Project Harbour Field Survey Research Prototype

Participant Consent and Privacy Notice

Version: 3 | Effective: 22 September 2026

Data Controller: Université de Fribourg, Av. de l'Europe 20, 1700 Fribourg, Switzerland. (hereinafter: the "Controller", "Unifr" or "we")

Participant: [NAME, LOCATION, EMAIL – pulled from registration page] (hereinafter: "Participant" or "Data Subject")

1 Definitions

Prototype.

The pre-release version of the Project Harbour digital application that assesses and trains conversational competence through a science-driven framework.

Field Survey Research.

The closed Field Survey Research programme described in Error: Reference source not found.

Participant.

An individual who has accepted this Agreement and been granted access to the Prototype as part of the Field Survey Research programme. In this Agreement, the Participant is the Data Subject.

Prototype Survey Period.

The duration of access by the Participant to the Prototype for the purpose of the closed Field Survey Research, commencing on the date the Participant receives an invitation e-mail and running for nine (9) weeks from that date.

Questionnaire.

The structured Participant Observation and Suggestion questionnaire integrated into the Prototype, through which Participants submit pseudonymised observations and suggestions at agreed intervals.

Voice Data.

Audio recordings of a Participant's spoken utterances captured by the Application during conversational practice sessions (limited to ten minutes per session), together with any derived data – such as automatic transcriptions, phonetic features, behavioural indicators, or analysis scores – extracted from those recordings.

Data Controller.

The entity that determines the purposes and means of processing personal data. In the context of this Agreement, the Data Controller is the Université de Fribourg, represented by Dr Samy Rima, Scientific Leader of Project Harbour.

Data Processor.

An entity that processes personal data on behalf of and under the instructions of the Data Controller,

Data Subject.

An identified or identifiable natural person whose personal data is processed. In this Agreement, the Data Subject is the Participant.

Personal Data.

Any information relating to an identified or identifiable natural person.

Profiling.

Any form of automated processing of personal data to evaluate, analyse, or predict aspects of a natural person's personality – including conversational behaviour, social competence, or communication patterns.

Pseudonymisation/ Pseudonymised Data.

Pseudonymisation describes the processing of personal data in such a manner that it can no longer be attributed to a specific individual without the use of additional information, which is kept separately and subject to technical and organisational measures to prevent re-attribution. Data that has undergone Pseudonymisation is described as Pseudonymised Data.

Data processing

What data is collected

In connection with the Field Survey Research, Unifr collects the following personal data.

Account data and consent:

Name, location and email address provided at registration; account authentication credentials; access dates to the application; and a record of consent given under this Agreement.

Voice data:

Audio recordings of conversational practice sessions (approximately ten minutes per session) captured by the Prototype; automatic transcriptions of those recordings; and session metadata (user identifier, scenario identifier, timestamp, and analysis scores).

Speech analysis and scoring data

Data generated by the Prototype's analysis of the recorded speech, including the final pedagogical feedback.

Technical and usage data:

Application usage data (pages visited, features used, session duration, error events); and technical environment data (device type, operating system, browser type).

Participant's answers to the Questionnaire

Feedback submitted by the Participant related to their experience, needs and preferences.

Lawful basis for processing

We process your personal data based on the present consent and on the statutory basis that requires the Unifr to contribute to the advancement of scientific knowledge through research (University Act of the Canton of Fribourg) and your consent.

For the purposes of the GDPR, the data processing relies on the consent (GDPR Art. 6 (1)(a)) and the public interest in conducting scientific research activities (GDPR Art. 6 (1)(e)).

Nature and purposes of data processing

The purpose of processing personal data is :

- to test an early version of the application - the Prototype - to inform further developments in terms of features, feedback quality, and user experience;
- to grant the Participants free access to the Prototype and offer the Participants pedagogical feedback on expression;
- the conclusion of the Legal Terms and Confidentiality Agreement and for sending emails reminders
- to send update communications about Project Harbour by email.

Voice Data is processed as follows:

(1) cloud-based generative AI services, accessed via API, performs audio and text analysis and supports real-time voice interaction;
(2) open-source models running server-side, perform voice activity detection and speech processing.
(3) the analysis generates pedagogical feedback on expression quality covering rhythm, clarity, conversational dynamics, and stylistic dimensions, in the sense of Profiling;

The Participant will be prompted to grant microphone access within the Prototype before any recording begins. Refusing microphone access is considered a withdrawal of consent to Voice Data processing. It may result in loss of access to the Prototype and require termination of participation (see clause Legal Terms and Confidentiality Agreement).

Data Security

We undertake to implement appropriate technical and organisational measures to guarantee the security of your personal data. These measures aim to ensure their confidentiality, integrity,

availability and traceability, taking into account the risks involved, in particular to protect them against unauthorised access, loss, destruction, or damage.

They include, without limitation:

- access controls on a need-to-know basis; multi-factor authentication for systems holding personal data; logging and periodic review of all access;
- encryption of personal data in transit using TLS 1.2 or higher;
- encryption of personal data at rest using AES-256-GCM
- Pseudonymisation of all research and feedback data before it enters the research environment, with the Pseudonymisation key – the sole key capable of linking any research or feedback record to an identified Participant's account.
- Pseudonymisation key is held exclusively by the Controller in a separate system with very restrictive access;
- Account data held for Prototype access management is stored in a separate database from the pseudonymised data held for feedback collection and research. These two environments will never be combined, nor linked.
- The Pseudonymised Data are used together for product improvement purposes and are accessible only to the following authorised roles: The Data Controller, the Project Assistant at the University of Fribourg, the Project IT Consultant, and the Project Application Design Consultant. A re-identification process will only occur where strictly necessary for a legitimate purpose, including responding to a Data Subject rights request under clause 3.5.
- documented incident response procedures reviewed annually;

Data protection commitment

We will:

(1) hold personal data in strict confidence and process it only for the purposes described in clause 2.4;
(2) not sell personal data or share it with third parties for their own commercial purposes;
(3) retain personal data only for as long as necessary:
    - Technical and usage data, Participants answers to Questionnaire, Voice Data, Speech analysis and pedagogical feedback will be retained for three (3) years from the end of the Participant's Prototype Period, after which it will be securely deleted or irreversibly anonymised; anonymised derived data may thereafter be retained without limit of time for research or commercial purposes; consent records will be retained for as long as required by applicable law; and
(4) Exercise due diligence in the selection of the external processors which may process personal data and conclude data processing agreements with them. We undertake, to the extent reasonable, to ensure that our processors comply with the applicable rules on cross-border data communication.

Service providers (processors)

In certain domains listed below, we work with external service providers who are given access to personal data and process it at our request on behalf of and in accordance with our instructions:

- IT and Design consultant for the Project Platform: Eric Maussion and Zhana Klein
- Data and Application Cloud Hosting: Google LLC
- Product analytics and user experience: PostHog
- Audio processing with AI tools (e.g. audio and text analysis, voice activity detection and speech processing, Real-time voice) : Open AI, Google LLC

Cross-border disclosure of personal data

Wherever possible, we process personal data in Switzerland. For certain IT services delegated to processors (cloud, product analytics and user experience, audio processing with AI tools), personal data may be disclosed outside Switzerland if the State of destination ensures an adequate level of protection, recognised by an adequacy decision or by the Swiss-U.S. Data Privacy Framework for certified organisations or if an appropriate level of data protection is guaranteed by standard data protection clauses that the European Commission or the Federal Data Protection and Information Commissioner have approved.

Data subject rights

The Participant has the following rights, exercisable within the limits of the legal requirements, by contacting hello@project-harbour.ch:

(1) **Right of access :** to request confirmation of whether personal data is held and receive a copy, including of Voice Data and any derived data.
(2) **Right to rectification:** to request correction of inaccurate or incomplete personal data.
(3) **Right to erasure:** to request deletion of personal data, including Voice Data, subject to any applicable legal retention obligations.
(4) **Right to restriction of processing:** to request limitation of processing in certain circumstances.
(5) **Right to data portability:** to receive personal data that the Participant has provided, in a structured, machine-readable format.
(6) **Right to object to Profiling:** to object to the processing of personal data for Profiling purposes.
(7) **Right to withdraw consent.**

We will respond to rights requests without undue delay and within 30 days of receipt, extendable by a further 30 days where complexity requires, with prior notice to the Participant.

The Participant also has the right to lodge a complaint with a supervisory authority, in Switzerland with the Fribourg Cantonal Data Protection Commissioner (Préposé cantonal à la protection des données et à la transparence).

Sensitive personal data

We do not anticipate collecting sensitive personal data. Voice Data is collected for conversational analysis only and is not processed for biometric identification purposes. If the Prototype design changes to involve sensitive personal data categories, we will obtain separate express consent from each Participant before such collection commences. Participants are instructed not to share any sensitive data during the sessions. Inappropriate/ sensitive personal data sharing leads to the conversational agent to redirect the conversation, yet does not delete it from the recording.

Contact details of Data Protection Officer

University of Fribourg, Data Protection Officer, Av. de l'Europe 20, 1700 Fribourg, Switzerland, dpo@unifr.ch

Language

This Consent and Privacy Notice is drafted in English. In the event of any inconsistency between the English version and any translation, the English version prevails unless otherwise required by applicable law.

Acceptance

By checking the box(es) in the Agreement acceptance page and clicking "Agree and Proceed", the Participant confirms that they have read and understood this Consent and Privacy Notice in its entirety.

Where to find this Consent and Privacy Notice

A current copy of this Consent and Privacy Notice is available in the Profile menu of the Prototype.