Data Handling and Storage Plan for the VR Embodiment Study

1. Types of Data Collected

The study gathers behavioral and self-reported data from participants during the virtual reality (VR) experience. This includes responses to slider-based questions assessing perceived embodiment and fear levels. Optionally, physiological data such as heart rate may also be recorded. No personally identifying information is collected at any point.

2. Pseudonymization and Data Structure

Each participant receives a randomly assigned, non-identifying participant code. All data are linked exclusively to this code. No names, contact details, or key files are created or retained. This process ensures complete pseudonymization from the outset.

3. Storage and Security

All data will be securely stored on encrypted, access-controlled institutional servers provided by Karolinska Institutet. Data will not be stored on personal computers or external cloud platforms. Regular backups and technical safeguards are implemented to prevent unauthorized access or loss.

4. Duration of Storage

Data will be retained for up to 10 years in accordance with Karolinska Institutet's data management policies and the General Data Protection Regulation (GDPR). Participants retain the right to request deletion of their data at any point before anonymization and analysis for publication are completed.

5. Access Rights and Confidentiality

Only members of the designated research team, including the principal investigator and authorized staff, will have access to the raw data. No third parties will be granted access to individual-level information. Data will solely be used for the purpose of this approved study.

6. Data Sharing and Publication

Study results will be reported exclusively in aggregate form. No individual-level data will be published or disclosed in any way that could enable identification or re-identification. If physiological data are collected, they will be presented only as part of group-level summaries.

This data handling plan is designed to ensure strict compliance with ethical research standards, institutional guidelines, and the EU General Data Protection Regulation (GDPR).