Data use agreement for identifiable human data

Adapted version of RU-HD-1.1

I request access to the data in the Research Documentation Collection “CABB dataset” (https://doi.org/10.34973/0d94-kj55) in the digital repository of the Radboud University, established at Nijmegen, the Netherlands (hereinafter referred to as the Radboud University), and I agree to the following:

1. I will comply with all relevant rules and regulations imposed by my institution and my government, including but not limited to the General Data Protection Regulation and other relevant privacy laws. This may mean that I need my research to be approved or declared exempt by a committee that oversees research on human subjects, e.g. my Institutional Review Board or Ethics Committee.

2. I will not attempt to establish the identity of or attempt to contact any of the included human subjects. I will not link this data to any other database in a way that could provide identifying information. I understand that under no circumstances will any personal information about individual subjects be released to me under these Data Use Terms.

3. I will not redistribute or share the data with others, including individuals in my research group, unless they have independently applied and been granted access to this data.

4. I will adhere to the participant-specific permission to disseminate audio/video data for educational and promotional purposes. Thus, I will not show or incorporate the data in presentations, lectures, papers, webpages etc., unless participants have provided explicit consent for this (consent overview can be found in the collection).

5. I will acknowledge the use of the data and data derived from the data when publicly presenting any results or algorithms that benefitted from their use, as follows:
   (a) Papers, book chapters, books, posters, oral presentations, and all other presentations of results derived from the data should acknowledge the origin of the data as follows: "Data were provided (in part) by the Radboud University, Nijmegen, The Netherlands".
   (b) Papers, book chapters, books, posters, oral presentations, and all other presentations using the data should cite the following publication describing the methods developed and used by the Radboud University to acquire and process the data:
   doi: 10.1016/j.neuroimage.2022.119734
   (c) Neither the Radboud University, nor the researchers that provide this data should be included as an author of publications or presentations *if this authorship would be based solely on the use of this data*.

6. Failure to abide by these guidelines will result in termination of my privileges to access to these data.

☐ I confirm that the location where the data will be stored (at my host research institution/university) meets the necessary requirements to protect the personal data as described in the Appendix (page 3).

☐ I confirm that I will use the data for scientific purposes only.

[please provide a short description (1-2 lines) of the reason(s) for downloading the repository and/or description of how the data will be used for research]

Signed and agreed by:

....
Date [year, month, day]

....
Name [legal name, e.g. name as in Passport]

....
Signature

Appendix: security measures

Access to the dataset comes with the responsibility for the user to decide upon and implement sufficient security measures (based on a risk assessment), which should minimally include the following:

- Encryption – data must be stored and transmitted in encrypted form, using protocols that meet the current market standards with regard to strong encryption.
- Information security program – an information security program is in place to ensure an adequate level of data security based on assessed risks.
- Patching and anti-virus – the system must be patched regularly and have an up to date anti-virus software in place.
- Firewall – adequate security measures must be in place to protect the storage network including an up to date firewall
- Physical security measures – physical measures must be in place to ensure that the personal data is secure. These measures can include, but are not limited to, physical access control, measures in case of fire, break-in or water damage.
- Monitoring – the IT environment must be monitored on malicious actions or technical issues that can lead to, or are a result of, a personal data breach.
- Authentication and authorisation – systems must be in place that limit the access to personal data based upon the necessity of the researcher. These systems must meet the current market standards with regards to strong authentication.
- Auditing – systems must be routinely monitored in order to expose potential intrusions and to verify whether all security requirements are met.