Deklaracja

Wzmocnienie współpracy regionalnej w zakresie ochrony danych, sztucznej inteligencji i danych dotyczących zdrowia

DOROCZNE SPOTKANIE ORGANÓW OCHRONY DANYCH OSOBOWYCH Z EUROPY ŚRODKOWEJ I WSCHODNIEJ

Zadar, Chorwacja | 24–26 września 2026 r.

Preambuła

Sztuczna inteligencja oraz rosnące wykorzystanie i wymiana danych dotyczących zdrowia zmieniają sposób funkcjonowania usług publicznych, opieki zdrowotnej, badań naukowych i codziennego życia. Korzyści wynikające z tych zmian zależą od poszanowania godności człowieka, prywatności i ochrony danych osobowych, zasady niedyskryminacji oraz zapewnienia skutecznych środków ochrony prawnej. Ochrona osób fizycznych i umożliwianie odpowiedzialnych innowacji to cele wzajemnie się wzmacniające, które wymagają uwzględnienia odpowiednich zabezpieczeń na etapie projektowania, wdrażania i nadzoru nad systemami cyfrowymi.

Inicjatywa Organów Ochrony Danych Osobowych z Europy Środkowej i Wschodniej (CEEDPA) zrzesza organy działające zarówno w Unii Europejskiej, jak i poza nią, funkcjonujące w ramach różnych systemów prawnych i rozwiązań instytucjonalnych. Jej trwałą wartością są bezpośredni dialog, wzajemna pomoc oraz wymiana praktycznych doświadczeń. Relacje te wspierają dążenie do zbieżności w kierunku wysokich standardów ochrony, przy jednoczesnym poszanowaniu niezależności i zakresu odpowiedzialności każdego organu.

Doroczne spotkanie w Zadarze, nawiązując do tej tradycji, stwarza okazję do odnowienia naszego wspólnego zobowiązania i powiązania go z praktycznymi działaniami w obszarze sztucznej inteligencji, zarządzania danymi dotyczącymi zdrowia oraz skutecznego nadzoru. Konwencja nr 108 Rady Europy i jej modernizacja stanowią wspólny punkt odniesienia dla współpracy w całym regionie, obok mających zastosowanie przepisów prawa krajowego i prawa Unii Europejskiej.

Uznając, że:

Ryzyka wynikające z technologii cyfrowych i transgranicznego przetwarzania danych nie mogą być skutecznie rozwiązywane przez organy działające w izolacji, a różnice między systemami prawnymi powinny sprzyjać dialogowi i wzajemnemu uczeniu się;

Oceny ryzyka w obszarze bezpieczeństwa, oceny skutków dla ochrony danych osobowych (DPIA) oraz oceny skutków dla praw podstawowych (FRIA) służą uzupełniającym się celom, lecz różnią się zakresem, wymogami prawnymi i konsekwencjami;

Wrażliwy charakter danych dotyczących zdrowia oraz konsekwencje ich niewłaściwego wykorzystania dla osób fizycznych i grup wymagają skutecznych zabezpieczeń na wszystkich etapach ich gromadzenia, udostępniania, wymiany i ponownego wykorzystywania;

Niezależne, odpowiednio wyposażone w zasoby i dostępne organy nadzorcze są niezbędne dla budowania zaufania publicznego, skutecznego egzekwowania prawa oraz rzeczywistego korzystania przez osoby fizyczne z przysługujących im praw;

Przypominając:

Deklarację warszawską w sprawie przyszłej współpracy z 17 grudnia 2001 r., Deklarację smolenicką w sprawie przyszłej współpracy z 24 maja 2005 r., Deklarację kazimierską w sprawie przyszłej współpracy z 3 czerwca 2008 r. oraz Deklarację w sprawie wzajemnej pomocy i zacieśnionej współpracy z 2–3 kwietnia 2014 r.;

Zasady wyrażone w Europejskiej konwencji praw człowieka, Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Konwencja nr 108, ETS nr 108), jej Protokole dodatkowym (ETS nr 181) oraz Protokole zmieniającym (CETS nr 223);

Znaczenie, w granicach ich odpowiednich zakresów stosowania, Karty praw podstawowych Unii Europejskiej, rozporządzenia (UE) 2016/679 (RODO), rozporządzenia (UE) 2024/1689 (akt w sprawie sztucznej inteligencji) oraz rozporządzenia (UE) 2025/327 w sprawie Europejskiej przestrzeni danych dotyczących zdrowia (EHDS);

Wkład Rady Europy w prace dotyczące sztucznej inteligencji i praw człowieka, w tym opracowanie metodyki HUDERIA, a także wkład Europejskiej Rady Ochrony Danych, Europejskiego Inspektora Ochrony Danych i innych forów współpracy w rozwijanie praktycznych sposobów reagowania na pojawiające się wyzwania;

uczestniczące w inicjatywie organy ochrony danych osobowych z Europy Środkowej i Wschodniej niniejszym deklarują swoje zobowiązanie, w granicach przysługujących im kompetencji i mających zastosowanie ram prawnych, z uwzględnieniem zakresu stosowania i dat rozpoczęcia stosowania odpowiednich instrumentów prawnych, do podejmowania następujących działań:

1. Wzmacnianie wspólnych podstaw i współpracy regionalnej

Promowanie wysokich standardów ochrony w całym regionie, wspieranie szerszego przystępowania do Konwencji nr 108 oraz zachęcanie właściwych stron do niezwłocznej ratyfikacji Protokołu zmieniającego i jego skutecznego wdrażania. Współpraca powinna wspierać organy przeprowadzające reformy prawne lub instytucjonalne oraz umożliwiać wszystkim uczestniczącym organom dzielenie się doświadczeniami.

2. Promowanie spójnej i merytorycznej oceny ryzyka związanego z systemami sztucznej inteligencji

W szczególności:

a) Zachęcanie do koordynowania procesów oceny z wykorzystaniem wspólnej podstawy faktycznej i dowodowej, obejmującej cel systemu, kontekst jego wdrożenia, przepływy danych oraz osoby, na które system oddziałuje.

b) Promowanie oceny zgodności z prawem, niezbędności i proporcjonalności przetwarzania, a także mniej ingerujących alternatyw przed wdrożeniem systemu, z jednoczesnym uwzględnieniem ryzyka dla osób fizycznych i grup. Środki bezpieczeństwa i korzystne wyniki oceny ryzyka nie mogą zastępować podstawy prawnej ani uzasadniać przetwarzania naruszającego prawa podstawowe.

c) Zachęcanie do przeprowadzania ocen na wszystkich etapach cyklu życia systemu, z udokumentowanym podziałem odpowiedzialności, dowodami skuteczności zastosowanych zabezpieczeń oraz ponowną oceną w przypadku zmiany systemu, jego celów, wykorzystywanych danych lub kontekstu wdrożenia. Oceny powinny prowadzić do konkretnych decyzji o zgodnym z prawem wdrożeniu systemu, jego modyfikacji, zawieszeniu lub rezygnacji z wdrożenia, a także do uprzednich konsultacji lub zastosowania innych procedur regulacyjnych, jeżeli są one wymagane.

d) Wymiana doświadczeń dotyczących praktycznych metod oceny, w tym metodyki HUDERIA oraz odpowiednich narzędzi do oceny skutków dla prywatności i praw człowieka, przy uznaniu, że ich stosowanie musi być dostosowane do konkretnego kontekstu i samo w sobie nie stanowi potwierdzenia zgodności z prawem.

3. Zapewnienie centralnego miejsca osobom i społecznościom, na które oddziałuje sztuczna inteligencja, w zarządzaniu jej wykorzystaniem

W szczególności:

a) Promowanie rzeczywistego udziału osób, na które oddziałują systemy, oraz odpowiednich interesariuszy, ze szczególnym uwzględnieniem dzieci i osób znajdujących się w sytuacjach szczególnej podatności na zagrożenia. Oceny powinny uwzględniać skutki dyskryminacyjne, skumulowane oraz dotyczące całych grup, zwłaszcza w przypadkach, gdy sztuczna inteligencja wpływa na dostęp do edukacji, opieki zdrowotnej, zabezpieczenia społecznego lub innych podstawowych usług.

b) Zachęcanie do zapewniania zrozumiałych informacji, skutecznego nadzoru człowieka oraz dostępnych mechanizmów umożliwiających kwestionowanie wyników, korygowanie błędów i uzyskiwanie środków ochrony prawnej. Nadzór człowieka powinien być sprawowany przez osoby posiadające odpowiednie kompetencje, informacje, czas i uprawnienia, aby móc zakwestionować, a w uzasadnionych przypadkach odrzucić lub zmienić wynik wygenerowany przez system sztucznej inteligencji.

4. Rozwijanie wiarygodnych zasad zarządzania danymi dotyczącymi zdrowia i ich odpowiedzialnego wykorzystywania

W szczególności:

Wymiana doświadczeń i promowanie zabezpieczeń dotyczących wykorzystywania oraz udostępniania danych dotyczących zdrowia w opiece zdrowotnej, badaniach naukowych i innych zgodnych z prawem działaniach, ze szczególnym uwzględnieniem następujących kwestii:

a) Zapewnienie rzeczywistej możliwości korzystania przez osoby fizyczne z przysługujących im praw poprzez przekazywanie jasnych informacji, ustanowienie dostępnych procedur oraz wiarygodnych rozwiązań w zakresie uwierzytelniania i reprezentacji, w tym praktycznych sposobów uzyskiwania dostępu do własnych danych dotyczących zdrowia, żądania ich sprostowania i wykonywania innych praw wynikających z obowiązujących przepisów.

b) Zapewnienie, aby dalsze wykorzystywanie danych dotyczących zdrowia odbywało się na podstawie prawnej i w jasno określonych celach, z poszanowaniem zasady ograniczenia celu oraz minimalizacji danych, a także przy zastosowaniu skutecznych zabezpieczeń przed nieuprawnionym wykorzystaniem, dyskryminacją i innymi szkodliwymi konsekwencjami.

c) Promowanie wykorzystywania danych zanonimizowanych do celów badawczych i innych celów wtórnych, jeżeli realizacja danego celu jest w ten sposób możliwa. Jeżeli wykorzystanie danych osobowych jest niezbędne, należy stosować zabezpieczenia odpowiednie do ich wrażliwego charakteru i związanego z nimi ryzyka, w tym pseudonimizację, ograniczenia dostępu, bezpieczne przetwarzanie, rejestrowanie operacji oraz kontrolę ujawnianych wyników. Zabezpieczenia powinny uwzględniać ryzyko ponownej identyfikacji, w tym ryzyko wynikające z łączenia zbiorów danych.

d) Promowanie przejrzystości i rozliczalności w ramach rozwiązań służących udostępnianiu danych dotyczących zdrowia, w tym zapewnianie jasnych informacji o zbiorach danych, zamierzonych sposobach ich wykorzystania i warunkach dostępu, przy jednoczesnej ochronie poufności oraz zapewnieniu, że możliwość odnalezienia informacji o zbiorze danych nie oznacza sama w sobie upoważnienia do jego wykorzystania.

e) Doprecyzowanie zakresów odpowiedzialności i wzmocnienie praktycznej współpracy między organami ochrony danych, właściwymi organami ds. zdrowia i innymi odpowiednimi instytucjami, z uwzględnieniem krajowych rozwiązań instytucjonalnych. Współpraca ta powinna wspierać skuteczne rozpatrywanie skarg, skoordynowane reagowanie na incydenty oraz bezpieczną wymianę informacji, przy jednoczesnym zachowaniu uprawnień i niezależności zainteresowanych organów.

5. Wzmacnianie niezależności, potencjału i skuteczności organów nadzorczych

W szczególności:

a) Apelowanie do rządów i parlamentów o zagwarantowanie niezależności instytucjonalnej organów ochrony danych oraz zapewnienie im zasobów kadrowych, technicznych i finansowych adekwatnych do zakresu ich obowiązków, w tym nowych zadań wynikających z regulacji dotyczących środowiska cyfrowego. Organy te powinny być angażowane na wczesnym etapie prac nad odpowiednimi zmianami legislacyjnymi i instytucjonalnymi.

b) Wymiana doświadczeń w zakresie zapewniania interdyscyplinarnej wiedzy eksperckiej, szkolenia personelu, ustalania priorytetów nadzorczych oraz oceny własnej działalności. Ocena ta powinna uwzględniać jakość, terminowość i praktyczne skutki działań nadzorczych dla przestrzegania przepisów oraz realizacji praw osób fizycznych, z uwzględnieniem różnic w zakresie kompetencji, zasobów i uwarunkowań krajowych.

6. Zapewnienie praktycznego, inkluzywnego i trwałego charakteru współpracy

W szczególności:

a) Ułatwianie bezpośrednich kontaktów zawodowych, dobrowolnej wymiany doświadczeń między organami oraz wzajemnej pomocy, również w sprawach transgranicznych, w zakresie dozwolonym przez prawo. Wymiana informacji musi odbywać się z poszanowaniem obowiązujących wymogów dotyczących poufności, ochrony danych osobowych i przekazywania danych do państw trzecich lub organizacji międzynarodowych.

b) Wykorzystywanie istniejących kanałów współpracy oraz dorobku Rady Europy, Konferencji Wiosennej, Europejskiej Rady Ochrony Danych (EROD), Europejskiego Inspektora Ochrony Danych (EIOD) i innych właściwych sieci współpracy, tak aby unikać niepotrzebnego powielania działań i udostępniać przydatne doświadczenia organom w całej inicjatywie.

Niniejsza deklaracja odnawia zobowiązanie uczestniczących organów do przekładania wspólnych zasad na skuteczną ochronę osób fizycznych. Poprzez praktyczną współpracę w obszarze sztucznej inteligencji i danych dotyczących zdrowia dążymy do wzmocnienia rozliczalności, zaufania publicznego i poszanowania praw podstawowych w całej Europie Środkowej i Wschodniej.

W ramach realizacji powyższych zobowiązań uczestniczące organy, na zasadzie dobrowolności oraz z uwzględnieniem zakresu swoich kompetencji i dostępnych zasobów, postanawiają:

a) Udostępniać uzgodnione, nieobjęte poufnością wnioski oraz materiały możliwe do ponownego wykorzystania, wypracowane podczas warsztatów w Zadarze, w tym praktyczne wnioski dotyczące ocen systemów sztucznej inteligencji i współpracy w zakresie zarządzania danymi dotyczącymi zdrowia.

b) Dokonać oceny postępów podczas kolejnego dorocznego spotkania, na podstawie dobrowolnie przekazanych informacji, oraz uzgodnić priorytety dalszej współpracy.

c) Upowszechniać przyjętą deklarację za pośrednictwem stron internetowych uczestniczących organów i odpowiednich sieci współpracy, a także przekazywać ją do wiadomości właściwym instytucjom krajowym.