

Uczestnicy programu „Twoje dane - Twoja sprawa” świętują XX
Dzień Ochrony Danych Osobowych - edukacja, świadomość i
odpowiedzialność za dane osobowe w cyfrowym świecie

Uczestnicy programu
„Twoje dane - Twoja
sprawa” świętują XX
Dzień Ochrony Danych
Osobowych - edukacja,
świadomość i
odpowiedzialność za
dane osobowe w

Uczestnicy programu „Twoje dane – Twoja sprawa” świętują XX
Dzień Ochrony Danych Osobowych – edukacja, świadomość i
odpowiedzialność za dane osobowe w cyfrowym świecie

cyfrowym świecie

Posted on 2026-01-30

Na przełomie stycznia i lutego 2026 r. już po raz dwudziesty obchodziliśmy Dzień Ochrony Danych Osobowych. To święto, ustanowione przez Komitet Ministrów Rady Europy w rocznicę przyjęcia Konwencji nr 108, które przypomina o fundamentalnym znaczeniu prawa do prywatności i ochrony danych osobowych w życiu każdego człowieka. Obchody z tej okazji, organizowane przez szkoły oraz placówki doskonalenia nauczycieli, służą wzmocnieniu świadomości młodych ludzi w zakresie ochrony danych osobowych oraz kształtowaniu odpowiedzialnych postaw w świecie nowych technologii.

Uczestnicy programu podejmują liczne działania informacyjne i społeczne, które nie tylko zwiększają wiedzę uczniów o przysługujących im prawach, w szczególności do ochrony danych osobowych, lecz także promują dobre praktyki w zakresie ochrony prywatności. Program edukacyjny „Twoje dane – Twoja sprawa” od lat wspiera szkoły i placówki doskonalenia nauczycieli w budowaniu kultury poszanowania danych osobowych, a jednocześnie rozwija kompetencje cyfrowe uczniów i nauczycieli, odpowiadając na wyzwania współczesnej rzeczywistości.

W ramach tegorocznych obchodów przygotowano i udostępniono szkołom materiały edukacyjne, w tym krótką poradę z cyklu „Warto wiedzieć” oraz webinarium poświęcone technologii deepfake i konsekwencjom, do jakich może doprowadzić jej niewłaściwe użytkowanie. Przygotowane dla uczestników programu materiały są wykorzystywane podczas lekcji, zajęć wychowawczych, wydarzeń tematycznych oraz w szkolnych gazetkach, stając się impulsem do rozmów o bezpieczeństwie w sieci, odpowiedzialnym korzystaniu z technologii i świadomym podejmowaniu decyzji w środowisku cyfrowym. W niniejszym biuletynie publikujemy również treść porady przekazanej uczestnikom programu, aby mogła

Uczestnicy programu „Twoje dane – Twoja sprawa” świętują XX
Dzień Ochrony Danych Osobowych – edukacja, świadomość i
odpowiedzialność za dane osobowe w cyfrowym świecie

służyć jako wsparcie do kolejnych działań edukacyjnych dla wszystkich osób zainteresowanych ochroną danych osobowych dzieci i młodzieży.

Deepfake – nowe wyzwania dla ochrony danych osobowych i bezpieczeństwa dzieci

Szczególne miejsce w tegorocznych obchodach zajęło webinarium skierowane do przedstawicieli szkół, placówek doskonalenia nauczycieli oraz rodziców i opiekunów, zatytułowane: „Deepfake- nowe wyzwania w cyfrowym świecie. Jak zapobiegać i reagować w trosce o bezpieczeństwo dzieci”. Podczas spotkania omówiono wyzwania, jakie dla ochrony danych osobowych stwarza technologia deepfake, tj. treści audio i wideo generowanych z wykorzystaniem sztucznej inteligencji, które mogą wprowadzać odbiorców w błąd, naruszać prywatność oraz prowadzić do poważnych konsekwencji dla osób, których dane osobowe, w szczególności wizerunek, zostały wykorzystane.

Uczestnicy poznali metody rozpoznawania fałszywych materiałów, zagrożenia związane z dezinformacją oraz sposoby reagowania w sytuacjach kryzysowych w środowisku szkolnym.

W pierwszej części webinarium Michał Sajdak (Sekurak.pl) przedstawił techniczne aspekty funkcjonowania deepfake'ów, ich wykrywania oraz przykłady wykorzystania tej technologii w cyberatakach. Materiał ukierunkowany był na zwiększenie świadomości uczestników programu odnośnie do możliwości skutecznego rozpoznawania i osłabiania wpływu tego rodzaju ataków. Druga część, prowadzona przez Natalię Misiuk – zastępcę Dyrektora Departamentu Inicjatyw Edukacyjnych UODO – dotyczyła relacji pomiędzy deepfake'ami a ochroną danych osobowych, roli Prezesa UODO, znaczenia rozmów z dziećmi i młodzieżą oraz praktycznych wskazówek dotyczących reagowania na niebezpieczne treści.

„Warto wiedzieć” – praktyczne wskazówki dla uczniów

Integralną częścią działań edukacyjnych była porada z cyklu „Warto wiedzieć”, która w przystępny sposób wyjaśnia, czym jest deepfake, jakie zagrożenia może powodować oraz jak bezpiecznie korzystać z narzędzi opartych na sztucznej inteligencji. Podejmowane działania

Uczestnicy programu „Twoje dane – Twoja sprawa” świętują XX
Dzień Ochrony Danych Osobowych – edukacja, świadomość i
odpowiedzialność za dane osobowe w cyfrowym świecie

podkreślają znaczenie krytycznego podejścia do treści publikowanych w internecie, konieczność weryfikowania źródeł informacji oraz potrzebę reagowania na sytuacje budzące niepokój.

Wspólna odpowiedzialność za przyszłość

Z okazji jubileuszowych obchodów XX Dnia Ochrony Danych Osobowych do uczestników programu „Twoje dane – Twoja sprawa”, skierowany został list od Mirosława Wróblewskiego, prezesa UODO, który wyraził w nim uznanie dla dyrektorów, nauczycieli i uczniów za ich konsekwentne zaangażowanie w budowanie kultury ochrony danych osobowych. Podkreślił, że edukacja – rzetelna, atrakcyjna i oparta na wartościach – stanowi jedno z najskuteczniejszych narzędzi przygotowujących młode pokolenie do świadomego i bezpiecznego funkcjonowania w cyfrowym świecie.

Tegoroczne obchody po raz kolejny dowiodły, że ochrona danych osobowych to nie tylko przepisy prawa, lecz przede wszystkim codzienne wybory, postawy i odpowiedzialność każdego z nas. Dzięki wspólnym inicjatywom edukacyjnym oraz zaangażowaniu środowiska oświatowego możliwe jest skuteczne budowanie świadomości, która przynosi realne korzyści już dziś i przekłada się na długofalowe pozytywne zmiany społeczne.

Uczestnicy programu „Twoje dane – Twoja sprawa” świętują XX Dzień Ochrony Danych Osobowych – edukacja, świadomość i odpowiedzialność za dane osobowe w cyfrowym świecie

7 EDUKACJA



Warto wiedzieć...

Deepfake

Nowe wyzwania dla ochrony danych osobowych i bezpieczeństwa

Deepfake to technologia wykorzystująca sztuczną inteligencję, która pozwala na tworzenie fałszywych, ale bardzo realistycznych obrazów, filmów lub dźwięków. Może sprawiać wrażenie, że ktoś powiedział lub zrobił coś, co w rzeczywistości nigdy się nie wydarzyło. Technologia ta jest niestety również wykorzystywana w działalności przestępczej, kradzieży tożsamości, wyłudzeniach pieniędzy lub danych osobowych.

Przykłady zagrożeń:

- może kogoś ośmieszyć lub skrzywdzić np. przez przerabianie zdjęć konkretnej osoby,
- może być używana do oszukiwania ludzi np. do tworzenia fałszywych wiadomości lub podszywania się pod kogoś w celu wyłudzenia danych osobowych lub pieniędzy,
- może stać się narzędziem hejtu, szantażu lub zastraszania,
- może sprawić, że trudno odróżnić to, co prawdziwe, od tego, co zostało zmanipulowane.

Jak rozpoznać deepfake? Zwróć uwagę na szczegóły m.in.:

- twarz, która wygląda nienaturalnie, jest zniekształcona lub „nie pasuje” do reszty ciała,
- ruchy ust, które nie pokrywają się z tym, co słyszysz,
- ruchy ciała, które mogą być bardzo nienaturalne lub nierealistyczne,
- źródło pochodzenia nagrania – sprawdź, czy materiał pochodzi z wiarygodnego i zaufanego źródła,
- treść, która brzmi nierealnie, absurdalnie albo sprzecznie z tym, co wiesz o świecie.

Jak bezpiecznie korzystać z takich narzędzi?

- nie używaj zdjęć prawdziwych osób,
- nie twórz materiałów, które kogoś ośmieszają lub mogą przestraszyć,
- jeśli tworzysz deepfake na potrzeby zabawy – wyraźnie zaznacz, że materiał jest fałszywy.

Technologia jest narzędziem — decyduj świadomie, w jakim celu jej używasz.



PAMIĘTAJ!

Technologia deepfake może być wykorzystana w zarówno dobrych, jak i złych celach. Z jednej strony może pomóc np. w poprawie jakości produkcji filmowych i dźwiękowych. Z drugiej jednak – może służyć do tworzenia fałszywych treści, które szerzą dezinformację. Należy pamiętać, że nie wszystko, co znajduje się w internecie, jest prawdziwe, a wiele deepfake'ów do złudzenia przypomina prawdziwe materiały. Jeśli coś wzbudza Twoje wątpliwości lub niepokój – porozmawiaj o tym z osobą dorosłą.



Uczestnicy programu „Twoje dane – Twoja sprawa” świętują XX Dzień Ochrony Danych Osobowych – edukacja, świadomość i odpowiedzialność za dane osobowe w cyfrowym świecie

7 EDUKACJA



Warto wiedzieć...

Trudne słowa – proste wyjaśnienia

Co oznaczają słowa, które pojawiają się w poradzie?

• **Deepfake** – to technologia wykorzystująca sztuczną inteligencję do tworzenia fałszywych, ale bardzo realistycznych obrazów, filmów lub dźwięków w celu pokazania czegoś, co nigdy się nie wydarzyło. Wykorzystuje do tego techniki uczenia (deep learning) i fałszowania (fake).

• **Deepfake audio** – koncentruje się na manipulacji dźwiękiem i ludzkim głosem.

Za pomocą tej technologii można tworzyć fałszywe nagrania głosowe, w których osoba wydaje się mówić lub śpiewać coś, czego w rzeczywistości nie powiedziała lub nie zaśpiewała. Deepfake audio jest często wykorzystywany w tworzeniu fałszywych nagrań rozmów telefonicznych lub przemówień.

• **Deepfake video** – polega na manipulacji materiałami filmowymi, w szczególności twarzami i ciałami. Dzięki tej technologii można stworzyć nieprawdziwe materiały video. Deepfake video jest używane do różnych celów np. do manipulacji informacjami i tworzenia fałszywych treści.

• **Dezinformacja** – to celowe rozpowszechnianie fałszywych lub wprowadzających w błąd treści, informacji, tzw. fake newsów. Technologia deepfake bardzo często jest wykorzystywana do tworzenia takich treści.

• **Sztuczna inteligencja** – zwana również AI (ang. Artificial Intelligence), to dziedzina informatyki zajmująca się tworzeniem maszyn i systemów, które potrafią wykonywać zadania wymagające ludzkiej inteligencji. Obejmuje to takie umiejętności jak rozumowanie, uczenie się, rozwiązywanie problemów, postrzeganie i podejmowanie decyzji.

• **Dane osobowe** – to informacje, które mogą pomóc kogoś zidentyfikować, np. imię i nazwisko, adres, numer telefonu, e-mail, głos czy wizerunek. Takich danych nie powinno się udostępniać nieznanym osobom i aplikacjom bez potrzeby.

