PhonInter Lab | VIZJA University

Data Privacy and Storage Policy

Laboratory of Phonetics and Oral Interpretation
Approved by Dr Habil. Yan Kapranov, VIZJA University Professor
Head of the Laboratory
School of Humanities and Fine Arts | VIZJA University
Document PIL 09 EN | Version 3.0 | Revision 31 October 2026
Room 205, ul. Okopowa 59, 01-043 Warsaw, Poland

This edition applies from publication. University-wide rules and competent university decisions take precedence.

Purpose and legal context

This Policy establishes rules for collecting, processing, storing, accessing, sharing, retaining, and deleting data and recordings generated in the Laboratory. It supports compliance with institutional regulations, GDPR, Polish data protection requirements, research ethics, and responsible academic practice.

This Policy does not replace university-wide data protection rules. If a conflict arises, applicable university regulations and legal requirements prevail.

Institutional responsibilities

The Head coordinates operational compliance within the laboratory. This document does not make the Head an independent data controller or replace the university privacy notice, Data Protection Officer or authorised IT incident process. Use the university's official contact channels to obtain the current privacy notice and data protection contact.

Scope

This Policy applies to all users and to all data generated, collected, processed, stored, transferred, analyzed, or deleted in connection with laboratory activities.

Data categories

- Audio and video recordings: recordings created during training sessions, pronunciation practice, interpretation exercises, interviews, research, or demonstrations.
- Transcripts and annotations: text files, phonetic annotations, translation/interpreting outputs, feedback notes, and analysis files.
- Research data: experimental data, participant responses, metadata, coding sheets, and project datasets.
- Administrative data: names, IDs, affiliations, course details, booking records, training records, attendance logs, and access records.
- Technical data: software outputs, system logs, equipment usage logs, maintenance notes, and incident records.

Authorized purposes

- teaching, training, assessment, and feedback;
- academic research and student projects approved by the relevant supervisor or institutional authority;
- technical maintenance, troubleshooting, and quality improvement;
- institutional reporting, audit, safety, and compliance purposes;
- documentation of incidents, maintenance, access, and user readiness.

Consent and participant information

Before collecting identifiable recordings or other personal data, the responsible university unit must establish the lawful basis, purpose, access, retention period and participant information. Obtain informed consent where it is the applicable basis or is otherwise required. A laboratory approval or a student's participation alone does not establish a lawful basis.

Use the approved participant information and consent documents. Explain recording, intended uses and any proposed sharing before collection. Do not promise unrestricted erasure or withdrawal where an applicable exception may apply; refer such requests to the university data protection process.

Research with participants requires any applicable ethics and institutional approvals before data collection. Collect no unnecessary diagnoses, identification document copies or participant details.

Storage and access

- Laboratory data must be stored only on university-approved servers, systems, or repositories unless written authorization specifies otherwise.
- Access must be limited to authorized users with a legitimate academic, research, administrative, technical, or legal need.
- Personal USB drives, private cloud storage, personal email accounts, and non-approved platforms must not be used for laboratory data unless explicitly authorized.
- Files should be clearly labeled using project, course, date, and responsible-person identifiers without exposing unnecessary personal data.
- Access to sensitive or identifiable data should be documented where required.

Retention and deletion

Do not retain identifiable data longer than necessary for its documented purpose. The responsible university unit sets and records the applicable retention period or review criteria before collection, considering university schedules, assessment, ethics, project and funder requirements. This edition does not impose a universal course plus one academic year rule.

At the end of the authorised period, arrange secure deletion or irreversible anonymisation, unless a documented requirement justifies further retention. Apply the approved process to working copies and backups. Preserve evidence subject to an incident or legal hold.

External sharing and transfer

- External sharing requires a legitimate purpose, authorization, and appropriate safeguards.
- Where possible, data should be anonymized or pseudonymized before sharing.
- Identifiable data may be shared only where participants have been informed and where a lawful basis and institutional approval exist.
- Transfers to external collaborators must follow approved project, legal, and data protection arrangements.

Ai supported tools and external platforms

AI supported tools may support transcription, speech processing, feedback, annotation, translation/interpreting training, or research analysis only under conditions that protect personal data, confidentiality, academic integrity, and methodological transparency.

- Personal data, identifiable recordings, confidential materials, unpublished research data, assessment materials, or institutional records must not be uploaded to public AI tools without explicit authorization.
- AI-generated outputs must be checked by a competent user before use in teaching, assessment, research, or publication.
- Use of AI tools in research, assessment, or publication must be disclosed where required by institutional, course, funder, or journal rules.
- Where AI tools are used, users should minimize data input, avoid unnecessary identifiers, and follow approved data protection safeguards.

Security measures

- password-protected access to systems and files;
- restricted access based on user role and legitimate need;
- regular software updates and technical maintenance;
- secure storage of physical documents and consent forms;
- use of anonymization or pseudonymization where appropriate;
- prompt reporting of suspected unauthorized access, loss, disclosure, or breach.

Incident management and data breach response

- Suspected data loss, unauthorized disclosure, unauthorized access, or improper upload must be reported immediately to the Head of the Laboratory and relevant university unit.
- Affected systems or files should be secured without destroying evidence.
- The Incident Report Form should be completed where appropriate.
- Notification of affected parties or authorities must follow GDPR and institutional procedures.

User rights

Data subjects may have rights to access, correction, deletion, restriction, objection, or other rights under applicable data protection law and institutional procedures. Requests should be handled through the appropriate university process.

Responsibilities

- Users: handle data responsibly, follow consent and storage procedures, and report risks immediately.
- Instructors and supervisors: ensure students and project participants follow approved procedures.
- Technical staff: support secure systems, maintenance, and access controls.
- Head of the Laboratory: oversees implementation of this Policy within laboratory operations and escalates issues to relevant university units.

Review and updates

This Policy is reviewed annually or earlier if legal requirements, institutional regulations, technology, software platforms, research procedures, or data protection risks change.

Reference

Regulation EU 2016 679 GDPR: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

University contact: https://vizja.pl/kontakt/