, including ISO 27018. MindSampler's commitment to these standards emphasizes its dedication to ensuring the privacy and security of user data in line with international laws and best practices.

4. Data Collection and Usage

Personally Identifiable Information (PII)

MindSampler does not request PII from participants. Participants can sign up either completely anonymously or using their email, adapting to the requirements of researchers and the IRB.

Passive Information Security Protocols

MindSampler respects participants' privacy and autonomy when collecting passive information. Upon the app's installation, participants are greeted with a clear notification detailing the potential sharing of sensor data pertinent to their study. Rather than seek broad permission, MindSampler employs a granular, sensor-by-sensor opt-in process. This approach guarantees that participants are fully aware of the specific sensor data they authorize. Additionally, explicit consent is acquired through individual push notifications for each sensor, ensuring that data collection is always intentional and fully approved by the participant. This sensor data, encompassing metrics like accelerometer readings and ambient decibel levels, serves to augment the depth and accuracy of the research. Importantly, this data is only relayed to researchers after obtaining unequivocal participant consent, which they can revoke at any time. This reinforces our commitment to transparency, participant agency, and stringent security, aligning with the most rigorous ethical standards.

Survey Data Handling

MindSampler uses researchers' own Qualtrics accounts for the secure storage of survey answers. This has two major advantages in terms of data privacy and security.

- **Data safety.** Qualtrics emphasizes data protection with high-end firewall systems, regular vulnerability scans, and annual third-party penetration tests. Qualtrics holds notable certifications, including SOC 2 Type II for Security, Availability, and Confidentiality; ISO 27001, 27017, and 27018; FedRAMP Authorization; IRAP compliance; HITRUST for healthcare; TISAX for the German automotive industry; and PCI certification for call recordings.

- **Data Ownership & Visibility.** All study responses are owned by the researcher who created the study. MindSampler's design ensures that participant responses are directly stored in the researcher's Qualtrics account. The MindSampler team cannot access these responses unless the researcher explicitly transfers specific data to MindSampler's servers for advanced functionalities, such as follow-up surveys or personalized app feedback. In the latter case, only senior MindSampler managers trained in data privacy can access our backend database. Access to all of our backend services is logged and audited.

5. Compliance with Regulations

MindSampler's operations and data management practices comply with the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). This ensures the highest level of data privacy and security for both European and American participants.

6. Data Retention and Deletion

Participants can choose to uninstall the app at any juncture. They hold the right to request data deletion, which can easily be done from the app and is executed within 30 days of the request. Our compliance with GDPR grants participants the right to data portability, access, and rectification. As we do not have access to the survey data, which are stored on the researcher's Qualtrics account, we strongly encourage researchers to inform participants of their right to manage their data in the consent form of their study.

7. Contact Information

For further information or clarification, please contact the MindSampler team at info@mindsampler.com.