PhonInter Lab | Uniwersytet VIZJA

Polityka ochrony i przechowywania danych

Laboratorium Fonetyki i Przekładu Ustnego

Zatwierdził dr hab. Yan Kapranov, prof. Uniwersytetu VIZJA
Kierownik Laboratorium
Wydział Nauk Humanistycznych i Sztuki | Uniwersytet VIZJA

Dokument PIL 09 PL | Wersja 3.0 | Aktualizacja 31 października 2026

Sala 205, ul. Okopowa 59, 01-043 Warszawa, Polska

Edycja obowiązuje od publikacji. Pierwszeństwo mają regulacje ogólnouczelniane i decyzje właściwych organów Uczelni.

Cel i kontekst prawny

Polityka określa zasady gromadzenia, przetwarzania, przechowywania, dostępu, udostępniania, retencji i usuwania danych oraz nagrań powstających w Laboratorium. Wspiera zgodność z regulacjami Uczelni, RODO/GDPR, polskimi przepisami o ochronie danych, zasadami etyki badań oraz odpowiedzialną praktyką akademicką.

Polityka nie zastępuje ogólnouczelnianych regulacji ochrony danych. W przypadku rozbieżności pierwszeństwo mają obowiązujące przepisy prawa i regulacje Uczelni.

Odpowiedzialność instytucjonalna

Kierownik koordynuje stosowanie zasad w bieżącej pracy laboratorium. Dokument nie ustanawia Kierownika odrębnym administratorem danych i nie zastępuje informacji Uczelni, Inspektora Ochrony Danych ani zatwierdzonej procedury incydentów IT. Aktualną informację i kontakt dotyczący ochrony danych należy uzyskać oficjalnymi kanałami Uczelni.

Zakres

Polityka dotyczy wszystkich użytkowników oraz wszystkich danych generowanych, gromadzonych, przetwarzanych, przechowywanych, przekazywanych, analizowanych lub usuwanych w związku z działaniami Laboratorium.

Kategorie danych

- Nagrania audio i wideo: materiały tworzone podczas szkoleń, ćwiczeń wymowy, ćwiczeń tłumaczeniowych, wywiadów, badań lub prezentacji.
- Transkrypcje i adnotacje: pliki tekstowe, zapisy fonetyczne, wyniki tłumaczeń, notatki z informacji zwrotnej i pliki analityczne.
- Dane badawcze: dane eksperymentalne, odpowiedzi uczestników, metadane, arkusze kodowania i zbiory danych projektowych.
- Dane administracyjne: imiona i nazwiska, numery albumu lub identyfikatory, afiliacje, informacje o kursach, rezerwacje, ewidencja szkoleń, obecności i dostępu.
- Dane techniczne: wyniki działania oprogramowania, logi systemowe, rejestry użycia sprzętu, notatki konserwacyjne i raporty incydentów.

Dozwolone cele przetwarzania

- dydaktyka, szkolenia, ocena i informacja zwrotna;
- badania naukowe i projekty studenckie zatwierdzone przez właściwego opiekuna lub jednostkę;
- utrzymanie techniczne, rozwiązywanie problemów i poprawa jakości;
- sprawozdawczość instytucjonalna, audyt, bezpieczeństwo i zgodność;
- dokumentowanie incydentów, konserwacji, dostępu i gotowości użytkowników.

Zgoda i informacja dla uczestników

Przed gromadzeniem identyfikowalnych nagrań lub innych danych osobowych właściwa jednostka Uczelni ustala podstawę prawną, cel, dostęp, okres przechowywania i informację dla uczestników. Świadomą zgodę należy uzyskać, gdy stanowi właściwą podstawę lub jest wymagana z innych przyczyn. Sama zgoda laboratorium ani uczestnictwo studenta nie stanowią podstawy prawnej.

Należy stosować zatwierdzone informacje dla uczestników i formularze zgody. Przed zbieraniem danych wyjaśnić zakres nagrywania, planowane wykorzystanie i ewentualne udostępnianie. Nie należy obiecywać bezwarunkowego usunięcia danych lub wycofania udziału, jeśli mogą obowiązywać wyjątki; takie wnioski kieruje się do właściwej procedury ochrony danych Uczelni.

Badania z udziałem osób wymagają odpowiednich zgód etycznych i instytucjonalnych przed zebraniem danych. Nie gromadzić zbędnych diagnoz, kopii dokumentów tożsamości ani danych uczestników.

Przechowywanie i dostęp

- Dane laboratoryjne należy przechowywać wyłącznie na zatwierdzonych serwerach, systemach lub repozytoriach Uczelni, chyba że pisemna zgoda stanowi inaczej.
- Dostęp powinien być ograniczony do osób uprawnionych i posiadających uzasadnioną potrzebę dydaktyczną, badawczą, administracyjną, techniczną lub prawną.
- Prywatne nośniki USB, prywatne chmury, prywatna poczta elektroniczna i niezatwierdzone platformy nie mogą być wykorzystywane do danych laboratoryjnych bez wyraźnej zgody.
- Pliki powinny być opisane w sposób umożliwiający identyfikację projektu, kursu, daty i osoby odpowiedzialnej bez ujawniania niepotrzebnych danych osobowych.
- Dostęp do danych wrażliwych lub identyfikowalnych powinien być dokumentowany tam, gdzie jest to wymagane.

Retencja i usuwanie

Danych identyfikowalnych nie należy przechowywać dłużej, niż jest to niezbędne dla udokumentowanego celu. Właściwa jednostka Uczelni określa i dokumentuje termin retencji lub kryteria przeglądu przed zebraniem danych, uwzględniając regulacje Uczelni, ocenianie, etykę, projekt i wymagania grantodawcy. Edycja nie ustanawia ogólnej zasady przechowywania przez czas kursu i dodatkowy rok akademicki.

Po zakończeniu dozwolonego okresu należy zapewnić bezpieczne usunięcie lub nieodwracalną anonimizację, chyba że udokumentowany wymóg uzasadnia dalszą retencję. Zatwierdzona procedura obejmuje kopie robocze i zapasowe. Należy zachować dowody objęte postępowaniem incydentowym lub obowiązkiem zabezpieczenia.

Udostępnianie zewnętrzne i transfer

- Udostępnianie zewnętrzne wymaga uzasadnionego celu, upoważnienia i odpowiednich zabezpieczeń.
- Dane powinny być anonimizowane lub pseudonimizowane zawsze, gdy jest to możliwe.
- Dane identyfikowalne mogą być udostępniane wyłącznie wtedy, gdy uczestnicy zostali poinformowani oraz istnieje podstawa prawna i zatwierdzenie instytucjonalne.
- Przekazywanie danych współpracownikom zewnętrznym musi być zgodne z zatwierdzonym projektem, przepisami i zasadami ochrony danych.

Narzędzia AI i platformy zewnętrzne

Narzędzia wspierane przez sztuczną inteligencję mogą wspomagać transkrypcję, przetwarzanie mowy, informację zwrotną, adnotację, ćwiczenia tłumaczeniowe lub analizę badawczą wyłącznie w warunkach chroniących dane osobowe, poufność, integralność akademicką i przejrzystość metodologiczną.

- Danych osobowych, identyfikowalnych nagrań, materiałów poufnych, nieopublikowanych danych badawczych, materiałów oceniania i dokumentacji instytucjonalnej nie wolno przesyłać do publicznych narzędzi AI bez wyraźnego upoważnienia.
- Wyniki wygenerowane przez AI muszą zostać zweryfikowane przez kompetentnego użytkownika przed użyciem w dydaktyce, ocenie, badaniu lub publikacji.
- Użycie AI w badaniach, ocenianiu lub publikacji powinno być ujawniane zgodnie z wymaganiami Uczelni, kursu, grantodawcy lub czasopisma.
- Użytkownicy powinni minimalizować zakres wprowadzanych danych, usuwać zbędne identyfikatory i stosować zatwierdzone zabezpieczenia.

Środki bezpieczeństwa

- dostęp do systemów i plików chroniony hasłem;
- dostęp ograniczony według roli i uzasadnionej potrzeby;
- regularne aktualizacje oprogramowania i konserwacja techniczna;
- bezpieczne przechowywanie dokumentów papierowych i formularzy zgody;
- anonimizacja lub pseudonimizacja tam, gdzie jest to zasadne;

- niezwłoczne zgłaszanie podejrzeń nieuprawnionego dostępu, utraty, ujawnienia lub naruszenia danych.

Reakcja na incydenty i naruszenia danych

- Podejrzenie utraty danych, nieuprawnionego ujawnienia, nieuprawnionego dostępu lub niewłaściwego przesłania materiałów należy natychmiast zgłosić Kierownikowi Laboratorium i właściwej jednostce Uczelni.
- Systemy lub pliki należy zabezpieczyć bez niszczenia możliwych dowodów.
- W razie potrzeby należy wypełnić Formularz zgłoszenia incydentu.
- Powiadamianie osób, których dane dotyczą, lub organów musi odbywać się zgodnie z RODO/GDPR i procedurami Uczelni.

Prawa osób których dane dotyczą

Osoby, których dane dotyczą, mogą posiadać prawo dostępu, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu lub inne prawa wynikające z obowiązującego prawa ochrony danych i procedur Uczelni. Wnioski powinny być obsługiwane właściwą ścieżką instytucjonalną.

Odpowiedzialność

- Użytkownicy: przetwarzają dane odpowiedzialnie, stosują procedury zgody i przechowywania oraz natychmiast zgłaszają ryzyka.
- Prowadzący i promotorzy: zapewniają, że studenci i uczestnicy projektów stosują zatwierdzone procedury.
- Personel techniczny: wspiera bezpieczne systemy, konserwację i kontrolę dostępu.
- Kierownik Laboratorium: nadzoruje wdrażanie niniejszej Polityki w operacjach laboratoryjnych i eskaluje problemy do właściwych jednostek Uczelni.

Przegląd i aktualizacje

Polityka jest przeglądana co najmniej raz w roku albo wcześniej, jeżeli zmienią się wymogi prawne, regulacje Uczelni, technologie, platformy oprogramowania, procedury badawcze lub ryzyka ochrony danych.

Podstawa odniesienia

Rozporządzenie UE 2016 679 RODO: https://eur-lex.europa.eu/eli/reg/2016/679/oj/pol

Kontakt z Uczelnią: https://vizja.pl/kontakt/