

Privacy notice for thesis “Designing in-flight entertainment systems for neurodiverse passengers”

This privacy notice describes how your personal data will be used in the thesis research as a participating individual. For more details how the study is carried out, read the introductory page of the questionnaire.

1. What is the purpose of processing the personal data?

The purpose of processing the personal data is to collect material for a master’s thesis on the topic “Designing in-flight entertainment systems for neurodiverse passengers”. This research study examines which accessibility needs neurodiverse passengers have in in-flight entertainment systems (IFE). The purpose of processing personal data is to analyse accessibility requirements, derive design recommendations, produce prototypes, and publish aggregated, non-identifying research results. The thesis research material will be collected using Webropol questionnaires.

2. What personal data will be processed in the thesis work?

- Responses you provide in the online questionnaire (ratings, multiple choice, short open text, ranking).
- Direct identifier: system generated submission timestamp (the only direct identifier collected). No names, email addresses or logins are collected in the main survey.
- Special category data: self reported health information (neurodiversity: ADHD, ASD, dyslexia, prefer not to say) and related sensory/cognitive needs.

Special categories of personal data (sensitive personal data)

- ☒ In addition, the following special categories of personal data are processed:
- ☒ Data concerning health (self-reported neurodiversity, sensory or cognitive conditions)

Personal data is collected from the following sources:

From the participant: questionnaire through Webropol

3. Processing of personal identifiers in the analysis stage and thesis

The research study only processes personal data necessary for the thesis. During analysis the data are processed so that you are not directly identifiable to the researchers. Direct identifiers (the system timestamp) are pseudonymised by replacing the timestamp with a random identifier and original timestamps are removed from working files.

- The research data is pseudonymised immediately after the survey has been closed by assigning a random number for the time stamp.
- In case the research participant reveals sensitive personal data or identifiable information and processing of such personal data is not necessary for conducting the research and not a point of interest, such data is deleted in the transcription phase.
- Rough classification of survey data is used, for example an age range is used instead of the exact age, to make identification more difficult.

Your identity will be impossible to determine in the published thesis.

4. Legal basis for processing personal data

☒ The legal basis for processing personal data is the express consent of the research participant to data collection and analysis.

Withdrawal of consent will have no effect on an approved thesis, because an approved thesis is an academic publication, where the processing of personal data serves the purpose of academic expression (Articles 6 and 85 of the General Data Protection Regulation (EU) 2016/679 and section 27 of the Data Protection Act of Finland (1050/2018)). No data may be erased from an approved thesis.

5. Sharing personal data

Material containing your personal data may be shared with the thesis supervisor Antti Oulasvirta if necessary for the advising process.

Personal information is not shared with parties outside Aalto University.

Processors:

Webropol (survey platform) is used to collect questionnaire responses. Webropol processes data as a data processor under contract with Aalto University and is approved for use by Aalto University and complies with applicable GDPR requirements. Research data will not be transferred to external partners for other purposes.

The thesis advisor (collaborator) is based in Germany. This collaborator will receive only aggregated, irreversibly anonymised outputs related to the thesis and will not receive personal data or pseudonymised individual records.

The study is supported by an aviation industry partner. For thesis write-up, only aggregated, irreversibly anonymised outputs from both quantitative and qualitative analyses will be transferred to the student researcher's work computer because this data is not considered as personal data anymore. For thematic analysis, this means theme names and definitions, aggregated counts (with suppression of small cells), and non-identifying illustrative examples (paraphrased or composite quotes only). No verbatim free-text responses, individual-level records, or pseudonymised rows will be transferred. Aggregated outputs will be prepared to prevent identification (small cells suppressed; no cells with $n \leq 5$ reported). Because these outputs will be irreversibly anonymised and cannot be linked back to individuals, they are not treated as personal data and may be shared with third parties (for example, thesis examiners, or the industry aviation partner supporting this thesis).

6. International data transfers

[x]: Research data containing personal data will not be transferred outside the European Union/ European Economic Area or to international organizations.

7. Storage and protection of personal data

During this research, the privacy of the research participant is protected as follows:

The thesis research follows a research plan.

The thesis research has a thesis supervisor:
Antti Oulasvirta (antti.oulasvirta@aalto.fi)

Information processed in IT systems: Your personal data is processed and preserved in secure IT systems, which are approved by Aalto University and suitable for personal data. Access to all computers and IT systems are protected by username and strong personal password. Access to IT systems containing personal data is technically restricted in a manner, that only researchers participating in the study and persons necessary for the implementation of the study have access to your personal data.

- Secure transfer: after survey closure, the Webropol export is transferred via encrypted channel to Aalto Virtual Desktop Infrastructure (VDI) and stored on Aalto-managed OneDrive for analysis.
- Working environment: analysis is performed on Aalto-approved systems (VDI / OneDrive / Aalto Jupyter Notebook). Access is limited to the student researcher and Aalto supervisor, protected by Aalto credentials and strong authentication (M365 login, MFA where available).
- Personal devices: dataset files will not be downloaded to personal devices. If accessed outside the VDI, files remain in the cloud and are opened via M365 web/remote session only.

Aggregated anonymised outputs described in Section 5 will be transferred to the student researcher's work computer for thesis write-up only after irreversibility of anonymisation has been confirmed and with supervisor approval. Transfers will use encrypted channels and the data will be stored encrypted on the destination device. Original personal data remain on Aalto-approved systems.

The computers and information systems used are protected with a username and password. Access to research data containing personal data has been restricted so that only the student and the thesis advisor have access to your personal data.

8. Retention and deletion of personal data

Consent forms with name and contact information: none collected.

Research data containing personal data (questionnaire responses and associated pseudonymised identifiers) will be retained on Aalto-approved systems until the thesis has been approved and subsequently deleted within 6 months after thesis approval (expected by

end of Spring 2026). At the end of the retention period all copies on Aalto systems will be securely deleted in accordance with Aalto procedures.

Code key data / link between time stamp and pseudonymised code: no separate code key is retained. The system-generated time stamp (the only direct identifier collected) is pseudonymised immediately after survey closure by replacing it with a random identifier, original timestamps are deleted from working files after pseudonymisation.

Aggregated outputs transferred for thesis write-up will be retained and deleted in accordance with this Section, original personal data remain on Aalto systems as described in Section 8.

Deletion during the study and on request

While the survey is open and before the dataset has been pseudonymised (i.e., before survey closure and the immediate pseudonymisation step), participants may request that their submission be deleted. To request deletion during this period, contact the student researcher at ida.parkkali@aalto.fi. We will delete identifiable submissions as soon as practicable after a valid request and confirm deletion by e-mail if contact details are provided.

After the dataset has been pseudonymised and original timestamps removed, we may not be able to link a pseudonymised response back to the submitting individual. Consequently, it may not be possible to locate and delete an individual participant's record after pseudonymisation. If you wish to attempt deletion after pseudonymisation, contact the student researcher with any additional identifying information that would enable us to locate your response. We will consider and handle such requests in accordance with GDPR and Aalto procedures.

9. Rights of the research participant

According to the General Data Protection Regulation (GDPR), you have the right to:

- be informed of the processing of your personal data
- access the personal data collected concerning yourself
- request the rectification of your personal data
- request that the processing of your personal data be restricted
- object to the processing of your personal data
- request the erasure of your personal data. It should be noted, however, that an approved thesis is an academic publication, where the processing of personal data serves the purpose of academic expression (Articles 6 and 85 of the General Data Protection Regulation (EU) 2016/679 and section 27 of the Data Protection Act of Finland (1050/2018)). No data may be erased from an approved thesis.
- If the research does not require or no longer requires the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of the data subject using his or her rights. If the controller does not recognise the data that may be linked to a specific data subject, the data subject has no right to access or rectify their personal data, to object to their processing or to request the erasure of data. However, if the data subject provides additional information that allows their identification from the research data, the rights will not be restricted.

10. Contact details of the controller

The controller of this research is student: Ida Parkkali (ida.parkkali@aalto.fi)

11. Contact details of the Aalto University data protection officer and those of the supervisory authority

If the research participant has any questions regarding data protection or personal data processing, they can contact the Aalto University data protection officer, tel. (09) 47001 (exchange), dpo@aalto.fi

If the research participant considers the processing of their personal data to be an infringement of privacy protection legislation, they have the right to lodge a complaint with the Data Protection Ombudsman, which is the supervisory authority. (Read more at <https://tietosuoja.fi/en/home>.)