**Ethics Committee guidelines online research** 10-5-2022

* **Audio/video streaming (also applies to non-recorded data)**

For research including audio/video streaming you can use Microsoft Teams. Zoom can only be used when end-to-end encryption has been activated. Skype should not be used for research.

* **Collecting personal data
Personal data entails data that can be traced to an individual; f.x. name/ e-mail address / telephone nr/ IP address / or a combination of personal information (date of birth / gender / religion / medical information etc.)**

Are you in contact with your participants at **any time** before, during or after the research?

**No** - I do not know who my participants are.

1. Always supply information about the research and the right to stop at any time.
2. Anonymous consent is sufficient (participants have to actively consent fx. ticking an empty(!) box).
Please note that since you do not have any means to relate your data to an individual, participants cannot withdraw after completion. They can only withdraw during the test (which means that they will not complete the test).
3. The standard storing period for anonymous data is 10 years.

**Yes** - I know who my participants are (e.g. email contact).

1. Always use information letters and ask for consent.
2. State the platform through which you want to collect data.

Qualtrics is the preferred platform. You can log in with your UvAnetID at [https://uva.eu.qualtrics.com](https://eur04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fuva.eu.qualtrics.com%2F&data=05%7C01%7CG.Lindeboom%40uva.nl%7C8b23b11f3710400bc68108da28e341ae%7Ca0f1cacd618c4403b94576fb3d6874e5%7C0%7C0%7C637867253762474987%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=b%2FRn1UOHNd0M1K8v1dX4fXLPwDncDNLwC1xPAaGMXkU%3D&reserved=0)

Commercial survey software with which the UvA has no license agreement is not OK. Use of Pavlovia.org: only if data is removed immediately after completion.

1. Make sure you disable ‘store IP address’ if possible.
2. Ask as little personal information as possible.
3. Keep personal data separate from non-personal data of the participants at all times.
4. Do this by asking the personal data of participants through a separate document and not via the online tool. Communicate this document together with the consent form to and from the participant via SURFfilesender: <https://www.surf.nl/surffilesender-veilig-en-versleuteld-bestanden-versturen> Do not use email!.
5. Anonymise your data set as soon as your data collection has finished. Remove all personal data so that no one can trace the data in your set to an individual, including the researcher! This means contact with the participant is lost.
6. Pseudonymise your data set as soon as you have completed data collection if anonymising your dataset is not possible because your research requires the personal data or if you need to be in contact with the participants later on.
7. Encrypt personal data and store it away from the data set (use f.x. VeraCrypt or Bitlocker).
8. Store the key to the pseudonymised set separate from the dataset (not in the same directory or folder!).
9. The standard storing period for anonymised data is 10 years. Delete personal data as soon as possible.

For more information about personal data check the *Ethics & GDPR instruction* at the Ethics Committee website: <https://aihr.uva.nl/about-aihr/ethics-committee/ethics-committee.html>

For questions on audio/video streaming and secure data storage contact the data steward at datasteward-fgw@uva.nl