URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 09/09/24

www.uodo.gov.pl

SPIS TREŚCI

WPROWADZENIE

Mirosław Wróblewski, Prezes Urzędu Ochrony Danych Osobowych S. 3

Karol Witowski, p.o. Rzecznika Prasowego UODO S. 5

1. ROZMOWA Z EKSPERTEM

Na dobre szkolenie nigdy nie jest za późno S. 7
– Dominika Dörre-Kolasa, członkini Społecznego Zespołu Ekspertów przy PUODO

2. UODO SYGNALIZUJE

Potrzebna nowelizacja przepisów ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich S. 12

Weryfikowanie pracowników firmy sprzątającej pod względem karalności na tle seksualnym S. 13

Podmiot ustawowo zobowiązany do sprawdzenia niekaralności osób na tle seksualnym sam musi wykonać swoje obowiązki S. 15

Numer alarmowy straży miejskiej – realizacja obowiązku informacyjnego S. 18

3. WYBRANE DECYZJE UODO

Odpowiedzialność dyrekcji szkoły za dane zawarte w piśmie z sądu rodzinnego S. 20

4. NARUSZENIA I KONTROLE

Prawa i obowiązki kontrolowanego S. 21

5. NOWE TECHNOLOGIE

Systemy rozpoznawania głosu a ich wpływ na ochronę danych i prywatność S. 26

6. SPRAWY MIĘDZYNARODOWE

W jaki sposób należy kontrolować i monitorować swoje polityki i procedury dotyczące prywatności danych w handlu elektronicznym S. 30

Dlaczego musimy uregulować korzystanie ze sztucznej inteligencji? S. 32

CNIL: zagrożenia związane z europejskim certyfikatem umożliwiającym zagranicznym organom dostęp do wrażliwych danych S. 49

DPC z zadowoleniem przyjmuje zgodę X na zawieszenie przetwarzania danych osobowych w celu szkolenia narzędzia AI „Grok” S. 51

7. EDUKACJA

Zaproszenie do uczestnictwa w XV edycji programu „Twoje dane – Twoja sprawa” S. 52

Zaproszenie na konferencję „RODO w edukacji” S. 53

Lista konferencji UODO S. 54

Szanowni Państwo,

powódź na południu kraju jest katastrofą, która jest sprawdzianem dla całego państwa. Instytucje publiczne muszą zareagować na to wyzwanie tak, by ułatwić odbudowę i powrót do normalnego życia. My w Urzędzie Ochrony Danych osobowych nie ograniczyliśmy się do zorganizowania zbiórki dla poszkodowanych w powodzi.

Pracujemy w trybie powodziowym

Rozumiemy, że wśród tysięcy pytań i problemów, jakie stają przed ludźmi na terenach dotkniętych powodzią, jest także pytanie o dane osobowe. A zadają je sobie teraz inspektorzy ochrony danych oraz ludzie, których dane dotyczą, jeśli wiedzą, że administratorzy tych danych zostali poszkodowani przez powódź.

Przypomnieliśmy więc, że co prawda istnieje obowiązek zgłoszenia naruszenia danych w ciągu 72 godzin, ale biegnie on dopiero od momentu jego stwierdzenia. Zdajemy sobie sprawę, że w wielu przypadkach będzie to możliwe dopiero po opanowaniu sytuacji i wstępnym oszacowaniu potencjalnych strat.

Pokreśliliśmy też, że jeśli nawet tak zdefiniowanego obowiązku nie da się wypełnić, trzeba będzie po prostu wyjaśnić przyczynę opóźnienia odwołując się do nadzwyczajnych warunków związanych z sytuacją powodziową.

UODO doskonale rozumie tę sytuację. Zwracamy jednak uwagę, że problemu utraty danych czy naruszenia ich bezpieczeństwa nie należy lekceważyć ani tym bardziej ukrywać. To też jest bardzo dotkliwy skutek powodzi, a zebranie danych o jego skali pozwoli na podjęcie odpowiednich działań.

UODO rusza w kraj

Korzystając z kolejnego wydania Biuletynu chciałbym też Państwu przekazać, że zaczynamy spotkania regionalne w Polsce. UODO nie ma jednostek terenowych, a sprawy związane z ochroną danych osobowych czy nietypowe problemy związane z tymi zagadnieniami występują wszędzie tam, gdzie są ludzie. Będziemy organizować spotkania z osobami zainteresowanymi tematyką, przedstawicielami organizacji pozarządowych, praktykami ochrony danych, władzami samorządowymi. Chcemy poznać Państwa perspektywę i lepiej zrozumieć Wasze problemy związane z ochroną danych osobowych. Pierwsze spotkania zostały zaplanowane w Krakowie i Tarnowie.

Kolejne będą odbywać się w miarę uzgodnień z władzami wojewódzkimi i samorządowymi. Po szczegóły zapraszam na naszą stronę internetową.

Spotkania regionalne są częścią programu otwarcia Urzędu Ochrony Danych Osobowych, o którym opowiadam Państwu w kolejnych Biuletynach. Jego częścią są regularne spotkania, które odbywamy z przedstawicielami społeczeństwa obywatelskiego i reprezentantów środowiska, które zawodowo zajmuje się kwestią danych osobowych. We wrześniu spotkaliśmy się m.in. z przedstawicielami Związku Miast Polskich, inspektorami ochrony danych osobowych w sądach, przedstawicielami Fundacji Onkologicznej Alivia; UNICEF; WWF; PAH a także Lekarzami bez Granic. Byliśmy obecni na spotkaniach Tour de Konstytucja, a także na 6. Warszawskiej Olimpiadzie Seniorów.

Bezpieczne dane w Ukrainie

Chciałbym zwrócić Państwa uwagę szczególnie na jedno spotkanie – z Yuliią Derkachenko, przedstawicielką Komisarza Parlamentu Ukrainy ds. Praw Informacyjnych. Spotkanie odbyło się w ramach organizowanego w Warszawie Forum Wymiany Doświadczeń Organów Ochrony Danych (Data Protection Authorities Experience Exchange Forum) 3 – 5 września. Wspieranie Ukrainy i wzmacnianie bezpieczeństwa danych obywateli Europy odbywa się także w ramach takich projektów jak EU4DigitalUA, którego celem jest cyfryzacja Ukrainy, w tym wsparcie w dostosowaniu ukraińskich przepisów ochrony danych osobowych do ram prawnych UE (warto wiedzieć, że koordynatorem projektu jest hiszpańska fundacja FIIAPP).

Ukraina przygotowuje się do utworzenia niezależnego organu nadzorczego, przedstawiciele Komisarza Parlamentu Ukrainy ds. Praw Człowieka poprosili UODO o podzielenie się doświadczeniami w tym obszarze. W ramach tej inicjatywy, przedstawiciele wybranych departamentów omawiali zadania i praktyczne aspekty pracy Urzędu w zakresie działalności edukacyjnej, legislacji i współpracy międzynarodowej. Nie zabrakło też tematów związanych z rozpatrywaniem skarg, prowadzeniem kontroli i postępowań w zakresie naruszeń oraz monitoringu i egzekwowania prawa, w tym nakładania administracyjnych kar pieniężnych.

Mirosław Wróblewski
Prezes UODO

Drodzy Czytelnicy!

Wrzesień to miesiąc, w którym naturalnie dużo miejsca poświęcamy edukacji. Co roku zachęcamy szkoły i placówki edukacyjne do udziału w ogólnopolskim programie edukacyjnym „Twoje dane – Twoja sprawa”. Nabór do aktualnej edycji potrwa do 24 października.

Z uwagi na to, że świętujemy jubileusz XV. edycji programu, na 10 października zaplanowaliśmy wyjątkową konferencję „RODO w edukacji”. Obok ekspertów Urzędu swój udział w wydarzeniu potwierdzili m.in. Rzeczniczka Praw Dziecka Monika Horna-Cieślak, Ministra Edukacji Narodowej Barbara Nowacka czy Mazowiecka Kuratorka Oświaty Wioletta Krzyżanowska.

Pozostając w temacie szkolnictwa, zachęcam do zapoznania się z wybraną przez nas decyzją Prezesa UODO o udzieleniu upomnienia szkole za publiczne przypisanie rodzicom ucznia autorstwa anonimu napisanego do sądu rodzinnego. Powiadomienie rodziców o wpłynięciu anonimu do sądu oraz poinformowanie o treści i przypisywanie autorstwa stanowiło naruszenie przepisów o ochronie danych osobowych.

W związku z prośbą o pomoc, z jaką zwrócił się jeden z inspektorów ochrony danych powołany przez uczelnię medyczną, tłumaczymy jak postępować w zgodzie z przepisami ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich.

Jak zauważył Prezes UODO w korespondencji skierowanej do Ministerstwa Sprawiedliwości potrzebna jest nowelizacja przepisów ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich. W tym kontekście zaciekawić może Was też temat weryfikacji pracowników firmy sprzątającej pod względem karalności na tle seksualnym.

Obowiązkową lekturą numeru jest wywiad z Dominiką Dörre-Kolasą – radczynią prawną, wykładowczynią uniwersytecką, bardzo aktywną członkinią Społecznego Zespołu Ekspertów przy PUODO. Dała się poznać przez swoje zaangażowanie w przybliżanie praktycznej wykładni stosowania ustawy o ochronie sygnalistów, a także prace nad aktualizacją poradnika ds. zatrudnienia. Cieszymy się, że znalazła chwilę, by porozmawiać z nami na temat bieżących spraw, jakimi zajmuje się jako członkini SZE.

Dowiadujecie się, że w Waszej firmie została zaplanowana kontrola Urzędu Ochrony Danych Osobowych? W tym numerze przedstawiamy Wam Wasze prawa i obowiązki jako podmiotu kontrolowanego, abyście wiedzieli, czego możecie się spodziewać i oczekiwać od nas – kontrolujących. Mamy także świadomość, że dla większości z Was jest to sytuacja stresogenna,

jednak zapewniamy, że kontrolujący starają się przeprowadzić niezbędne czynności w jak najlepszej atmosferze, a decyzja o nałożeniu kary jest ostatecznością.

Technologia rozpoznawania głosu staje się integralną częścią codziennego życia, umożliwiając bardziej naturalną i intuicyjną interakcję z urządzeniami elektronicznymi. Przyglądamy się, jaki wpływ mają systemy rozpoznawania głosu na ochronę danych i prywatność.

Unijny akt w sprawie sztucznej inteligencji jest pierwszym na świecie kompleksowym zbiorem przepisów dotyczących sztucznej inteligencji. Jego celem jest zaradzenie zagrożeniom dla zdrowia, bezpieczeństwa i praw podstawowych. Akt w formie rozporządzenia chroni również demokrację, praworządność i środowisko. Dlaczego musimy uregulować korzystanie ze sztucznej inteligencji? – temat przybliży Wam obszerny materiał Komisji Europejskiej, w formie pytań i odpowiedzi na ważne zagadnienia odnoszące się do AI Act.

Choć wrzesień przebiega pod znakiem edukacji, innych interesujących wątków w pierwszym powitalnym jesień numerze, jak widzicie, również nie zabraknie. Życzymy łatwego wejścia w nowy rok szkolny i stawienia czoła wyzwaniom dotyczącym ochrony danych osobowych, które się z nim wiążą.

Karol Witowski
p.o. Rzecznika Prasowego UODO

1 ROZMOWA Z EKSPERTEM

NA DOBRE SZKOLENIE NIGDY NIE JEST ZA PÓŹNO

Z Dominiką Dörre-Kolasą, członkinią Społecznego Zespołu Ekspertów przy PUODO rozmawiał Karol Witowski, p.o. Rzecznika Prasowego UODO

16.09.2024 r. w Gdańsku odbyła się konferencja „Wdrożenie ustawy o sygnalistach oraz ochrona danych osobowych w miejscu pracy". Wraz z dr Arletą Nerką prowadziła Pani panel „Procedura zgłoszeń wewnętrznych i działań następczych – zgodne z RODO". Na wstępie podkreśliła Pani, że procedura nie jest tylko dokumentem. Powinna odzwierciedlać procesy przetwarzania danych.

Procedura powinna odzwierciedlać to, co się dzieje. Z mojego doświadczenia – jestem czynnym radcą prawnym, praktykiem – obserwuję tendencję zupełnie odwrotną.

Podmioty skupiają się na samym dokumencie, żeby go mieć na 25 września (wtedy zaczną obowiązywać nowe przepisy) lub, jak niektórzy wierzą, 1 stycznia (obowiązek wdrożenia procedury zgłoszeń wewnętrznych dotyczy podmiotów, na rzecz których według stanu na dzień 1 stycznia danego roku wykonuje pracę zarobkową co najmniej 50 osób). Procedury często tworzone są według listy z ustawy, by ten dokument zawierał w sobie wszystkie elementy, a to nie jest wystarczające. Podobnie przekonsultowanie z przedstawicielami osób wykonujących pracę nie powinno być tylko odhaczoną formalnością. Jak jakakolwiek procedura ma działać, to trzeba ją dobrze wdrożyć, a pracownicy powinni ją rozumieć. Czasem takie spojrzenie z perspektywy ich przedstawicieli może dostarczyć informacji o tym, czy zapisy dokumentu są zrozumiałe.

Niewiele organizacji patrzy na procedurę z perspektywy procesów przetwarzania danych. Chciałabym, żeby w okresie stosowania ustawy, bo teraz obawiam się, że już nie zdążymy, zmienić to myślenie. Zadbajmy, jak pan prezes Mirosław Wróblewski, podkreślił – o to, żeby od momentu przyjęcia zgłoszenia, analizy tego zgłoszenia, a później, działań następczych – te wszystkie czynności, które będą podejmowane, były podejmowane zgodnie z zasadami ochrony danych osobowych przez osoby, które rozumieją na czym polegają ryzyka ich naruszenia.

1 ROZMOWA Z EKSPERTEM

Apeluje Pani, by organizacje przeprowadziły szkolenia z ochrony danych dla osób, które będą się zajmowały przyjmowaniem zgłoszeń i ich analizą. Dlaczego to takie ważne, by zrobić je teraz? Większość firm robiła takie szkolenia jakiś czas temu.

Obawiam się, że większość firm przeprowadziła szkolenia dawno temu, a nawet jak są one cyklicznie ponawiane, to przeważnie cechuje je duży poziom ogólności. Pamiętajmy, że na dobre szkolenie nigdy nie jest za późno. Lepiej je przeprowadzić teraz, lub w nieodległym czasie od rozpoczęcia stosowania zapisów procedur – zanim dojdzie do sytuacji, że dane zawarte w zgłoszeniu zostaną ujawnione lub utracone. Szkolenia mogą też pomóc we wdrożeniu praktycznych rozwiązań, odpowiadających realiom danej firmy czy instytucji. Najlepiej byłoby, aby były „uszyte na miarę" i dedykowane konkretnej firmie, z uwzględnieniem tych ryzyk, które są powiązane z przyjętymi przez organizację sposobami przyjmowania zgłoszeń i prowadzenia działań następczych.

Czyje dane osobowe podmiot prawny ma chronić w związku ze stosowaniem ustawy o ochronie sygnalistów?

Choć ta ustawa rzeczywiście nazywa się ustawą o ochronie sygnalistów, to należy podkreślić, że sygnalista nie jest „lepszym" podmiotem danych, który zasługuje na ochronę niż np. osoba, której dane dotyczą, czy też świadkowie. Oczywiście zaakcentowanie w ustawie konieczności zachowania w poufności tożsamości sygnalisty ma uzasadnienie w tym, żeby go chronić przed działaniami odwetowymi. Ochrona jego danych nie jest zatem silniejsza, tylko nieco inna, gdyż nacisk położony jest na te dane, które pozwalają na ustalenie jego tożsamości. Byłoby dobrze, aby to zogniskowanie ochrony danych na osobie sygnalisty uległo zmianie, tak by osoby przyjmujące zgłoszenia i analizujące je, nie skupiały się szczególnie na sygnaliście, bo nie ma żadnej różnicy w zasadach ochrony danych osobowych sygnalisty i innych osób.

Podobny problem obserwujemy w innych procedurach wewnątrzzakładowych. Tak dzieje się często w procedurach antymobbingowych czy antydyskryminacyjnych, gdzie po zgłoszeniu działań noszących np. znamiona mobbingu, koncentrujemy się na ofierze. Tymczasem, jeżeli już, powinniśmy koncentrować się na domniemanym sprawcy, ale pamiętać, że reguły, zasady ochrony danych osobowych w tym zakresie są takie same, niezależnie od tego, o której osobie uczestniczącej w procedurze mówimy.

Ustawa o ochronie sygnalistów spotkała się z falą krytyki ze strony ekspertów ochrony danych osobowych. Co, Pani zdaniem, trzeba zmienić/ doprecyzować w tej ustawie, żeby uznać ją za dobrą?

1 ROZMOWA Z EKSPERTEM

Prawda jest taka, że czas pokaże, co jest dobrym, a co złym rozwiązaniem. Na tę chwilę w mojej ocenie największy problem będzie ze stosowaniem wspólnej procedury w grupach kapitałowych. Nie jest bowiem jasne, czy wspólna procedura daje możliwość korzystania ze wspólnych zasobów, nie tylko do przyjmowania zgłoszeń, ale również do podejmowania działań następczych.

W bardzo wielu podmiotach od lat funkcjonują systemy zgłaszania nieprawidłowości – one są sprawdzone, wyspecjalizowane. Większość podmiotów nie ma możliwości zorganizować wewnątrz swoich zasobów osób, które będą merytorycznie przygotowane i na tyle bezstronne. Nie są w stanie znaleźć takich osób.

Praktyka jak widzę jest bardzo różna, od utrzymywania status quo, po tworzenie rozwiązań, które tylko z pozoru mają odzwierciedlać wymaganie ustawy, aby działania następcze były prowadzone przez jednostki czy podmioty funkcjonujące w strukturze wewnątrz podmiotu prawnego. Wolałabym jednak, aby nie ukrywać rzeczywistych działań w tym zakresie, gdyż to może osłabić ochronę danych osobowych przetwarzanych w ramach tych procesów. Nie bez znaczenia dla ich oceny z perspektywy zasad ochrony danych będzie oczywiście całkowity brak przejrzystości i transparentności.

Jak powinno wyglądać upoważnienie podmiotów zewnętrznych? Które elementy należy w bezwzględnie uwzględnić?

Zacznę od tego, że zgłoszenia nie muszą być przyjmowane wyłącznie przez wewnętrzną jednostkę organizacyjną bądź osobę w strukturze. Tu jest możliwość powierzenia określonych czynności na zewnątrz. W art. 28 ustawy jest napisane, że upoważnienie podmiotu zewnętrznego, o którym mowa w art. 25 ust. 1 pkt 1, wymaga zawarcia umowy w celu powierzenia obsługi przyjmowania zgłoszeń wewnętrznych, potwierdzania przyjęcia zgłoszenia, przekazywania informacji zwrotnej oraz dostarczania informacji na temat procedury zgłoszeń wewnętrznych z zastosowaniem rozwiązań technicznych i organizacyjnych zapewniających zgodność tych czynności z ustawą.

Podpisując umowę, musimy zdecydować, co ten podmiot ma robić, jakie działania. Może np. tylko przyjmować zgłoszenia. Do tego, do czego ten podmiot upoważnimy, będzie wynikało to, co on może robić z danymi osobowymi – nie tylko zgłaszającego. Wraz z przyjęciem kwestionariusza zgłoszenia, podmiot dostaje masę informacji: nt. współpracowników sygnalisty, przełożonego, osoby której dotyczy zgłoszenie.

W ramach umowy należy określić procesy przetwarzania danych: czy ten podmiot ma wyłącznie umożliwić wpływ zgłoszeń, a następnie ma je przekazać, czy też będą one przechowywane z możliwością dostępu do nich uprawnionych osób, czy podmiot ten może się kontaktować z sygnalistą np. odpowiadać na jego pytania, informować go o przyjęciu zgłoszenia, przekazywania mu informacji zwrotnej itp.

1 ROZMOWA Z EKSPERTEM

Jak to działa w praktyce? Podmioty upoważnione do działań następczych również otrzymują loginy i hasła do zgłoszenia i na platformie odbywa się cały proces komunikacji z sygnalistą. O ile z ustawy to nam wprost nie wynika, że tak można działać, to pod kątem umowy powierzenia przetwarzania danych, musimy te wszystkie elementy uwzględnić.

To, co jest warte podkreślenia, to jest to, iż zanim wybierzemy podmiot, sprawdzamy, czy on daje odpowiednie gwarancje zarówno techniczne, jak i organizacyjne, a więc wypisujemy nasze oczekiwania względem podmiotu, a on zapewnia, że jest je w stanie spełnić. Jeśli tak, to podpisujemy umowę. Praktyka niestety jest zupełnie inna.

Wybór podmiotu, który będzie przetwarzał nasze dane osobowe podlega RODO. Dlatego wybierając ten podmiot, powinniśmy go oceniać z perspektywy wycieku danych. Zastanowić się, co zrobimy, gdy dane zostaną ujawnione, np. okaże się, że wiadomości mailowe zostały przekierowane na inną skrzynkę. Ważne, by sprawdzić, jak ten podmiot wtedy zareaguje. Spytać jakie ma zabezpieczenia. Warto rozmawiać z procesorami.

Jeśli z uwagi na ograniczony budżet, wybieramy najtańszy podmiot, zdajmy sobie sprawę z ryzyka, jakie to za sobą niesie.

Podkreśliła Pani podczas seminarium, że podmiot prawny nie ma kompetencji śledczych i nie może przesłuchiwać świadków w trybie KPK. Tymczasem na podstawie procedur niektórych podmiotów można wywnioskować, że jest inaczej.

Bo nie ma. Ustawa nie daje mu takich kompetencji, co więcej w wielu przypadkach osoby prowadzące postepowania wyjaśniające nie znają przepisów postepowania karnego na tyle, aby się nimi sprawnie posługiwać. Nikt chyba nie myślałby o np. przymusowym doprowadzeniu świadka przed oblicze takiej wewnątrz firmowej komisji. Można oczywiście zapisać, że jak ktoś ma wiedzę o okolicznościach, o które będzie pytany, to jest obowiązany do ich ujawnienia, podobnie jak w przypadku dowodów, ale ciągle nie będzie to się odbywało na takich samych zasadach jak procedują podmioty publiczne.

Prowadziła Pani również panel podczas seminarium UODO „Praktyczne problemy w stosowaniu przepisów ustawy o ochronie sygnalistów z perspektywy RODO. Przyczynek do dyskusji nad wątpliwościami zgłoszonymi w trakcie konsultacji społecznych.” Czy Pani zdaniem to seminarium pozwoliło wyjaśnić pewne kwestie czy raczej zrodziły się nowe wątpliwości? W czasie spotkania panowała prawdziwa burza mózgów.

1 ROZMOWA Z EKSPERTEM

Wiele wątpliwości udało się wyjaśnić, ale liczny udział słuchaczy podczas kolejnych wydarzeń poświęconych tej problematyce pokazuje, iż jest niesłabnąca potrzeba organizowania takich wydarzeń. Jest też oczywistym, że pojawią się najprawdopodobniej nowe pytania jak zaczniemy stosować ustawę.

Jest Pani członkiem Społecznego Zespołu Ekspertów przy PUODO. Prowadzi Pani projekt naukowo-badawczy, realizowany w Katedrze Prawa Pracy i Polityki Społecznej, który zainaugurował spotkanie w siedzibie Urzędu – 31 lipca 2024 r. odbyło się w UODO seminarium „Przetwarzanie danych osobowych przez związki zawodowe. Od teorii do praktyki w kierunku poradnika". Uczestniczy też Pani w pracach podgrupy roboczej poświęconym poradnikowi ds. zatrudnienia. Chodzi o aktualizację poradnika dotyczącego przetwarzania danych przy zatrudnianiu, który pod nazwą „Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców" ukazał się w 2018 r. Na jakim etapie są prace?

Jeżeli chodzi o poradnik dla związków zawodowych, to w najbliższym czasie rozpocznie się badanie ankietowe, którego zwieńczeniem będzie przedstawienie raportu z badania podczas konferencji, najprawdopodobniej w pierwszym tygodniu grudnia.

Co do poradnika dla pracodawców, tam jest nieco łatwiej, gdyż jest punkt odniesienia w postaci poradnika, którego zapisy są przez nas analizowane wspólnie z pracownikami Urzędu i w miarę potrzeby poddawane zmianom. Zdarza się, ze mamy różne punkty widzenia, ale staramy się wówczas w drodze dyskusji i przedstawiania argumentów wypracowywać rozwiązania, które pozwolą na to, aby poradnik był jak najbardziej użyteczny i odpowiadał na aktualne bolączki pracodawców.

Na co dzień kieruje Pani zespołem ochrony danych osobowych w kancelarii oraz wykłada Pani w Katedrze Prawa Pracy i Polityki Społecznej Uniwersytetu Jagiellońskiego. Jednocześnie jest Pani bardzo zaangażowana w prace SZE przy PUODO. Jest Pani bardzo zapracowana. Czy w Pani życiu jest miejsce na pasje inne niż prawo, czy pracy i nauce oddaje się Pani całkowicie?

Nie jest łatwo godzić te wszystkie aktywności, to fakt. Czasu wolnego faktycznie nie mam za wiele, a jak już się pojawi, szybko udaje się go wypełnić np. pracą nad publikacjami. Nie jestem w tym zakresie asertywna, zwłaszcza że propozycje przychodzą od osób, które lubię i cenię. Ale dla moich dwóch berneńskich psów pasterskich czas znajdę zawsze.

POTRZEBNA NOWELIZACJA PRZEPISÓW USTAWY O PRZECIWDZIAŁANIU ZAGROŻENIOM PRZESTĘPCZOŚCIĄ NA TLE SEKSUALNYM I OCHRONIE MAŁOLETNICH

W korespondencji skierowanej do Ministerstwa Sprawiedliwości Prezes UODO wskazał, że przepisy ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich wymagają doprecyzowania.

W związku z nowelizacją ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich do UODO wpływają pytania i prośby o interpretację nowych przepisów. Świadczą one o tym, że przyjęte regulacje są nieprecyzyjne.

W opinii Prezesa UODO konieczne jest wyeliminowanie tych wątpliwości poprzez wprowadzenie odpowiednich zmian w powołanej ustawie. Jej przepisy powinny precyzyjnie określać, czyje dane osobowe, w jakim zakresie i w związku z realizacją jakiego celu mają być przetwarzane.

Taka analiza i wyważenie wartości jest bardzo istotne, ponieważ analizowane przepisy służą ważnemu celowi, jakim jest bezpieczeństwo dzieci. Jednocześnie na ich podstawie przetwarzane są dane dotyczące wyroków skazujących oraz czynów zabronionych, co wiąże się ze znaczną ingerencją w prawa i wolności osób fizycznych.

Na co powinien zwrócić uwagę administrator związany zmienionymi przepisami ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym, UODO wskazał w komunikacie „Jak stosować „ustawę Kamilka" w zgodzie ze standardami ochrony danych osobowych".

Natomiast w tym wydaniu Biuletynu UODO w materiałach „Weryfikowanie pracowników firmy sprzątającej pod względem karalności na tle seksualnym" oraz „Podmiot ustawowo zobowiązany do sprawdzenia niekaralności osób na tle seksualnym sam musi wykonać swoje obowiązki" przedstawiamy wskazówki związane ze stosowaniem tych przepisów w obecnym brzmieniu. Zostały one przygotowane na podstawie wyjaśnień udzielonych inspektorom ochrony danych.

WERYFIKOWANIE PRACOWNIKÓW FIRMY SPRZĄTAJĄCEJ POD WZGLĘDEM KARALNOŚCI NA TLE SEKSUALNYM

Firma, która świadczy usługi utrzymania czystości na terenie szpitala, nie ma podstaw, aby od zatrudnianych w niej osób żądać informacji o niekaralności za przestępstwa na tle seksualnym. Także szpital nie może żądać przedstawienia takich danych.

Jednym z kluczowych rozwiązań mających chronić dzieci przed wykorzystaniem seksualnym jest obowiązkowa weryfikacja osób, które mają z nimi kontakt w czasie pracy. Odbywa się ona zarówno poprzez pozyskiwanie informacji z Rejestru Sprawców Przestępstw na Tle Seksualnym, jak i poprzez obowiązek przedłożenia zaświadczenia o niekaralności z Krajowego Rejestru Karnego.

Rejestr Sprawców Przestępstw na Tle Seksualnym (utworzony na mocy art. 4 ust. 1 ustawy z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniu przestępczością na tle seksualnym i ochronie małoletnich, zwany dalej "Rejestrem") składa się z trzech oddzielnych baz danych:

• rejestru z dostępem ograniczonym,

• rejestru publicznego,

• rejestru osób, w stosunku do których Państwowa Komisja do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15, wydała postanowienie o wpisie w Rejestrze.

W Rejestrze z dostępem ograniczonym (zgodnie z art. 6 ww. ustawy) gromadzi się, z zastrzeżeniem art. 9 ust. 1-3, dane o osobach:

• prawomocnie skazanych za popełnienie przestępstw, o których mowa w art. 2, czyli przeciwko wolności seksualnej wymienionych w rozdziale XXV ustawy z dnia 6 czerwca 1997 r. - Kodeks karny,

• przeciwko którym prawomocnie warunkowo umorzono postępowanie karne w sprawach o przestępstwa, o których mowa w art. 2,

• wobec których prawomocnie orzeczono środki zabezpieczające w sprawach o przestępstwa, o których mowa w art. 2,

• nieletnich, wobec których prawomocnie orzeczono środki wychowawcze, środek poprawczy lub środek leczniczy na podstawie ustawy z dnia 9 czerwca 2022 r. o wspieraniu i resocjalizacji nieletnich w sprawach o czyny karalne, o których mowa w art. 2, z wyłączeniem art. 200 § 1 Kodeksu

karnego.

Omawiana ustawa w art. 12 wymienia podmioty, którym przysługuje prawo do uzyskania informacji o osobie ujętej w Rejestrze, której dane zostały zgromadzone w Rejestrze z dostępem ograniczonym. Prawo to przysługuje m.in. pracodawcy przed nawiązaniem z osobą stosunku pracy związanej z wychowaniem, edukacją, wypoczynkiem, leczeniem, świadczeniem porad psychologicznych, rozwojem duchowym, uprawianiem sportu lub realizacją innych zainteresowań przez małoletnich, lub z opieką nad nimi, w zakresie uzyskania informacji, czy dane tej osoby są zgromadzone w tym Rejestrze (art. 12 pkt 6).

Zatem skoro przepis wyraźnie określa, w jakich sytuacjach pracodawca może pozyskać informacje z ww. Rejestru, wymieniając, że chodzi o zatrudnienie związane z wychowaniem, edukacją, wypoczynkiem, leczeniem, świadczeniem porad psychologicznych, rozwojem duchowym, uprawianiem sportu lub realizacją innych zainteresowań przez małoletnich, lub z opieką nad nimi, to uprawnienia tego nie można odnieść do pracowników zatrudnionych w innym charakterze. Tym samym pracodawca, którego firma świadczy usługi utrzymania czystości na terenie szpitala, nie ma podstaw, aby pozyskiwać dane z ww. Rejestru.

O ile szpital jest zobowiązany do wprowadzenia standardów ochrony małoletnich, zgodnie z art. 22b ww. ustawy, i w tym celu ma prawo pozyskać informacje z ww. Rejestru, to może to zrobić tylko wobec swoich pracowników przed nawiązaniem z nimi stosunku pracy związanej z tymi czynnościami, o których mowa w art. 12 pkt 6 ustawy.

Szczegółowe zasady związane z obowiązkiem pracodawcy w zakresie uzyskania informacji z Rejestru przed zatrudnieniem, a także obowiązek przedłożenia informacji z Krajowego Rejestru Karnego lub rejestru karnego innego państwa określa Rozdział 3 ww. ustawy.

Fot. pixabay

PODMIOT USTAWOWO ZOBOWIĄZANY DO SPRAWDZENIA NIEKARALNOŚCI OSÓB NA TLE SEKSUALNYM SAM MUSI WYKONAĆ SWOJE OBOWIĄZKI

Porozumienia nie mogą zastępować norm prawnych ani tworzyć niewynikających z nich nowych kompetencji.

O pomoc w ustaleniu właściwego sposobu postępowania w związku ze stosowaniem przepisów ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich zwrócił się jeden z inspektorów ochrony danych (IOD) powołany przez uczelnię medyczną.

Jak wskazał, uczelnia medyczna jest organizatorem procesu kształcenia, w tym praktyk oraz zajęć klinicznych, które odbywają się w podmiotach leczniczych, na podstawie zawartych z tymi podmiotami umów. W związku z tym, że organizowana działalność spełnia przesłanki z art. 21 ust. 1 wyżej powołanej ustawy, tj. wiąże się z edukacją, leczeniem, opieką nad małoletnimi pacjentami podmiotów leczniczych, Uczelnia dokonuje weryfikacji skierowanych na praktyki i zajęcia w podmiocie leczniczym studentów w Rejestrze z dostępem ograniczonym poprzez konto instytucjonalne oraz w Rejestrze osób, w stosunku do których Państwowa Komisja do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15 wydała postanowienie o wpisie w Rejestrze.

Jeżeli okazałoby się, że student, który ma zostać skierowany na praktykę widnieje w ww. rejestrach, uczelnia nie może dopuścić go do odbycia tejże praktyki.

Jednocześnie uczelnia zobowiązała studentów do dostarczenia jej informacji z Krajowego Rejestru Karnego w zakresie przestępstw określonych w rozdziale XIX i XXV Kodeksu karnego, w art. 189a i art. 207 Kodeksu karnego oraz w ustawie z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii
lub za odpowiadające tym przestępstwom czyny zabronione określone w przepisach prawa obcego.

Kwestią sporną jest natomiast zwracanie się przez podmioty lecznicze, w których studenci będą odbywali praktyki, o:

1) przedkładanie przez uczelnię podmiotowi leczniczemu przed rozpoczęciem praktyki aktualnej

informacji, czy dane studenta są zamieszczone w Rejestrze z dostępem ograniczonym lub w Rejestrze osób, w stosunku do których Państwowa Komisja do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15 wydała postanowienie o wpisie w Rejestrze,

2) składanie przez uczelnię oświadczeń, że studenci posiadają aktualne zaświadczenie z Krajowego Rejestru Karnego w zakresie przestępstw określonych w rozdziale XIX i XXV Kodeksu karnego, w art. 189a i art. 207 Kodeksu karnego oraz w ustawie z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii lub za odpowiadające tym przestępstwom czyny zabronione określone w przepisach prawa obcego,

3) umowne zagwarantowanie podmiotowi leczniczemu uprawnienia do weryfikacji danych zgromadzonych przez uczelnię w wykonaniu obowiązków z art. 21 ww. ustawy poprzez udostępnienie tych danych w formie kopii lub wglądu w oryginały dokumentów.

UODO, odpowiadając na wątpliwości IOD, wskazał, że przepisy ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich określają, jakie podmioty są zobowiązane do pozyskiwania danych osób podlegających sprawdzeniu, o którym mowa w art. 21 tej ustawy.

Zgodnie z ustępem 1 powołanego przepisu przed nawiązaniem z osobą stosunku pracy lub przed dopuszczeniem osoby do innej działalności związanej z wychowaniem, edukacją, wypoczynkiem, leczeniem, świadczeniem porad psychologicznych, rozwojem duchowym, uprawianiem sportu lub realizacją innych zainteresowań przez małoletnich, lub z opieką nad nimi na pracodawcy lub innym organizatorze takiej działalności oraz na osobie, z którą ma być nawiązany stosunek pracy lub która ma być dopuszczona do takiej działalności, ciążą obowiązki określone w ust. 2-8, w tym obowiązek pozyskania informacji z Rejestru Sprawców Przestępstw na Tle Seksualnym, z Krajowego Rejestru Karnego lub rejestru karnego innego państwa.

Pozyskane informacje pracodawca lub inny organizator załącza do akt osobowych pracownika albo dokumentacji dotyczącej osoby dopuszczonej do takiej działalności (art. 21 ust. 9).

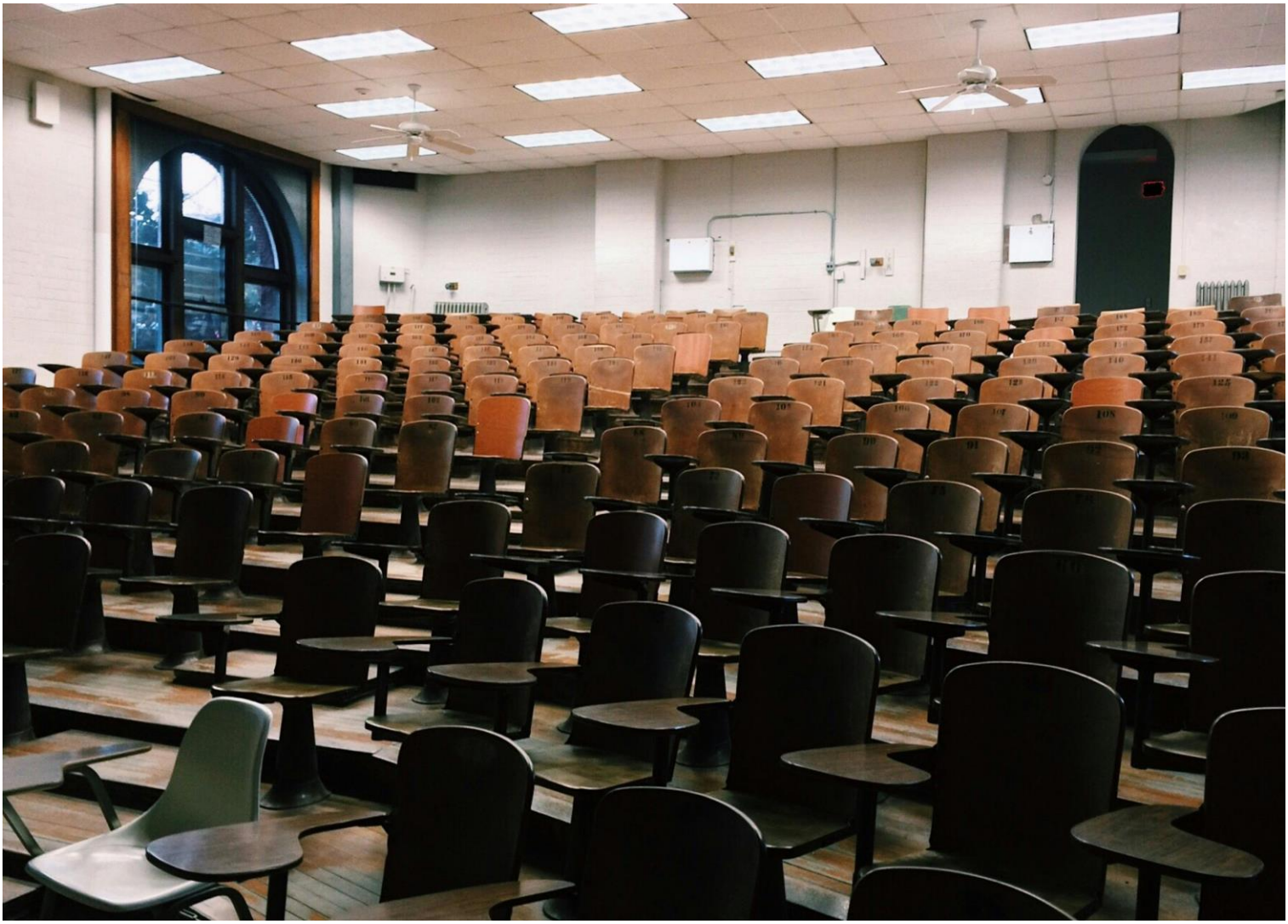
Z powyższych przepisów wynika, że każdy z wymienionych wyżej podmiotów zobowiązany jest do odrębnego pozyskania wskazanych informacji w opisany w ustawie sposób. Ustawodawca nie przewidział współdziałania między nimi – ani wymiany, ani udostępniania informacji pozyskanych przez nie na podstawie powołanej ustawy.

Jeżeli prawodawca określił katalog działań służących osiągnięciu wskazanego celu, to podmiot go realizujący powinien podejmować jedynie te z nich, które są wskazane w przepisach prawa. Uregulowania te stanowią podstawę prawną legalizującą przetwarzanie danych osobowych przez wskazane w nich podmioty.

Natomiast wszelkie porozumienia zawierane pomiędzy takimi podmiotami nie mogą zastępować

norm prawnych ani tworzyć niewynikających z nich nowych kompetencji.

W przedstawionej sytuacji przede wszystkim należałoby ustalić, który z podmiotów, czy może oba, zobowiązane są do dokonania sprawdzenia osób, o którym mowa w art. 21 ustawy o ochronie małoletnich. Następnie każdy podmiot zobowiązany powinien samodzielnie wykonać ciążące na nim obowiązki.



Fot. pexels

NUMER ALARMOWY STRAŻY MIEJSKIEJ – REALIZACJA OBOWIĄZKU INFORMACYJNEGO

Istota, specyfika oraz cel przetwarzania danych osobowych w związku z wykonywaniem połączeń alarmowych do straży miejskiej uzasadniają przyjęcie założenia, że do spełnienia obowiązku informacyjnego wystarczające jest udostępnienie stosownej klauzuli w Biuletynie Informacji Publicznej, na stronie internetowej straży miejskiej oraz w widocznym miejscu w jej siedzibie.

W wielu miejscowościach pod numerem 986 działa telefon alarmowy do straży miejskiej. Połączenia z nim cechują się dużą specyfiką – często wykonywane są w sytuacji stresogennej, w pośpiechu i poczuciu zagrożenia.

Niejednokrotnie szybkie uzyskanie połączenia z numerem alarmowym jest kluczowe dla ochrony życia i zdrowia ludzkiego czy mienia. Straż miejska – we współpracy z innymi służbami – realizuje bowiem wiele istotnych zadań. Udziela m.in. pomocy przy usuwaniu skutków wypadków, awarii technicznych czy klęsk żywiołowych, dba o ochronę porządku publicznego. Tymczasem przed połączeniem z dyżurnym trzeba wysłuchać dość długiego komunikatu dotyczącego przetwarzania danych osobowych.

W opinii UODO nie jest to konieczne.

Rozważając sposób dopełnienia obowiązku informacyjnego wobec osób dzwoniących na numer alarmowy, w każdym przypadku należy dążyć do pogodzenia obowiązków wynikających z RODO z podstawowym celem przetwarzania danych osobowych, jakim jest szybkie udzielenie pomocy.

W tym kontekście warto zwrócić uwagę na regulację zawartą w art. 10 ust. 13 ustawy z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego, zgodnie z którą w związku z przetwarzaniem danych osobowych w systemie teleinformatycznym wspomagającym realizację zadań przez centra powiadamiania ratunkowego, wykonanie obowiązku informacyjnego, o którym mowa w art. 13 ust. 1 i 2 RODO, następuje przez udostępnienie informacji w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw administracji publicznej, wojewody lub podmiotu, o którym mowa w art. 7 ust. 2, na ich stronach internetowych oraz w widocznym miejscu w ich siedzibie.

2 UODO SYGNALIZUJE

Istotne z punktu widzenia ustawowych zadań straży miejskiej są w omawianym zakresie również postanowienia ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Stosownie do jej art. 22 ust. 2, informacje dotyczące realizacji praw osób, w tym m.in. o nazwie, siedzibie i danych kontaktowych administratora oraz celu, do których mają posłużyć dane osobowe, udostępnia się na stronie internetowej, w Biuletynie Informacji Publicznej na stronie podmiotowej właściwego organu lub urzędu lub w jego siedzibie.

Jak z kolei wskazano w Wytycznych Grupy Roboczej Art. 29 w sprawie przejrzystości na podstawie rozporządzenia 2016/679, „jeżeli administrator danych prowadzi stronę internetową (lub prowadzi całość lub część swojej działalności za pośrednictwem strony internetowej), GR29 zaleca stosowanie warstwowych oświadczeń o ochronie prywatności / warstwowych informacji o polityce prywatności, dzięki którym osoby odwiedzające stronę internetową mogą zapoznać się z najbardziej interesującymi dla nich fragmentami danego oświadczenia o ochronie prywatności / informacji o polityce prywatności (więcej informacji na temat oświadczeń o ochronie prywatności / informacji o polityce prywatności znajduje się w pkt 35–37). Osoby, których dane dotyczą, powinny mieć jednak dostęp do wszystkich skierowanych do nich informacji również w jednym miejscu lub w ramach jednego dokumentu (elektronicznego lub papierowego), który powinien być łatwo dostępny dla takiej osoby, jeżeli zechce ona zapoznać się ze wszystkimi skierowanymi do niej informacjami”.

Zgodnie z pkt 19 wytycznych najważniejsze jest, aby wybrane metody udzielania informacji były dostosowane do konkretnej sytuacji, tj. do sposobu komunikacji między administratorem danych a osobą, której dane dotyczą, lub sposobu zbierania informacji odnoszących się do tej osoby. Wybór tych rozwiązań należy do administratora. Wytyczne te co do zasady uznają jednak zebranie wszystkich niezbędnych informacji w formie pisemnej lub na stronie internetowej podmiotu za wystarczające.

Biorąc pod uwagę zakres zadań straży miejskiej, istotę, specyfikę oraz cel przetwarzania danych osobowych w związku z wykonywaniem połączeń alarmowych do straży, obowiązujące przepisy prawa dotyczące numerów alarmowych oraz powołane wyżej wytyczne Grupy Roboczej Art. 29, zasadnie można przyjąć, że do spełnienia obowiązku informacyjnego wystarczające jest udostępnienie stosownej klauzuli w Biuletynie Informacji Publicznej, na stronie internetowej straży miejskiej oraz w widocznym miejscu w jej siedzibie.

ODPOWIEDZIALNOŚĆ DYREKCJI SZKOŁY ZA DANE ZAWARTE W PIŚMIE Z SĄDU RODZINNEGO

Prezes UODO udzielił upomnienia szkole w miejscowości Z. za publiczne przypisanie rodzicom ucznia autorstwa anonimu napisanego do sądu rodzinnego przez kogoś ze wspólnoty szkolnej w sprawie tego, co dzieje się w jednej z klas.

Sąd rodzinny w Z. przekazał szkole anonimowe pismo opisujące problem placówki (dotyczyło agresywnych zachowań uczniów w klasie). Na zebraniu rodziców dyrektorka ogłosiła, kto jej zdaniem to pismo napisał. Przypisała jego autorstwo rodzicom, którzy doprowadzili do zwołania zebrania w sprawie zachowania dzieci w klasie. Ostrzegła, że informowanie o problemach uczniów doprowadzi do sądowej i policyjnej ingerencji w życie rodzin. Wskazani przez nią rodzice zaprotestowali. A potem poskarżyli się do UODO – podkreślili, że nie są autorami tego pisma. Mówili o tym zresztą na zebraniu. Zgłaszali też, że niezgodne z prawem jest ujawnianie treści pisma sądowego na forum klasy, skoro żaden z rodziców nie jest jego autorem ani nie zostało doręczone żadnej osobie wymienionej w jego treści.

Po zbadaniu sprawy UODO stwierdził, że dyrekcja szkoły po otrzymaniu pisma z sądu stała się administratorem danych osób wymienionych w tym piśmie. Jednak mogła te dane przetwarzać wyłącznie w celu, dla jakiego została zobowiązana przez sąd, a więc sporządzenia opinii na temat konkretnych dzieci. Powiadomienie rodziców o wpłynięciu anonimu do sądu oraz poinformowanie o treści i przypisywanie autorstwa stanowiło naruszenie przepisów o ochronie danych osobowych.

Okoliczności te potwierdzają, że przetwarzanie danych osobowych skarżących podczas zebrania, stanowiło naruszenie art. 6 ust. 1 w zw. z art. 5 ust. 1 lit. a i lit. b RODO.

Sygnatura sprawy: DS.523.2738.2023

PRAWA I OBOWIĄZKI KONTROLOWANEGO

Dowiadujesz się, że została zaplanowana u Ciebie kontrola Urzędu Ochrony Danych Osobowych. Zastanawiasz się, co robić? Przedstawimy Ci Twoje prawa i obowiązki jako podmiotu kontrolowanego, abyś wiedział, czego możesz się spodziewać i oczekiwać od nas – kontrolujących.

Czym jest kontrola ochrony danych osobowych

Kontrolę przestrzegania przepisów o ochronie danych osobowych przeprowadza Prezes Urzędu Ochrony Danych Osobowych. Kontrolę prowadzi się zgodnie z zatwierdzonym przez Prezesa Urzędu planem kontroli lub na podstawie uzyskanych przez Prezesa Urzędu informacji lub w ramach monitorowania przestrzegania stosowania rozporządzenia 2016/679.

W 2024 r. obowiązuje plan kontroli sektorowych, który zakłada kontrole:

• podmiotów, które przetwarzają dane osobowe przy użyciu aplikacji internetowych (webowych),

• kontrole prawidłowości spełniania obowiązku informacyjnego określonego w art. 13 i 14 RODO,

• organów przetwarzających dane osobowe w wielkoskalowych systemach informacyjnych UE do walki z przestępczością i ochrony granic, czyli w Systemie Informacyjnym Schengen i Wizowym Systemie Informacyjnym.

Kontrolę przeprowadza upoważniony przez Prezesa Urzędu pracownik Urzędu. Może zaistnieć sytuacja, w której do kontroli zostanie upoważniony członek lub pracownik organu nadzorczego państwa członkowskiego Unii Europejskiej. Prezes Urzędu może również upoważnić do udziału w kontroli osobę posiadającą wiedzę specjalistyczną, jeżeli przeprowadzenie czynności kontrolnych wymaga takiej wiedzy.

Czynności kontrolnych dokonuje się w obecności kontrolowanego lub osoby przez niego upoważnionej. Kontrolowany jest obowiązany do pisemnego wskazania osoby upoważnionej do reprezentowania go w trakcie kontroli. Kontrolujący ustala stan faktyczny na podstawie dowodów zebranych w postępowaniu kontrolnym, a w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń.

4 NARUSZENIA I KONTROLE

Obowiązki kontrolowanego

Kontrolowany ma obowiązek zapewnić kontrolującym warunki i środki niezbędne do sprawnego przeprowadzenia kontroli, a w szczególności sporządzić we własnym zakresie kopie lub wydruki dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub systemach informatycznych lub teleinformatycznych służących do przetwarzania danych. W tym celu należy zapewnić kontrolującym wstęp na grunt oraz do budynków, lokali lub innych pomieszczeń w godzinach od 600 do 2200. Prezes Urzędu lub kontrolujący może zwrócić się do właściwego miejscowo komendanta Policji o pomoc, jeżeli jest to niezbędne do wykonywania czynności kontrolnych.

Kontrolujący może przesłuchać pracownika kontrolowanego w charakterze świadka. Za pracownika kontrolowanego uznaje się osobę zatrudnioną na podstawie stosunku pracy lub wykonującą pracę na podstawie umowy cywilnoprawnej. Kontrolujący ustala stan faktyczny na podstawie dowodów zebranych w postępowaniu kontrolnym, a w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń.

Dlatego kontrolowany musi zapewnić wgląd do dokumentów i informacji mających bezpośredni związek z zakresem przedmiotowym kontroli, a także możliwość przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych. Na żądanie kontrolującego kontrolowany musi złożyć pisemne lub ustne wyjaśnienia oraz złożyć w charakterze świadka osoby zeznania w zakresie niezbędnym do ustalenia stanu faktycznego. W przypadku otrzymania od kontrolującego zlecenia, kontrolowany musi sporządzić ekspertyzę i opinię.

Należy zapewnić dostęp do informacji objętych tajemnicą prawnie chronioną, chyba że przepisy szczególne stanowią inaczej. Strona kontrolowana może zastrzec informacje, dokumenty lub ich części zawierające tajemnicę przedsiębiorstwa. W takim przypadku kontrolowany jest zobowiązany przedstawić również wersję dokumentu niezawierającą informacji objętych zastrzeżeniem. W przypadku nieprzedstawienia wersji dokumentu niezawierającej informacji objętych zastrzeżeniem, zastrzeżenie uważa się za nieskuteczne. Prezes Urzędu Ochrony Danych Osobowych może uchylić zastrzeżenie, w drodze decyzji, jeżeli uzna, że informacje, dokumenty lub ich części nie spełniają przesłanek do objęcia ich tajemnicą przedsiębiorstwa. W przypadku ustawowego obowiązku przekazania informacji lub dokumentów otrzymanych od przedsiębiorców innym krajowym lub zagranicznym organom lub instytucjom, informacje i dokumenty przekazuje się wraz z zastrzeżeniem i pod warunkiem jego przestrzegania. Kontrolujący są obowiązani do zachowania w tajemnicy informacji, o których dowiedzieli się w toku kontroli.

4 NARUSZENIA I KONTROLE

Kontrolujący mogą żądać od strony przedstawienia tłumaczenia na język polski sporządzonej w języku obcym dokumentacji przedłożonej przez stronę. Tłumaczenia dokumentacji strona jest obowiązana wykonać na własny koszt.

Kontrolowany dokonuje potwierdzenia za zgodność z oryginałem sporządzonych kopii lub wydruków dokumentów i informacji mających bezpośredni związek z zakresem przedmiotowym kontroli. W przypadku odmowy potwierdzenia za zgodność z oryginałem, kontrolujący czyni o tym wzmiankę w protokole kontroli.

Niezapewnienie dostępu niezbędne do sprawnego przeprowadzenia kontroli skutkuje naruszeniem art. 58 ust. 1 RODO i podlega administracyjnej karze pieniężnej do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa, a w przypadku jednostek sektora finansów publicznych, tj. organów władzy publicznej, w tym organów administracji rządowej, organów kontroli państwowej i ochrony prawa oraz sądów i trybunałów, Narodowego Banku Polskiego – w wysokości do 100 000 złotych, zaś państwowych i samorządowych instytucji kultury do 10 000 złotych.

Przebieg czynności kontrolnych kontrolujący przedstawia w protokole kontroli, który zawiera:

1) wskazanie nazwy albo imienia i nazwiska oraz adresu kontrolowanego;

2) imię i nazwisko osoby reprezentującej kontrolowanego oraz nazwę organu reprezentującego kontrolowanego;

3) imię i nazwisko, stanowisko służbowe, numer legitymacji służbowej oraz numer imiennego upoważnienia kontrolującego, a w przypadku członka lub pracownika organu nadzorczego państwa członkowskiego Unii Europejskiej, imię i nazwisko, numer dokumentu potwierdzającego tożsamość oraz numer imiennego upoważnienia;

4) datę rozpoczęcia i zakończenia czynności kontrolnych;

5) określenie zakresu przedmiotowego kontroli;

6) opis stanu faktycznego ustalonego w toku kontroli oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych;

7) wyszczególnienie załączników;

8) omówienie dokonanych w protokole kontroli poprawek, skreśleń i uzupełnień;

9) pouczenie kontrolowanego o prawie zgłaszania zastrzeżeń do protokołu kontroli oraz o prawie odmowy podpisania protokołu kontroli;

10) datę i miejsce podpisania protokołu kontroli przez kontrolującego i kontrolowanego.

Protokół kontroli podpisuje kontrolujący i przekazuje kontrolowanemu w celu podpisania. Kontrolowany w ciągu 7 dni od dnia przedstawienia protokołu kontroli podpisuje go albo składa pisemne zastrzeżenia do jego treści. W przypadku złożenia zastrzeżeń, kontrolujący dokonuje ich analizy i, w razie potrzeby, podejmuje dodatkowe czynności kontrolne, a w przypadku stwierdzenia zasadności zastrzeżeń, zmienia lub uzupełnia odpowiednią część protokołu kontroli w formie aneksu do protokołu kontroli.

W razie nieuwzględnienia zastrzeżeń w całości albo części, kontrolujący przekazuje kontrolowanemu informacje o tym wraz z uzasadnieniem. Brak doręczenia kontrolującemu podpisanego protokołu kontroli i niezgłoszenie zastrzeżeń do jego treści w terminie 7 dni uznaje się za odmowę podpisania protokołu kontroli. O odmowie podpisania protokołu kontroli kontrolujący czyni wzmiankę w tym protokole, zawierającą datę jej dokonania. W przypadku braku doręczenia protokołu kontrolujący dokonuje wzmianki po upływie 7 dni.

Przedsiębiorco – Pamiętaj, że kontrola podlega ograniczeniom

Kontrola nie wiąże się jednak wyłącznie z obowiązkami ze strony podmiotu kontrolowanego. Polskie prawo wymaga, aby wobec przedsiębiorcy były spełnione dodatkowe wymogi ze strony kontrolującego organu.

W szczególności organ kontroli musi zawiadomić przedsiębiorcę o zamiarze wszczęcia kontroli. Kontrolę można wszczynać nie wcześniej niż po upływie 7 dni i nie później niż przed upływem 30 dni od dnia doręczenia zawiadomienia o zamiarze wszczęcia kontroli. Jeżeli kontrola nie zostanie wszczęta w terminie 30 dni od dnia doręczenia zawiadomienia, wszczęcie kontroli wymaga ponownego zawiadomienia.

Przedsiębiorca nie może podlegać więcej niż jednej kontroli w tym samym czasie. Dlatego jeżeli działalność gospodarcza przedsiębiorcy jest już objęta kontrolą innego organu, organ kontroli odstąpi od podjęcia czynności kontrolnych oraz może ustalić z przedsiębiorcą inny termin przeprowadzenia kontroli. Ważne jest, aby przedsiębiorca prowadził i przechowywał w swojej siedzibie książkę kontroli oraz upoważnienia i protokoły kontroli.

4 NARUSZENIA I KONTROLE

Źródła prawne

1. Art. 58 ust. 1 lit. b Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. U. UE L. z 2016 r. poz. 119

2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Rozdział 9 Kontrola przestrzegania przepisów o ochronie danych osobowych, Dz. U. z 2019 r. poz. 1781

3. Ustawa z dnia 6 marca 2018 r. Prawo Przedsiębiorców, Rozdział 5 Ograniczenia kontroli działalności gospodarczej, Dz. U. z 2024 r. poz. 236

Fot. pixabay

SYSTEMY ROZPOZNAWANIA GŁOSU A ICH WPŁYW NA OCHRONĘ DANYCH I PRYWATNOŚĆ

Technologie rozpoznawania głosu przeszły długą drogę, ewoluując od prostych aplikacji rozpoznających pojedyncze słowa, po zaawansowane systemy zdolne do interpretacji złożonych fraz, różnych akcentów oraz tonów emocjonalnych. Ta dynamicznie rozwijająca się dziedzina technologii staje się integralną częścią naszego codziennego życia, umożliwiając bardziej naturalną i intuicyjną interakcję z urządzeniami elektronicznymi.

Dzięki postępom w dziedzinie uczenia maszynowego i sztucznej inteligencji, tego typu systemy osiągają niespotykany wcześniej poziom precyzji i wszechstronności, otwierając drzwi do szerokiego zakresu zastosowań – od asystentów głosowych, poprzez transkrypcje mowy, aż po zaawansowane systemy biometryczne.

Zdarza się, że termin "rozpoznawanie głosu" używany jest zamiennie z terminem "rozpoznawanie mowy", mają one jednak nieco inne znaczenie. Różnica ta może wydawać się subtelna, ale ma istotne implikacje dla zrozumienia tego, jak działają te technologie i jakie są ich zastosowania.

Rozpoznawanie głosu skupia się na identyfikacji osoby na podstawie unikalnych cech jej głosu, natomiast rozpoznawanie mowy skupia się na konwersji mowy na tekst i często obejmuje także zrozumienie języka naturalnego.

Obie technologie są ze sobą ściśle powiązane i często wykorzystywane wspólnie. Na przykład, system rozpoznawania mowy może najpierw zidentyfikować osobę mówiącą (rozpoznawanie głosu), a następnie przetłumaczyć jej wypowiedź na inny język (rozpoznawanie mowy).

Rozwój tych technologii jest wspierany przez postępy w dziedzinie sztucznej inteligencji, w szczególności uczenia maszynowego. Algorytmy te uczą się rozpoznawać wzorce na podstawie ogromnych ilości danych, co pozwala na ciągłe poprawianie ich precyzji i skuteczności.

Obecnie, zarówno systemy rozpoznawania głosu, jak i systemy rozpoznawania mowy są wykorzystywane w wielu dziedzinach.

5 NOWE TECHNOLOGIE

Zastosowania dotyczące rozpoznawania głosu:

- Asystenci głosowi, np. Siri, Alexa czy Google Assistant, które stały się powszechnym elementem naszego codziennego życia.
- Umożliwiają one użytkownikom wykonywanie różnych zadań – od zarządzania kalendarzem, przez sterowanie urządzeniami domowymi, aż po szukanie informacji w Internecie – wszystko to za pomocą prostych komend głosowych. Dzięki funkcji rozpoznawania głosu, asystent może dostosować swoje odpowiedzi i usługi do indywidualnych potrzeb i preferencji każdej osoby, co sprawia, że interakcja staje się bardziej spersonalizowana.
- Systemy bezpieczeństwa i monitoringu, w których głos jest wykorzystywany jako dane biometryczne do identyfikacji i weryfikacji tożsamości.
- Takie rozwiązania są stosowane m.in. w bankowości, przy kontroli dostępu do zabezpieczonych obszarów, a także w aplikacjach mobilnych.
- Narzędzia do analizy emocji w głosie, które stają się coraz bardziej popularne, zwłaszcza w obsłudze klienta i badaniach rynkowych.
- Systemy te potrafią wykrywać emocje, takie jak radość, smutek, gniew, co pozwala firmom lepiej rozumieć swoich klientów i dostosowywać swoje usługi.

Zastosowania dotyczące rozpoznawania mowy:

- Transkrypcja mowy na tekst, która jest niezwykle przydatna w wielu branżach, takich jak dziennikarstwo, medycyna, prawo, czy edukacja, gdzie transkrypcja wywiadów, wykładów lub rozmów jest codziennością.
- Transkrypcja mowy na mowę, czyli tłumaczenie mowy w czasie rzeczywistym, co znacząco ułatwia komunikację międzynarodową i może być wykorzystywane podczas konferencji, podróży czy na polu edukacji.

Rozwój technologii do rozpoznawania głosu sprawił, że istotnym zagadnieniem stała się ochrona danych osobowych. W tym miejscu należy podkreślić, że głos uznaje się za daną osobową, gdyż umożliwia identyfikację osoby, której dotyczy. Głos dostarcza słuchaczowi dodatkowych informacji, np. o płci mówiącego, lokalizacji czy nastroju, które można wykorzystać do identyfikacji danej osoby. Co więcej, najnowocześniejsza nauka o danych biometrycznych umożliwia identyfikację lub weryfikację osoby na podstawie unikalnych cech jej głosu. W związku z tym, że głos bardzo często odnosi się (samodzielnie lub w połączeniu z innymi informacjami) do możliwej do zidentyfikowania osoby fizycznej, stanowi on dane osobowe w rozumieniu art. 4 RODO.

5 NOWE TECHNOLOGIE

W wytycznych EROD 02/2021 w sprawie VVA czyli wirtualnych asystentów głosowych, zwrócono między innymi uwagę na to, że administratorzy danych świadczący usługi VVA i ich podmioty przetwarzające muszą brać pod uwagę zarówno ogólne rozporządzenie o ochronie danych (RODO), jak i dyrektywę o e-prywatności. W wytycznych określono najistotniejsze wyzwania związane z zapewnieniem zgodności i przedstawiono zalecenia dla odpowiednich zainteresowanych stron dotyczące sposobów radzenia sobie z nimi.

Wyzwania związane z ochroną danych osobowych i prywatnością

Wykorzystanie systemów rozpoznawania głosu wiąże się z kilkoma kluczowymi wyzwaniami dotyczącymi prywatności:

• **Zbieranie danych dźwiękowych**

Systemy rozpoznawania głosu często wymagają stałego nasłuchu, aby mogły reagować na komendy użytkowników. Taki ciągły nasłuch wiąże się z ryzykiem rejestrowania prywatnych rozmów bez zgody użytkowników. Przykłady takich sytuacji pojawiały się już w przeszłości, gdy urządzenia nagrywały dźwięk, mimo że użytkownicy nie wydali żadnej komendy.

• **Przechowywanie danych**

Nagrania głosowe są często przechowywane przez firmy świadczące usługi rozpoznawania głosu. Przechowywanie tych danych niesie ze sobą ryzyko ich niewłaściwego wykorzystania, na przykład do celów analitycznych, marketingowych lub w przypadku wycieku danych. Brak odpowiednich zabezpieczeń może prowadzić do poważnych naruszeń prywatności.

• **Analiza biometryczna**

Głos jest unikalny dla każdej osoby i może być wykorzystywany do identyfikacji tożsamości. Wykorzystanie takich danych wiąże się z ryzykiem ich nieuprawnionego dostępu lub użycia. Przykładowo, w przypadku ich wycieku, osoba trzecia mogłaby uzyskać dostęp do zabezpieczonych systemów lub dokonać podszywania się pod daną osobę.

• **Brak transparentności**

Użytkownicy systemów rozpoznawania głosu często nie są w pełni świadomi, jakie dane są zbierane, w jaki sposób są one przetwarzane i do jakich celów mogą być wykorzystywane. Brak jasnych i przejrzystych polityk prywatności oraz brak informacji o tym, co dzieje się z ich danymi, może prowadzić do naruszeń praw użytkowników.

RODO a systemy rozpoznawania głosu

RODO, wprowadza ścisłe regulacje dotyczące ochrony danych osobowych, do których zaliczany

jest również głos:

• Jak wspomniano wcześniej systemy rozpoznawania głosu mają dostęp do informacji o charakterze prywatnym, które mogą być chronione na mocy art. 9 RODO, takich jak dane biometryczne. Dlatego projektanci i twórcy takich systemów muszą dokładnie określić, w jakich przypadkach przetwarzanie wiąże się ze specjalnymi kategoriami danych.

• Zgodnie z RODO, przed zbieraniem danych osobowych konieczne jest uzyskanie wyraźnej zgody użytkownika. Użytkownicy muszą być w pełni informowani o celu zbierania danych i sposobie ich przetwarzania.

• Użytkownicy mają prawo wiedzieć, jakie dane są zbierane, w jakim celu i jak długo będą przechowywane.

• Użytkownicy mogą zażądać usunięcia swoich danych osobowych, co ma szczególne znaczenie w przypadku danych biometrycznych.

• Twórcy aplikacji i systemów rozpoznawania głosu powinni wdrożyć odpowiednie zabezpieczenia, które mogą znacząco zmniejszyć ryzyko naruszeń prywatności np.:

  o Szyfrowanie danych end-to-end

  o Lokalne przetwarzanie danych głosowych bez przesyłania ich do chmury

  o Techniki federated learning: pozwalające na trenowanie modeli bez konieczności centralizacji danych użytkowników

  o Differential privacy: metoda dodawania kontrolowanego szumu do danych, aby chronić prywatność jednostek przy zachowaniu użyteczności danych zbiorczych

  o Regularne audyty bezpieczeństwa

  o Implementacja zasady privacy by design w procesie tworzenia systemów rozpoznawania głosu

Technologia rozpoznawania głosu, mimo licznych korzyści, budzi istotne obawy związane z prywatnością użytkowników. Głos ludzki stanowi cenne źródło informacji o jednostce, a jego nieuprawnione wykorzystanie może prowadzić do poważnych naruszeń prywatności.

Choć przypadki nadużyć są szeroko dyskutowane, wciąż brakuje kompleksowych rozwiązań, które w pełni zabezpieczyłyby dane głosowe. Dlatego niezwykle ważne jest połączenie zaawansowanych technologii zabezpieczeń z odpowiednimi regulacjami prawnymi, aby zapewnić, że rozwój technologii rozpoznawania głosu będzie się odbywał z poszanowaniem fundamentalnych praw człowieka.

W JAKI SPOSÓB NALEŻY KONTROLOWAĆ I MONITOROWAĆ SWOJE POLITYKI I PROCEDURY DOTYCZĄCE PRYWATNOŚCI DANYCH W HANDLU ELEKTRONICZNYM

Firma zajmująca się handlem elektronicznym musi upewnić się, że zasady i procedury dotyczące prywatności danych są zgodne z przepisami, przejrzyste i skuteczne.

Prywatność danych to nie tylko obowiązek prawny, ale także odpowiedzialność społeczna i przewaga konkurencyjna. Jak audytować i monitorować polityki i procedury dotyczące prywatności danych w handlu elektronicznym? Oto kilka pomocnych wskazówek.

Ocena inwentaryzacji danych

Pierwszym krokiem jest określenie, jakiego rodzaju dane są gromadzone, przechowywane, przetwarzane i udostępniane stronom trzecim.

Należy zmapować przepływ danych i cykl życia danych oraz udokumentować cel, podstawę prawną i okres przechowywania każdej kategorii danych. Trzeba również dokonać przeglądu środków bezpieczeństwa danych i planu reagowania na naruszenie danych. Pomoże to zrozumieć zagrożenia i luki w zakresie prywatności danych oraz ustalić priorytety działań.

Aktualizacja informacji o ochronie danych

Drugim krokiem jest poinformowanie klientów, pracowników i partnerów o zasadach i procedurach dotyczących prywatności danych.

Należy zaktualizować informacje dotyczące prywatności danych, takie jak polityka prywatności, polityka dotycząca plików cookie i formularze zgody, aby odzwierciedlić bieżące praktyki w zakresie danych i zachować zgodność z obowiązującymi przepisami i regulacjami. Informacje o prywatności danych mają być jasne, zwięzłe i dostępne, a osoby, których dane dotyczą, muszą być informowane o swoich prawach i możliwościach wyboru.

Wdrożenie kontroli prywatności danych

Trzecim krokiem jest wdrożenie środków kontroli prywatności danych, które umożliwią przestrzeganie obowiązków w zakresie prywatności danych i poszanowanie preferencji osób,

których dane dotyczą.

Należy stosować środki techniczne i organizacyjne, takie jak szyfrowanie, anonimizacja, kontrola dostępu i minimalizacja danych, aby chronić dane przed nieuprawnionym lub niezgodnym z prawem wykorzystaniem. Koniecznością jest również ustanowienie zasad i procedur obsługi wniosków o dostęp do danych, wniosków o przeniesienie danych, wniosków o usunięcie danych i powiadomień o naruszeniu danych.

Przeszkolenie pracowników i interesariuszy

Czwartym krokiem jest przeszkolenie pracowników i interesariuszy w zakresie polityk i procedur dotyczących prywatności danych oraz ich ról i obowiązków.

W tym kontekście warto się skupić na podniesieniu świadomości i edukacji swoich pracowników, wykonawców, dostawców i podmioty stowarzyszone w zakresie znaczenia prywatności danych i najlepszych praktyk. Niezbędne jest także monitorowanie ich zgodności i wydajności oraz zapewnienie wsparcia i dostarczenie informacji zwrotnych.

Przegląd relacji z podmiotami zewnętrznymi

Piątym krokiem jest przegląd relacji z podmiotami zewnętrznymi i upewnienie się, że przestrzegają one standardów i oczekiwań w zakresie prywatności danych.

Należy przeprowadzić analizę due diligence i weryfikację podmiotów przetwarzających dane, administratorów danych i odbiorców danych oraz zweryfikować ich referencje i praktyki w zakresie prywatności danych. Kolejną czynnością jest podpisanie z nimi umowy o przetwarzaniu danych lub umowy o udostępnianiu danych oraz określenie zakresu, warunków i zabezpieczeń przekazywania danych.

Przeprowadzanie regularnych audytów i przeglądów

Szóstym krokiem jest przeprowadzanie regularnych audytów i przeglądów polityk i procedur dotyczących prywatności danych oraz mierzenie ich skuteczności i zgodności.

Należy korzystać z wewnętrznych lub zewnętrznych audytorów lub narzędzi do samooceny, aby ocenić swoje wyniki w zakresie prywatności danych i zidentyfikować wszelkie kwestie lub ulepszenia. Konieczne jest również aktualizowanie polityk i procedur zgodnie ze zmianami w firmie, klientami, technologią lub prawem.

Źródło: LinkedIn Data Privacy

DLACZEGO MUSIMY UREGULOWAĆ KORZYSTANIE ZE SZTUCZNEJ INTELIGENCJI?

Unijny akt w sprawie sztucznej inteligencji (akt w sprawie AI) jest pierwszym na świecie kompleksowym zbiorem przepisów dotyczących sztucznej inteligencji. Jego celem jest zaradzenie zagrożeniom dla zdrowia, bezpieczeństwa i praw podstawowych. Akt w formie rozporządzenia chroni również demokrację, praworządność i środowisko.

Upowszechnienie systemów sztucznej inteligencji niesie ze sobą duży potencjał: może zapewnić korzyści społeczne, wzrost gospodarczy oraz pobudzić innowacyjność i zwiększyć globalną konkurencyjność UE. W pewnych przypadkach szczególne cechy niektórych systemów AI mogą jednak stwarzać nowe zagrożenia dla bezpieczeństwa użytkowników (w tym również fizycznego) i praw podstawowych. Niektóre potężne modele sztucznej inteligencji, które są powszechnie stosowane, mogą nawet stwarzać ryzyko systemowe.

Prowadzi to do braku pewności prawa i potencjalnie wolniejszej absorpcji technologii AI przez organy publiczne, przedsiębiorstwa i obywateli ze względu na brak zaufania. Rozbieżne działania regulacyjne organów krajowych groziłyby rozdrobnieniem rynku wewnętrznego.

W odpowiedzi na te wyzwania konieczne było podjęcie działań legislacyjnych w celu zapewnienia dobrze funkcjonującego wewnętrznego rynku systemów AI, na którym odpowiednio uwzględnia się zarówno korzyści, jak i zagrożenia.

Do kogo ma zastosowanie akt w sprawie AI?

Ramy prawne będą miały zastosowanie zarówno do podmiotów publicznych, jak i prywatnych w Unii i poza nią, jeżeli tylko dany **system AI** jest wprowadzany do obrotu w Unii lub jego stosowanie ma wpływ na jej mieszkańców.

Obowiązki wynikające z przepisów mogą obejmować zarówno dostawców (np. podmiot opracowujący narzędzie do profilowania kandydatów w procesie rekrutacji), jak i podmioty stosujące AI (np. bank nabywający takie narzędzie profilujące). Istnieją pewne wyjątki, w których te przepisy nie mają zastosowania. Nie obejmują one działań w zakresie badań, rozwoju i tworzenia prototypów, które poprzedzają wprowadzenie systemu AI do obrotu. Nie stosuje się ich również

w odniesieniu do systemów AI, które służą wyłącznie celom wojskowym, obronnym lub bezpieczeństwa narodowego, niezależnie od rodzaju podmiotu prowadzącego taką działalność.

Jakie są kategorie ryzyka?

Akt w sprawie AI wprowadza we wszystkich państwach członkowskich jednolite ramy prawne. Ich podstawą jest definicja AI, która uwzględnia dalszy rozwój technologii, i podejście oparte na analizie ryzyka:

o **Niedopuszczalne ryzyko:** kategoria ta obejmuje bardzo ograniczony zbiór szczególnie szkodliwych zastosowań sztucznej inteligencji, które są sprzeczne z wartościami UE, ponieważ naruszają prawa podstawowe i które w związku z tym będą zakazane:

- **wykorzystywanie słabości osób, stosowanie manipulacji i technik podprogowych;**
- **scoring obywateli** do celów publicznych i prywatnych;
- **indywidualne prognozowanie przestępczości** oparte wyłącznie na profilowaniu osób;
- **przeszukiwanie internetu** lub transmisji CCTV w celu pozyskania wizerunków twarzy na potrzeby tworzenia lub rozbudowy baz danych;
- **rozpoznawanie emocji w miejscu pracy i w placówkach edukacyjnych**, chyba że ze względów medycznych lub bezpieczeństwa (np. monitorowanie poziomu zmęczenia pilota);
- **kategoryzacja biometryczna** osób w celu ustalania ich rasy, poglądów politycznych, przynależności do związków zawodowych, przekonań religijnych lub filozoficznych lub orientacji seksualnej. Nadal możliwe będzie oznaczanie lub filtrowanie zbiorów danych i kategoryzacja danych w obszarze ścigania przestępstw;
- **zdalna identyfikacja biometryczna prowadzona w czasie rzeczywistym przez organy ścigania w przestrzeni publicznej**, z zastrzeżeniem wąsko określonych wyjątków (zob. poniżej).

o Komisja opublikuje wytyczne dotyczące zakazanych zastosowań AI, zanim związane z nimi przepisy wejdą w życie 2 lutego 2025 r.

o **Wysokie ryzyko:** we wniosku ustawodawczym za obarczone wysokim ryzykiem uznano ograniczoną liczbę systemów AI, które mogą mieć negatywny wpływ na bezpieczeństwo ludzi lub ich prawa podstawowe (chronione na mocy Karty praw podstawowych Unii Europejskiej). Do aktu załączono wykazy systemów AI wysokiego ryzyka, który może być poddawany przeglądowi, aby dostosować go w świetle ewolucji zastosowań AI.

o Dotyczy to również związanych z bezpieczeństwem elementów produktów objętych prawodawstwem sektorowym Unii. Będą one zawsze traktowane jako obarczone wysokim

ryzykiem, w przypadku gdy podlegają ocenie zgodności przeprowadzanej na podstawie tych przepisów sektorowych przez stronę trzecią.

o Takie systemy AI wysokiego ryzyka obejmują na przykład systemy AI oceniające, czy dana osoba kwalifikuje się do określonego leczenia, określonej pracy lub pożyczki na zakup mieszkania. Innym przykładem mogą być programy wykorzystywane przez policję do profilowania osób lub oceny ryzyka popełnienia przez nich przestępstwa (z wyjątkiem przypadków, w których jest to zakazane na mocy art. 5). Mogą to być także systemy AI sterujące robotami, dronami czy urządzeniami medycznymi.

o **Szczególne ryzyko w zakresie przejrzystości:** aby zwiększyć zaufanie do AI, należy korzystać z niej w przejrzysty sposób. Dlatego akt w sprawie AI wprowadza konkretne wymogi w zakresie przejrzystości w odniesieniu do niektórych zastosowań AI, na przykład gdy wiążą się one z ryzykiem manipulacji (np. w wyniku wykorzystania chatbotów) lub deepfake'ów. Użytkownicy powinni mieć świadomość, że wchodzą w interakcję z maszyną.

o Minimalne ryzyko: większość systemów AI można opracowywać i wykorzystywać z zastrzeżeniem obowiązujących przepisów bez konieczności stosowania się do dodatkowych obowiązków. Dostawcy tych systemów mogą dobrowolnie zdecydować się na stosowanie wymogów dotyczących wiarygodnej sztucznej inteligencji i zobowiązać się do przestrzegania dobrowolnych kodeksów postępowania.

W akcie w sprawie AI uwzględniono **ryzyko systemowe**, które może wynikać z **modeli AI ogólnego przeznaczenia**, w tym dużych **modeli generatywnej AI**. Mogą one być wykorzystywane do różnych zadań i stać się podstawą wielu systemów sztucznej inteligencji w UE. Niektóre z tych modeli mogą stwarzać ryzyko systemowe, jeżeli są bardzo zaawansowane lub szeroko stosowane. Na przykład potężne modele mogą powodować poważne wypadki lub być wykorzystywane do cyberataków na dużą skalę niezgodnie z ich przeznaczeniem. Wiele osób mogłoby ucierpieć, gdyby model rozpowszechniał szkodliwe uprzedzenia w wielu systemach o różnych zastosowaniach.

Skąd wiadomo, czy system sztucznej inteligencji jest obarczony wysokim ryzykiem?

Akt w sprawie AI przewiduje skuteczne metody klasyfikacji systemów AI jako systemów wysokiego ryzyka. Ma to na celu zapewnienie pewności prawa przedsiębiorstwom i innym podmiotom.

Klasyfikacja ryzyka opiera się na zamierzonym przeznaczeniu systemu AI, zgodnie z obowiązującymi przepisami UE dotyczącymi bezpieczeństwa produktów. Oznacza to, że klasyfikacja zależy od funkcji pełnionej przez system AI oraz od konkretnego celu i konkretnych zastosowań danego systemu.

System AI można sklasyfikować jako obarczony wysokim ryzykiem w dwóch przypadkach:

• jeżeli jest on elementem bezpieczeństwa wbudowanym w produkt objęty obowiązującymi przepisami dotyczącymi produktów (załącznik I) lub sam jest takim produktem. Może to być na przykład oprogramowanie medyczne oparte na sztucznej inteligencji;

• jeżeli wykorzystuje się go w konkretnych przypadkach zastosowania obarczonych wysokim ryzykiem wymienionych w załączniku III do aktu w sprawie AI. Wykaz ten obejmuje przypadki zastosowania w dziedzinach takich jak edukacja, zatrudnienie, egzekwowanie prawa lub migracja.

Komisja przygotowuje wytyczne dotyczące klasyfikacji systemów AI jako systemy wysokiego ryzyka, które opublikuje przed datą rozpoczęcia stosowania tych przepisów.

Jakie są przykłady przypadków zastosowania systemów wysokiego ryzyka określonych w załączniku III?

Załącznik III obejmuje osiem obszarów, w których wykorzystanie AI może być szczególnie ryzykowne, i zawiera wykaz konkretnych przypadków zastosowania dla każdego obszaru. System AI klasyfikuje się jako obarczony wysokim ryzykiem, jeżeli jest przeznaczony do wykorzystania w jednym z poniższych przypadków zastosowania.

Przykłady:

o systemy AI wykorzystywane jako elementy bezpieczeństwa w niektórych **infrastrukturach krytycznych**, np. w dziedzinie ruchu drogowego oraz w zaopatrzeniu w wodę, gaz, ogrzewanie i energię elektryczną;

o systemy AI wykorzystywane w **edukacji i szkoleniu zawodowym**, np. w celu oceny efektów uczenia się, kierowania procesem uczenia się i monitorowania nieuczciwego zachowania w trakcie testów;

o systemy AI wykorzystywane w **zatrudnieniu, zarządzaniu pracownikami** i dostępie do samozatrudnienia, np. zamieszczanie ukierunkowanych ogłoszeń o pracę, analizowanie i filtrowanie podań o pracę oraz ocena kandydatów;

o **systemy AI wykorzystywane w dostępie do podstawowych usług i świadczeń prywatnych i publicznych** (np. opieka zdrowotna), **ocenie zdolności kredytowej** osób fizycznych oraz ocenie i wycenie ryzyka w odniesieniu do **ubezpieczenia na życie i ubezpieczenia zdrowotnego**;

o systemy AI wykorzystywane w dziedzinach **egzekwowania prawa**, migracji i **kontroli granicznej** – o ile nie są zakazane z innego tytułu – jak i w dziedzinie sprawowania **wymiaru sprawiedliwości** i w **procesach demokratycznych**;

o systemy AI wykorzystywane do **identyfikacji biometrycznej, kategoryzacji biometrycznej i rozpoznawania emocji** – o ile nie są zakazane.

Jakie obowiązki spoczywają na dostawcach systemów AI wysokiego ryzyka?

Przed **wprowadzeniem do obrotu w UE systemu AI wysokiego ryzyka** lub wprowadzeniem go do użytku w inny sposób dostawcy muszą poddać go **ocenie zgodności.** Na tej podstawie będą w stanie wykazać, że ich system spełnia obowiązkowe wymogi dotyczące wiarygodnej sztucznej inteligencji (np. jakość danych, dokumentacja i identyfikowalność, przejrzystość, nadzór ze strony człowieka, dokładność, cyberbezpieczeństwo i solidność). Ocenę tę należy powtórzyć, jeżeli system lub jego przeznaczenie ulegną istotnej zmianie.

Systemy AI, które stanowią związane z bezpieczeństwem elementy produktów objętych przepisami sektorowymi Unii, zawsze będą traktowane jako obarczone wysokim ryzykiem, jeżeli na podstawie tych przepisów sektorowych podlegają ocenie zgodności przeprowadzanej przez stronę trzecią. Ocenie zgodności przeprowadzanej przez stronę trzecią będą przy tym podlegały wszystkie systemy biometryczne bez względu na ich zastosowanie.

Dostawcy systemów AI wysokiego ryzyka będą również musieli **wdrożyć systemy zarządzania jakością i ryzykiem**, aby zapewnić zgodność z nowymi wymogami i zminimalizować ryzyko dla użytkowników i osób, na które systemy te wywierają wpływ, nawet po wprowadzeniu produktu do obrotu.

Systemy sztucznej inteligencji wysokiego ryzyka stosowane przez organy publiczne lub podmioty działające w ich imieniu będą musiały zostać **zarejestrowane w publicznej unijnej bazie danych**, chyba że systemy te są wykorzystywane w obszarach egzekwowania prawa i migracji. Te ostatnie systemy będą musiały zostać zarejestrowane w niepublicznej części bazy danych, która będzie dostępna wyłącznie dla właściwych organów nadzorczych.

Aby zapewnić zgodność w całym cyklu życia systemu AI, organy nadzoru rynku będą przeprowadzać regularne kontrole, wspomagać monitorowanie systemów po ich wprowadzeniu do obrotu oraz umożliwią dostawcom dobrowolne zgłaszanie wszelkich znanych im poważnych incydentów lub naruszeń obowiązków w zakresie praw podstawowych. W wyjątkowych przypadkach organy mogą przyznać wyłączenia w odniesieniu do konkretnych systemów AI wysokiego ryzyka, które mają być wprowadzane do obrotu.

W przypadku wystąpienia naruszenia, dzięki wprowadzonym wymogom organy krajowe uzyskają dostęp do informacji niezbędnych do zbadania, czy system AI stosowano zgodnie z prawem.

6 SPRAWY MIĘDZYNARODOWE

Czemu ma służyć normalizacja przewidziana w akcie w sprawie AI?

Zgodnie z aktem systemy AI wysokiego ryzyka będą podlegać wymogom szczególnym. Europejskie normy zharmonizowane będą odgrywać kluczową rolę we wdrażaniu tych wymogów.

W maju 2023 r. Komisja Europejska upoważniła europejskie organizacje normalizacyjne CEN i CENELEC do opracowania norm dotyczących wymogów w odniesieniu do wysokiego ryzyka. Powierzony tym organizacjom mandat zostanie teraz zmieniony, aby dostosować go do ostatecznego tekstu aktu w sprawie AI.

Europejskie organizacje normalizacyjne będą miały czas do końca kwietnia 2025 r. na opracowanie i opublikowanie norm. Następnie Komisja oceni te normy i podejmie decyzję w sprawie ich zatwierdzenia. Przyjęte normy zostaną opublikowane w Dzienniku Urzędowym UE. Po publikacji systemy AI, które opracowano zgodnie z tymi normami, będą uznawane za domyślnie zgodne.

W jaki sposób reguluje się modele sztucznej inteligencji ogólnego przeznaczenia?

Modele sztucznej inteligencji ogólnego przeznaczenia, w tym **duże modele generatywnej AI,** mogą być wykorzystywane do różnych zadań. Poszczególne modele mogą być stosowane w dużej liczbie systemów sztucznej inteligencji.

Ważne jest, aby dostawca systemu AI, który wykorzystuje model sztucznej inteligencji ogólnego przeznaczenia, posiadał dostęp do wszystkich niezbędnych informacji, aby upewnić się, że jego system jest bezpieczny i zgodny z aktem w sprawie AI.

W związku z tym, akt w sprawie AI zobowiązuje dostawców takich modeli do **ujawniania określonych informacji dostawcom, którzy wykorzystują takie modele w swoich systemach.** Taka **przejrzystość** umożliwia lepsze zrozumienie tych modeli.

Dostawcy modeli muszą ponadto stosować zasady zapewniające **przestrzeganie prawa autorskiego** przy trenowaniu swoich modeli.

Niektóre z tych modeli mogą wiązać się z **ryzykiem systemowym**, ponieważ są bardzo zaawansowane lub szeroko stosowane.

Obecnie uznaje się, że modele AI ogólnego przeznaczenia, które zostały wytrenowane przy użyciu **całkowitej mocy obliczeniowej powyżej 10^25 FLOPS**, wiążą się z ryzykiem systemowym. Komisja może zaktualizować lub uzupełnić ten próg w świetle postępu technologicznego. Może też w oparciu o dalsze kryteria (np. liczbę użytkowników lub stopień autonomii modelu) wskazać inne modele jako stwarzające ryzyko systemowe.

Dostawcy modeli stwarzających ryzyko systemowe są zobowiązani do **oceny i ograniczania ryzyka, zgłaszania poważnych incydentów, przeprowadzania najnowocześniejszych testów i ocen modeli**

i zapewniania **cyberbezpieczeństwa.**

Dostawców zachęca się do współpracy z Urzędem ds. Sztucznej Inteligencji (Urząd ds. AI) i innymi zainteresowanymi stronami, aby opracować kodeks postępowania określający szczegółowe zasady, które pozwolą na bezpieczny i odpowiedzialny rozwój ich modeli. Taki kodeks powinien być głównym narzędziem wykorzystywanym przez dostawców modeli AI ogólnego przeznaczenia do wykazywania zgodności.

Dlaczego 10^25 FLOPS stanowi odpowiedni próg dla modeli sztucznej inteligencji ogólnego przeznaczenia obarczonych ryzykiem systemowym?

FLOPS jest wskaźnikiem, który odzwierciedla możliwości modelu, a dokładny próg FLOPS może zostać zaktualizowany w górę lub w dół przez Komisję, np. w świetle postępu w obiektywnym pomiarze możliwości modelu i zmian mocy obliczeniowej niezbędnej do uzyskania danego poziomu wydajności.

Nie mamy jeszcze wystarczającego zrozumienia możliwości modeli powyżej tego progu. Mogą one stwarzać ryzyko systemowe, w związku z czym uzasadnione jest nałożenie na ich dostawców dodatkowych obowiązków.

Jakie obowiązki akt w sprawie AI nakłada w zakresie oznakowania wyników działania sztucznej inteligencji?

Akt określa przepisy dotyczące przejrzystości w odniesieniu do treści tworzonych przez generatywną AI, aby przeciwdziałać manipulacji, oszustwom i wprowadzaniu w błąd.

Zobowiązuje on dostawców systemów generatywnej AI do opatrywania wyników działania AI oznaczeniem w formacie nadającym się do odczytu maszynowego i zadbania o możliwość identyfikacji tych wyników jako sztucznie wygenerowane lub zmanipulowane. Stosowane rozwiązania techniczne muszą być skuteczne, interoperacyjne, solidne i niezawodne w zakresie, w jakim jest to technicznie wykonalne, a przy tym muszą uwzględniać specyfikę i ograniczenia różnych rodzajów treści, koszty wdrażania oraz powszechnie uznany stan wiedzy technicznej, co może być odzwierciedlone w odpowiednich normach technicznych.

Podmioty stosujące systemy generatywnej AI, które generują obrazy, treści dźwiękowe lub treści wideo oraz nimi manipulują, co sprawia, że można je niesłusznie uznać za autentyczne lub prawdziwe („deepfake”), muszą w widoczny sposób ujawnić, że treści te zostały sztucznie wygenerowane lub zmanipulowane. Podmioty stosujące system AI, który generuje tekst publikowany w celu informowania społeczeństwa o sprawach leżących w interesie publicznym lub manipuluje takim tekstem, muszą również ujawnić, że tekst został sztucznie wygenerowany

lub zmanipulowany. Obowiązek ten nie ma zastosowania w przypadku, gdy treści wygenerowane przez AI poddano weryfikacji przez człowieka lub kontroli redakcyjnej oraz gdy odpowiedzialność redakcyjną za publikację treści ponosi osoba fizyczna lub prawna.

Urząd ds. AI wyda szczegółowe wytyczne dla dostawców i podmiotów stosujących AI dotyczące obowiązków określonych w art. 50, które zaczną mieć zastosowanie dwa lata po wejściu w życie aktu w sprawie AI (2 sierpnia 2026 r.).

Urząd będzie też zachęcał do opracowywania ogólnounijnych kodeksów postępowania i wspierał takie inicjatywy, aby ułatwić skuteczne wykonywanie obowiązków w zakresie wykrywania i oznaczania treści sztucznie wygenerowanych lub zmanipulowanych.

Czy akt w sprawie AI jest dostosowany do przyszłych wyzwań?

Akt w sprawie AI ustanawia ramy prawne, które opracowano z myślą o nowych zmianach, ich łatwym i szybkim dostosowywaniu oraz częstej ocenie.

W akcie określono ukierunkowane na wyniki wymogi i obowiązki, ale konkretne rozwiązania techniczne i operacyjne pozostawiono dla branżowych norm i kodeksów postępowania, które są elastyczne i mogą być dostosowywane do różnych przypadków zastosowania oraz które umożliwią wprowadzenie nowych rozwiązań technologicznych.

Same przepisy można zmienić w drodze aktów delegowanych i wykonawczych, na przykład w celu aktualizacji wykazu przypadków zastosowania wysokiego ryzyka w załączniku III.

Planowane są też częste oceny niektórych części aktu w sprawie AI, a ostatecznie i ocena całego rozporządzenia, aby zidentyfikować elementy wymagające aktualizacji czy zmiany.

W jaki sposób akt w sprawie AI reguluje identyfikację biometryczną?

Stosowanie **zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej** (tj. rozpoznawanie twarzy za pomocą CCTV) do celów ścigania przestępstw jest zabronione. Państwa członkowskie mogą wprowadzić przepisy określające wyjątki, które umożliwiłyby stosowanie zdalnej identyfikacji biometrycznej w czasie rzeczywistym w następujących przypadkach:

o działania organów ścigania związane z 16 określonymi bardzo poważnymi przestępstwami;

o ukierunkowane poszukiwanie konkretnych ofiar, uprowadzenia, handel ludźmi i wykorzystywanie seksualne ludzi oraz osoby zaginione; lub

o zapobieganie zagrożeniu życia lub bezpieczeństwa fizycznego osób lub reagowanie na obecne lub przewidywalne zagrożenie atakiem terrorystycznym.

Każdy wyjątkowy przypadek zastosowania wymaga **uprzedniej zgody organu sądowego**

lub niezależnego organu administracyjnego, którego decyzja jest wiążąca. W pilnych przypadkach zgoda może zostać wydana w ciągu 24 godzin. Jeżeli zgoda nie zostanie wydana, należy usunąć wszystkie dane i wyniki.

Takie zastosowanie musi być poprzedzone **wcześniejszą oceną skutków w zakresie praw podstawowych** i **zgłoszone właściwemu organowi nadzoru rynku i organowi ochrony danych**. W pilnych przypadkach korzystanie z systemu można rozpocząć bez rejestracji.

Wykorzystanie systemów AI **do zdalnej identyfikacji biometrycznej post factum** (identyfikacja osób w uprzednio zebranych materiałach wideo) osób objętych dochodzeniem wymaga **uprzedniego zezwolenia** organu sądowego lub niezależnego organu administracyjnego oraz powiadomienia odpowiedniego organu ochrony danych i organu nadzoru rynku.

Dlaczego potrzebne są szczegółowe przepisy dotyczące zdalnej identyfikacji biometrycznej?

Identyfikacja biometryczna może przybierać różne formy. Uwierzytelnianie biometryczne i weryfikacja biometryczna wykorzystywane np. do odblokowania smartfona lub na przejściach granicznych do weryfikacji tożsamości danej osoby na podstawie jej dokumentów podróży (porównanie „jeden do jednego") nie są przedmiotem regulacji, ponieważ nie stanowią one istotnego zagrożenia dla praw podstawowych.

Z kolei identyfikacja biometryczna może być wykorzystywana również zdalnie, na przykład do identyfikacji osób w tłumie, co może mieć znaczący wpływ na prywatność w przestrzeni publicznej.

Dokładność systemów rozpoznawania twarzy może znacznie różnić się w zależności od szeregu czynników, takich jak jakość kamer, oświetlenie, odległość, aktualność bazy danych, algorytm oraz pochodzenie etniczne, wiek lub płeć danej osoby. To samo dotyczy systemów rozpoznawania sposobu chodzenia i systemów rozpoznawania mowy oraz innych systemów biometrycznych. W wysoko zaawansowanych systemach stale zmniejsza się wskaźnik błędnego dopasowania.

Chociaż dokładność na poziomie 99 proc. może zasadniczo wydawać się wysoka, to nawet niewielkie ryzyko pomyłki jest problematyczne, gdy może skutkować podejrzeniem niewinnej osoby. Nawet poziom błędu wynoszący 0,1 proc. może mieć poważne konsekwencje w przypadku dużych populacji, na przykład na stacjach kolejowych.

W jaki sposób przedmiotowe przepisy chronią prawa podstawowe?

Na szczeblu UE i państw członkowskich istnieje już wysoki poziom ochrony praw podstawowych i niedyskryminacji, jednak złożoność i nieprzejrzystość niektórych zastosowań AI (tzw. czarne skrzynki) może rodzić problemy.

6 SPRAWY MIĘDZYNARODOWE

Podejście do sztucznej inteligencji ukierunkowane na człowieka oznacza zapewnienie zgodności zastosowań AI z prawodawstwem dotyczącym praw podstawowych. Dzięki wprowadzeniu wymogów w zakresie rozliczalności i przejrzystości, którym podlegać będzie opracowywanie systemów AI wysokiego ryzyka, oraz skuteczniejszemu egzekwowaniu obowiązujących przepisów kwestia zgodności z prawem będzie uwzględniana od samego początku projektowania tych systemów. W przypadku wystąpienia naruszeń, dzięki wprowadzonym wymogom, organy krajowe uzyskają dostęp do informacji niezbędnych do zbadania, czy stosowanie AI jest zgodne z prawem Unii.

Akt w sprawie AI wymaga od niektórych podmiotów stosujących systemy AI wysokiego ryzyka, aby przeprowadzały one ocenę skutków w zakresie praw podstawowych.

Czym jest ocena skutków w zakresie praw podstawowych? Kto musi przeprowadzić taką ocenę i kiedy?

Dostawcy systemów AI wysokiego ryzyka muszą przeprowadzić ocenę ryzyka i zaprojektować system, który stwarza jak najmniejsze ryzyko dla zdrowia, bezpieczeństwa i praw podstawowych.

Niektóre zagrożenia dla praw podstawowych można jednak w pełni zidentyfikować, dopiero gdy zna się kontekst, w którym dany system AI wysokiego ryzyka jest wykorzystywany. Jeżeli systemy AI wysokiego ryzyka są stosowane w szczególnie wrażliwych obszarach, w których może wystąpić brak równowagi sił, należy rozważyć takie ryzyko ze szczególną uwagą.

W związku z tym, podmioty stosujące AI, będące podmiotami prawa publicznego lub podmiotami prywatnymi świadczącymi usługi publiczne, oraz operatorzy udostępniający systemy AI wysokiego ryzyka, dokonujący oceny zdolności kredytowej lub oceny i wyceny ryzyka w odniesieniu do ubezpieczenia na życie i ubezpieczenia zdrowotnego, mają obowiązek przeprowadzania oceny skutków w zakresie praw podstawowych i powiadamiania organu krajowego o jej wynikach.

W praktyce wiele podmiotów stosujących AI będzie musiało również przeprowadzić ocenę skutków dla ochrony danych. Aby uniknąć ścisłego pokrywania się oceny skutków w zakresie praw podstawowych i oceny skutków dla ochrony danych, należy w takich przypadkach przeprowadzać je wspólnie.

W jaki sposób w rozporządzeniu uwzględniono kwestię tendencyjności AI pod względem rasy i płci?

Należy wyraźnie zaznaczyć, że **systemy AI nie są źródłem tendencyjności ani jej nie powielają**. **O ile są one prawidłowo zaprojektowane i stosowane, mogą przyczynić się do ograniczenia tendencyjności i istniejącej dyskryminacji strukturalnej,** a tym samym prowadzić do bardziej

sprawiedliwych i niedyskryminacyjnych decyzji (np. przy rekrutacji).

Nowe obowiązkowe wymogi dotyczące wszystkich systemów AI wysokiego ryzyka będą służyć temu celowi. Systemy AI muszą być **solidne pod względem technicznym**, tak aby były odpowiednie do stawianych celów i nie generowały tendencyjnych wyników, takich jak wyniki fałszywie dodatnie/ujemne, które wpływają w nieproporcjonalny sposób na grupy zmarginalizowane, w tym grupy pomijane ze względu na pochodzenie rasowe lub etniczne, płeć, wiek i inne cechy chronione.

Systemy wysokiego ryzyka będą również musiały być **trenowane i testowane przy użyciu wystarczająco reprezentatywnych zbiorów danych, aby zminimalizować ryzyko niesprawiedliwej tendencyjności zaszytej w modelu** oraz zapewnić eliminowanie tej tendencyjności za pomocą odpowiednich mechanizmów służących jej wykrywaniu i korygowaniu oraz innych środków łagodzących.

Musi również istnieć możliwość **identyfikacji i kontroli** tych systemów, co wiąże się z koniecznością **prowadzenia odpowiedniej dokumentacji**, obejmującej m.in. dane wykorzystane do trenowania algorytmu, które będą miały kluczowe znaczenie dla późniejszych analiz w przypadku ewentualnych nieprawidłowości.

Mechanizm służący zapewnieniu zgodności systemów AI z przepisami przed ich wprowadzeniem do obrotu, jak i po ich wprowadzeniu do obrotu będzie wymuszał regularne monitorowanie tych systemów i szybkie eliminowanie potencjalnych zagrożeń.

Od kiedy akt w sprawie AI będzie w pełni stosowany?

Akt w sprawie AI zacznie obowiązywać od 2 sierpnia 2026 r., czyli dwa lata po wejściu w życie, z wyjątkiem następujących przepisów szczegółowych:

- zakazy, definicje i przepisy dotyczące kompetencji w zakresie sztucznej inteligencji zaczną obowiązywać od 2 lutego 2025 r., czyli 6 miesięcy po wejściu w życie aktu;
- przepisy w zakresie zarządzania i obowiązki dotyczące AI ogólnego przeznaczenia zaczną obowiązywać 2 sierpnia 2025 r., czyli 12 miesięcy po wejściu w życie aktu;
- obowiązki dotyczące systemów AI, które sklasyfikowano jako systemy wysokiego ryzyka, ponieważ są wbudowane w produkty regulowane wymienione w załączniku II (wykaz unijnego prawodawstwa harmonizacyjnego), zaczną obowiązywać 2 sierpnia 2027 r., czyli 36 miesięcy po wejściu w życie aktu.

W jaki sposób akt w sprawie AI będzie egzekwowany?

W akcie w sprawie AI ustanowiono dwupoziomowy system zarządzania, w którym za nadzorowanie systemów AI i egzekwowanie dotyczących ich przepisów odpowiadają **organy krajowe**, podczas gdy

zarządzanie modelami AI ogólnego przeznaczenia leży w gestii organów unijnych.

Aby zapewnić spójność i współpracę w całej UE, powołana zostanie **Europejska Rada ds. Sztucznej Inteligencji** (Rada ds. AI), złożona z przedstawicieli państw członkowskich, z wyspecjalizowanymi podgrupami skupiającymi przedstawicieli krajowych organów regulacyjnych i innych właściwych organów.

Urząd ds. AI, będący organem wykonawczym Komisji do celów aktu w sprawie AI, będzie zapewniać Radzie ds. AI strategiczne wytyczne.

Akt w sprawie AI powołał też do życia dwa organy doradcze, które dostarczą wsparcie ekspertów – **panel naukowy i forum doradcze.** Organy te będą źródłem cennej wiedzy pochodzącej od zainteresowanych stron i interdyscyplinarnych środowisk naukowych, która będzie brana pod uwagę przy podejmowaniu decyzji i która umożliwi zrównoważone podejście do rozwoju AI.

Dlaczego potrzebna jest Europejska Rada ds. Sztucznej Inteligencji i czym będzie się ona zajmować?

W skład Europejskiej Rady ds. Sztucznej Inteligencji wchodzą **przedstawiciele wysokiego szczebla z państw członkowskich** i Europejski Inspektor Ochrony Danych (EIOD). Jako główny organ doradczy Rada ds. AI publikuje wytyczne dotyczące wszystkich kwestii związanych z polityką w zakresie AI, w szczególności przepisów, polityki w zakresie innowacji i doskonałości oraz współpracy międzynarodowej.

Rada ds. AI ma za zadanie ułatwić sprawne, skuteczne i zharmonizowane wdrażanie aktu w sprawie AI. Będzie ona też pełnić rolę forum, na którym organy regulacyjne ds. sztucznej inteligencji, a mianowicie Urząd ds. AI, organy krajowe i EIOD, będą mogły zadbać o spójne stosowanie aktu w sprawie AI.

Jakie kary przewidziano za naruszenie przepisów?

Państwa członkowskie będą musiały ustanowić skuteczne, proporcjonalne i odstraszające kary za naruszenie przepisów dotyczących systemów sztucznej inteligencji.

W rozporządzeniu określono maksymalne wysokości kar, które należy uwzględnić:

- **do 35 mln euro lub 7 proc.** całkowitego rocznego światowego obrotu w poprzednim roku obrotowym (w zależności od tego, która wartość jest wyższa) w przypadku naruszeń polegających **na stosowaniu zakazanych praktyk lub w przypadku nieprzestrzegania wymogów dotyczących przetwarzania danych;**
- **do 15 mln euro lub 3 proc.** całkowitego rocznego światowego obrotu w poprzednim roku obrotowym w przypadku **nieprzestrzegania któregokolwiek z pozostałych wymogów**

lub obowiązków określonych w rozporządzeniu;

- **do 7,5 mln euro lub 1,5 proc.** całkowitego rocznego światowego obrotu w poprzednim roku obrotowym za **przekazywanie jednostkom notyfikowanym i właściwym organom krajowym nieprawidłowych, niepełnych lub wprowadzających w błąd informacji** w odpowiedzi na zapytanie;
- w każdej kategorii naruszeń próg w przypadku MŚP stanowiłaby niższa z dwóch wspomnianych kwot, natomiast w przypadku innych przedsiębiorstw – wyższa.

Komisja może również egzekwować przepisy dotyczące dostawców modeli AI ogólnego przeznaczenia za pomocą kar pieniężnych, biorąc pod uwagę następujący próg:

- **do 15 mln euro lub 3 proc.** całkowitego rocznego światowego obrotu w poprzednim roku obrotowym w przypadku **niezastosowania się do któregokolwiek z obowiązków** lub środków wymaganych przez Komisję na mocy rozporządzenia.

Jako że instytucje, agencje i organy UE powinny dawać przykład, będą one także podlegać tym przepisom i ewentualnym karom. Do nakładania na nie kar finansowych za niezgodność z przepisami uprawniony będzie Europejski Inspektor Ochrony Danych.

Jak wygląda proces tworzenia kodeksu postępowania w zakresie AI ogólnego przeznaczenia?

Pierwszy kodeks jest opracowywany w ramach otwartego i przejrzystego procesu. Aby usprawnić wieloetapowy proces opracowywania kodeksu postępowania, utworzone zostanie forum ds. kodeksu postępowania. Zasiądą w nim wszyscy zainteresowani i kwalifikujący się dostawcy modeli AI ogólnego przeznaczenia, dostawcy niższego szczebla wykorzystujący model AI ogólnego przeznaczenia w swoich systemach AI, inne organizacje branżowe, inne organizacje zrzeszające zainteresowane strony, takie jak organizacje społeczeństwa obywatelskiego lub organizacje skupiające posiadaczy praw autorskich, a także przedstawiciele środowiska akademickiego i inni niezależni eksperci.

Urząd ds. AI opublikował zaproszenie do wyrażenia zainteresowania udziałem w opracowaniu pierwszego kodeksu postępowania. Jednocześnie rozpoczęto konsultacje z udziałem wielu zainteresowanych stron, w ramach których uczestnicy przedstawiają swoje opinie i uwagi na temat pierwszego kodeksu postępowania. Zebrane odpowiedzi i informacje będą stanowić podstawę dla pierwszego etapu opracowywania kodeksu postępowania. Kodeks będzie więc od samego początku czerpał z szerokiego spektrum perspektyw i wiedzy fachowej.

W ramach forum powstaną cztery grupy robocze. Każda z nich skupi się na omówieniu konkretnych tematów, które mają znaczenie w kontekście szczegółowego określenia obowiązków dostawców

modeli AI ogólnego przeznaczenia i modeli AI ogólnego przeznaczenia obarczonych ryzykiem systemowym. Uczestnicy forum mogą dołączyć do dowolnej liczby grup roboczych. Posiedzenia będą odbywały się wyłącznie online.

Urząd ds. AI wyznaczy przewodniczących i, w stosownych przypadkach, wiceprzewodniczących każdej z czterech grup roboczych forum, których wybierze spośród zainteresowanych niezależnych ekspertów. Przewodniczący podsumują informacje i komentarze zebrane od uczestników forum, które zostaną wykorzystane w wieloetapowym procesie opracowywania pierwszego kodeksu postępowania.

Jako główni adresaci kodeksu dostawcy modeli AI ogólnego przeznaczenia, oprócz możliwości udziału w forum, otrzymają zaproszenie do udziału w specjalnych warsztatach, w trakcie których będą mogli podzielić się swoimi uwagami do tekstu kodeksu na każdym etapie jego powstawania.

Ostateczna wersja pierwszego kodeksu postępowania zostanie przedstawiona po 9 miesiącach podczas posiedzenia zamykającego, które planowane jest na kwiecień, a następnie opublikowana. Podczas posiedzenia dostawcy modeli AI ogólnego przeznaczenia będą mogli podzielić się swoją decyzją w sprawie korzystania z kodeksu.

W jaki sposób zatwierdzony kodeks postępowania dla dostawców modeli AI ogólnego przeznaczenia stanie się głównym narzędziem służącym zapewnieniu zgodności systemów AI z przepisami?

Gdy kodeks postępowania będzie już gotowy, Urząd ds. AI i Rada ds. AI ocenią jego adekwatność i opublikują swoje oceny. Następnie Komisja będzie mogła zatwierdzić kodeks postępowania i uchwalić akty wykonawcze, które sprawią, że będzie on obowiązywał w całej Unii. Jeżeli do czasu rozpoczęcia stosowania rozporządzenia Urząd ds. AI nie zatwierdzi kodeksu postępowania, Komisja może ustanowić wspólne zasady wdrażania odpowiednich obowiązków.

Dostawcy modeli AI ogólnego przeznaczenia będą więc mogli wykazać zgodność z obowiązkami określonymi w akcie w sprawie AI za pomocą kodeksu postępowania.

Zgodnie z aktem w sprawie AI kodeks postępowania powinien obejmować cele, środki i, w stosownych przypadkach, kluczowe wskaźniki skuteczności działania (KPI).

Dostawcy przestrzegający kodeksu powinni regularnie składać Urzędowi ds. AI sprawozdania na temat wdrożonych środków i ich wyników, w tym – w stosownych przypadkach – wyników mierzonych na podstawie kluczowych wskaźników skuteczności działania.

Ułatwia to egzekwowanie przepisów przez Urząd ds. AI, czego podstawę stanowią uprawnienia przyznane Komisji na mocy aktu w sprawie AI. Urząd może m.in. przeprowadzać oceny modeli AI

ogólnego przeznaczenia, zobowiązywać dostawców modelu do przekazania informacji lub zastosowania określonych środków oraz nakładać sankcje.

Jeżeli zajdzie taka potrzeba, Urząd ds. AI będzie wspierał i ułatwiał przegląd i dostosowanie kodeksu, tak aby ten odzwierciedlał postęp technologiczny i najnowsze rozwiązania.

Po opublikowaniu normy zharmonizowanej i po tym jak Urząd ds. AI oceni, że we właściwym stopniu obejmuje ona swym zakresem odpowiednie obowiązki, zgodność z europejską normą zharmonizowaną powinna w odniesieniu do dostawców oznaczać domniemanie zgodności.

Dostawcy modeli AI ogólnego przeznaczenia powinni ponadto być w stanie wykazać zgodność za pomocą odpowiednich alternatywnych środków, jeżeli kodeksy postępowania lub normy zharmonizowane nie są dostępne lub jeśli zdecydują się z nich nie korzystać.

Czy akt w sprawie AI zawiera przepisy dotyczące ochrony środowiska i zrównoważonego rozwoju?

Celem wniosku w sprawie AI jest przeciwdziałanie zagrożeniom dla bezpieczeństwa i praw podstawowych, w tym prawa podstawowego do wysokiego poziomu ochrony środowiska. Środowisko jest też jednym z wyraźnie wymienionych i chronionych interesów prawnych.

Komisję zobowiązano do wystąpienia do europejskich organizacji normalizacyjnych o opracowanie dokumentu normalizacyjnego dotyczącego procesów sprawozdawczych i dokumentacyjnych w celu poprawy wydajności systemów sztucznej inteligencji, takich jak ograniczenie zużycia energii i innych zasobów przez system AI wysokiego ryzyka w jego cyklu życia, oraz w sprawie energooszczędnego rozwoju modeli AI ogólnego przeznaczenia.

Ponadto Komisję zobowiązano do składania – po raz pierwszy w terminie dwóch lat od daty rozpoczęcia stosowania rozporządzenia, a następnie co cztery lata – sprawozdania z przeglądu postępów w opracowywaniu dokumentów normalizacyjnych dotyczących energooszczędnego opracowywania modeli ogólnego przeznaczenia oraz do przeprowadzenia oceny potrzeby dalszych środków lub działań, w tym środków lub działań o charakterze wiążącym.

Ponadto dostawcy modeli AI ogólnego przeznaczenia, które wytrenowano na dużych ilościach danych i które w związku z tym są podatne na wysokie zużycie energii, są zobowiązani do ujawniania zużycia energii. W przypadku modeli AI ogólnego przeznaczenia wiążących się z ryzykiem systemowym należy ponadto ocenić efektywność energetyczną.

Komisja jest uprawniona do opracowania odpowiedniej i porównywalnej metodyki pomiaru na potrzeby tych obowiązków w zakresie ujawniania informacji.

W jaki sposób nowe przepisy mogą wspierać innowacje?

Ramy regulacyjne mogą zwiększyć upowszechnienie AI na dwa sposoby. Z jednej strony, zwiększenie

zaufania użytkowników zwiększy popyt na systemy AI wykorzystywane przez przedsiębiorstwa i organy publiczne. Z drugiej strony, dzięki zwiększeniu pewności prawa i harmonizacji przepisów dostawcy AI zyskają dostęp do większych rynków, na których będą mogli zaoferować produkty, które użytkownicy i konsumenci doceniają i chętnie kupują. Przepisy będą miały zastosowanie tylko w tych przypadkach, gdy jest to absolutnie konieczne, i w sposób minimalizujący obciążenie podmiotów gospodarczych, przy nierozbudowanej strukturze zarządzania.

Akt w sprawie AI umożliwia ponadto tworzenie **piaskownic regulacyjnych i mechanizmów testowania w warunkach rzeczywistych**, które zapewniają kontrolowane środowisko do testowania innowacyjnych technologii przez ograniczony czas, wspierając tym samym innowacje ze strony przedsiębiorstw, MŚP i przedsiębiorstw typu start-up zgodnie z aktem w sprawie AI. Działania te, wraz z innymi środkami, takimi jak dodatkowe **sieci centrów doskonałości AI oraz partnerstwo publiczno-prywatne na rzecz sztucznej inteligencji, danych i robotyki**, a także dostęp do **centrów innowacji cyfrowych** oraz **ośrodków testowo-doświadczalnych w dziedzinie AI** pomogą stworzyć przedsiębiorstwom odpowiednie warunki ramowe na potrzeby rozwoju i wdrażania AI.

Testowanie systemów AI wysokiego ryzyka w warunkach rzeczywistych będzie można prowadzić maksymalnie przez 6 miesięcy (czas ten może zostać przedłużony o kolejne 6 miesięcy). Przed rozpoczęciem testów należy sporządzić plan i przedłożyć go organowi nadzoru rynku, który musi zatwierdzić plan i szczegółowe warunki testów, z domyślnym zatwierdzeniem, jeżeli w ciągu 30 dni nie udzielono odpowiedzi. Testy mogą podlegać niezapowiedzianym kontrolom przeprowadzanym przez organ.

Testy w warunkach rzeczywistych można przeprowadzać wyłącznie pod warunkiem stosowania szczególnych zabezpieczeń, np. użytkownicy systemów testowanych w warunkach rzeczywistych muszą wyrazić świadomą zgodę, testowanie nie może mieć na nich żadnego negatywnego wpływu, wyniki muszą być odwracalne lub możliwe do pominięcia, a ich dane należy usunąć po zakończeniu testów. Szczególną ochronę przyznaje się grupom szczególnie wrażliwym, tj. ze względu na ich wiek, niepełnosprawność fizyczną lub umysłową.

Jakie znaczenie ma pakt na rzecz AI w kontekście wdrażania aktu w sprawie AI?

Pakt na rzecz AI zainicjował komisarz Thierry Breton w maju 2023 r. Ma on zacieśnić współpracę między Urzędem ds. AI a organizacjami (filar I) oraz zachęcić branżę do dobrowolnego zobowiązania się do rozpoczęcia wdrażania wymogów aktu w sprawie AI przed upływem przewidzianego prawem terminu (filar II).

W szczególności w ramach filaru I uczestnicy będą mogli budować społeczność opartą na współpracy, dzieląc się swoimi doświadczeniami i wiedzą. Urząd ds. AI będzie organizował

warsztaty, które pozwolą uczestnikom lepiej rozumieć akt w sprawie AI i wynikające z niego obowiązki, a także przygotować się do jego wdrożenia. Z kolei dla Urzędu ds. AI takie spotkania mogą być źródłem informacji na temat najlepszych praktyk i wyzwań, przed którymi stoją uczestnicy.

W ramach filaru II organizacje zachęca się do proaktywnego dzielenia się – poprzez dobrowolne zobowiązania – procesami i praktykami, które wdrażają, aby ich systemy były zgodne z nowymi przepisami. Te zobowiązania mają być „deklaracjami zaangażowania" i obejmować działania (planowane lub w trakcie realizacji), które umożliwią spełnienie niektórych wymogów aktu w sprawie AI.

Większość przepisów aktu (np. niektóre wymogi dotyczące systemów AI wysokiego ryzyka) zacznie obowiązywać pod koniec okresu przejściowego (tj. okresu między wejściem w życie aktu a datą rozpoczęcia stosowania).

W związku z tym Urząd ds. AI w ramach paktu na rzecz AI wzywa wszystkie organizacje do proaktywnego działania i wdrażania niektórych kluczowych przepisów aktu w sprawie AI, aby jak najszybciej ograniczyć ryzyko dla zdrowia, bezpieczeństwa i praw podstawowych.

Pozytywnej odpowiedzi na opublikowane w listopadzie 2023 r. zaproszenie do wyrażenia zainteresowania przystąpieniem do paktu na rzecz AI udzieliło już ponad 700 organizacji. Pierwsza sesja informacyjna odbyła się online 6 maja. Wzięło w niej udział 300 uczestników. Oficjalne podpisanie dobrowolnych zobowiązań zaplanowano na jesień 2024 r. W pierwszym tygodniu września odbędą się warsztaty poświęcone paktowi na rzecz AI.

Jaki jest międzynarodowy wymiar podejścia UE?

Wykorzystanie AI wiąże się z konsekwencjami i wyzwaniami, które mają wymiar ponadnarodowy, dlatego też tak ważna jest współpraca międzynarodowa w tym zakresie. Urząd ds. AI kieruje międzynarodowymi działaniami Unii Europejskiej w dziedzinie sztucznej inteligencji na podstawie aktu w sprawie AI i skoordynowanego planu w sprawie AI. We współpracy z partnerami międzynarodowymi UE promuje odpowiedzialne i mądre zarządzanie sztuczną inteligencją zgodnie z wielostronnym systemem opartym na zasadach i w poszanowaniu unijnych wartości.

UE angażuje się w dwu- i wielostronne działania, aby rozpowszechniać godną zaufania, ukierunkowaną na człowieka i etyczną AI. Uczestniczy w wielostronnych forach, na których omawiana jest sztuczna inteligencja – w szczególności G-7, G-20, OECD, Radzie Europy, Globalnym Partnerstwie na rzecz AI i Organizacji Narodów Zjednoczonych. UE utrzymuje też bliskie stosunki dwustronne np. z Kanadą, Stanami Zjednoczonymi, Indiami, Japonią, Koreą Południową, Singapurem oraz regionem Ameryki Łacińskiej i Karaibów.

Źródło: materiał Komisji Europejskiej

CNIL: ZAGROŻENIA ZWIĄZANE Z EUROPEJSKIM CERTYFIKATEM UMOŻLIWIAJĄCYM ZAGRANICZNYM ORGANOM DOSTĘP DO WRAŻLIWYCH DANYCH

Według francuskiego organu nadzorczego (CNIL) w obecnym stanie europejski system certyfikacji usług w chmurze (EUCS) nie pozwala już dostawcom na wykazanie, że chronią oni przechowywane dane przed niepożądanym dostępem. CNIL apeluje o zwiększenie poziomu ochrony danych osobowych w tym certyfikacie poprzez ponowne wprowadzenie odpowiednich gwarancji.

Dane wrażliwe, które muszą być szczególnie chronione

CNIL uważa, że dane przechowywane przez firmę podlegającą prawu pozaeuropejskiemu, jak ma to miejsce w przypadku dostawców usług hostingowych, których spółki macierzyste znajdują się w Stanach Zjednoczonych, mogą być narażone na ryzyko konieczności ujawnienia danych organom publicznym tego kraju. Ryzyko to jest ogólnie uważane za ograniczone, szczególnie w przypadku danych niewrażliwych powierzonych dostawcom usług z siedzibą w krajach zapewniających odpowiedni stopień ochrony danych. Dotyczy to w szczególności Stanów Zjednoczonych, które są krajem zapewniającym odpowiedni stopień ochrony danych od czasu decyzji Komisji Europejskiej z dnia 10 lipca 2023 r. (na warunkach określonych w Ramach ochrony danych UE-USA). Wzmocniona ochrona jest jednak wymagana w przypadku przetwarzania najbardziej wrażliwych danych (np. dużych baz danych dotyczących zdrowia, danych dotyczących przestępstw lub danych dotyczących nieletnich), w przypadku których dane przechowywane w Unii Europejskiej nie powinny być narażone na ryzyko nieuprawnionego dostępu ze strony organów w państwach trzecich.

W takich przypadkach CNIL zaleca korzystanie z usług dostawcy, który podlega wyłącznie prawu europejskiemu i zapewnia odpowiedni poziom ochrony. We Francji, w przypadku usług przetwarzania w chmurze, certyfikat SecNumCloud wydany przez Agence nationale de la sécurité des systèmes d'information (ANSSI) obejmuje to kryterium, chroniąc dane przed dostępem organów zagranicznych.

Niedociągnięcia i zagrożenia związane z europejskim projektem certyfikacji EUCS

Możliwość zapewnienia, w przypadku najbardziej wrażliwych operacji przetwarzania, że podmiot

przechowujący dane nie podlega przepisom pozaeuropejskim, nie jest już uwzględniona w projekcie EUCS dotyczącym europejskiej certyfikacji bezpieczeństwa usług w chmurze, pilotowanym przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA).

CNIL podkreśla, że od dawna zaleca, aby najbardziej wrażliwe bazy danych osobowych (takie jak krajowy system danych zdrowotnych (SNDS) lub dane dotyczące nieletnich), były chronione we Francji przed ich ujawnieniem organom publicznym w krajach trzecich.

CNIL wzywa do włączenia, na zasadzie opcjonalnej, kryteriów „odporności" na przepisy pozaeuropejskie, które mogłyby być inspirowane kwalifikacjami SecNumCloud już obowiązującymi we Francji, do europejskiego systemu certyfikacji EUCS, w celu zapewnienia najwyższej ochrony przetwarzania najbardziej wrażliwych danych osobowych dla europejskich podmiotów przemysłowych.

Źródło: komunikat francuskiego organu nadzorczego CNIL

Fot. pixabay

DPC Z ZADOWOLENIEM PRZYJMUJE ZGODĘ X NA ZAWIESZENIE PRZETWARZANIA DANYCH OSOBOWYCH W CELU SZKOLENIA NARZĘDZIA AI „GROK”

Irlandzki organ ochrony danych (DPC) z zadowoleniem przyjmuje zgodę X na zawieszenie przetwarzania danych osobowych zawartych w publicznych postach użytkowników X z UE/EOG, które były przetwarzane w okresie od 7 maja 2024 r. do 1 sierpnia 2024 r., w celu szkolenia AI „Grok”.

Porozumienie to zostało zawarte w kontekście pilnego wniosku do Sądu Najwyższego złożonego przez DPC na podstawie Sekcji 134 Ustawy o Ochronie Danych z 2018 roku. Wniosek został złożony przed sędzią Reynolds, która w swoich końcowych uwagach wskazała, że prawa i wolności podmiotów danych w całej UE/EOG były kluczowym elementem wniosku.

Był to pierwszy raz, kiedy jakikolwiek wiodący organ nadzorczy (LSA) podjął takie działania, i pierwszy raz, kiedy DPC starała się wykorzystać swoje uprawnienia na podstawie Sekcji 134. Wniosek ten został złożony w celu ochrony praw i wolności użytkowników X z UE/EOG i nastąpił po intensywnych konsultacjach między DPC a X w sprawie szkolenia modelu AI.

Komisarz (Przewodniczący) dr Des Hogan, wypowiadając się na temat tej decyzji, stwierdził:

„Mój kolega, Komisarz Dale Sunderland, i ja z zadowoleniem przyjmujemy zgodę X na zawieszenie przetwarzania, podczas gdy DPC, współpracując z naszymi regulatorami z UE/EOG, nadal bada, w jakim stopniu przetwarzanie jest zgodne z RODO. Jedną z naszych głównych ról jako niezależnego regulatora i organizacji opartej na prawach jest zapewnienie jak najlepszego wyniku dla podmiotów danych, a dzisiejsze wydarzenia pomogą nam nadal chronić prawa i wolności użytkowników X w całej UE i EOG. Będziemy nadal współpracować ze wszystkimi administratorami danych, aby zapewnić przestrzeganie praw naszych obywateli wynikających z Karty Praw Podstawowych UE i RODO.”

Źródło: nota prasowa irlandzkiego organu nadzorczego DPC

Zaproszenie do uczestnictwa w XV edycji programu
„Twoje dane – Twoja sprawa"

Już **2 września 2024** roku rusza XV jubileuszowa edycja ogólnopolskiego programu Urzędu Ochrony Danych Osobowych **„Twoje dane – Twoja sprawa".**

Program skierowany jest do szkół podstawowych i ponadpodstawowych oraz placówek doskonalenia nauczycieli.

Celem Programu jest poszerzenie oferty edukacyjnej szkół oraz placówek doskonalenia nauczycieli o treści związane z ochroną danych osobowych i prawem do prywatności oraz podniesienie kompetencji nauczycieli, doradców metodycznych i konsultantów w obszarze kształtowania wśród uczniów wiedzy i umiejętności związanych z ochroną danych osobowych i prawem każdego człowieka do prywatności.

Uczestnictwo w Programie jest bezpłatne.
Szczegółowe informacje znajdują się na stronie internetowej UODO.

Organizator Programu: UODO URZĄD OCHRONY DANYCH OSOBOWYCH

Patroni honorowi: Minister Edukacji, RZECZNIK PRAW DZIECKA

Patroni medialni: TVP2, PNS, głosnauczycielski, TIK edukacji, Portal Oświatowy, Polskie Radio dzieciom

Zaproszenie na konferencję
„RODO w edukacji"

Konferencja zainauguruje jubileuszową XV edycję ogólnopolskiego programu edukacyjnego Urzędu Ochrony Danych Osobowych **„Twoje dane – Twoja sprawa"**, która rozpoczęła się 2 września 2024 roku. Celem programu jest popularyzacja wiedzy o ochronie danych osobowych i prawa do prywatności.

Konferencja organizowana jest we współpracy z Miastem Stołecznym Warszawa oraz Warszawskim Centrum Innowacji Edukacyjno-Społecznych i Szkoleń. Odbędzie się **10 października 2024** roku w godz. 12.00–15.00 w siedzibie WCIES.

Wydarzenie skierowane do dyrektorów szkół oraz nauczycieli ma na celu przybliżenie aktualnych tematów związanych z ochroną danych osobowych w sektorze oświaty. Omówione zostaną praktyczne aspekty wdrażania regulacji prawnych i standardów ochrony danych osobowych dzieci w codziennej pracy.

Konferencja będzie doskonałą okazją do zapoznania się z najnowszymi zmianami w przepisach oraz analizy wyzwań związanych z edukacją na rzecz ochrony danych osobowych dzieci. Będzie to również forum wymiany doświadczeń między nauczycielami oraz sposobność do konsultacji z ekspertami Urzędu Ochrony Danych Osobowych. Ponadto porad prawnych podczas wydarzenia udzielą pracownicy Infolinii UODO.

Spotkanie będzie transmitowane na żywo.
Link do transmisji zostanie udostępniony w dniu konferencji **na stronie UODO**.
Link do rejestracji do udziału stacjonarnego
Program wydarzenia

URZĄD OCHRONY DANYCH OSOBOWYCH

LISTA KONFERENCJI UODO

październik 2024 r.

Konferencja
(stacjonarnie)
Ochrona danych jako element odporności społeczeństwa i państwa
7 października 2024 r.
Centrala ZUS
ul. Szamocka 3/5, Warszawa

Konferencja
(hybrydowo)
Czas wyzwań – projektowanie systemów AI oraz wdrożenie NIS2 w organizacji
9 października 2024 r.
oddział ZUS
ul. Gen. H. Dąbrowskiego 45, Chorzów

Konferencja
(hybrydowo)
RODO w edukacji
10 października 2024 r.
Warszawskie Centrum Innowacji Edukacyjno–Społecznych i Szkoleń
ul. Stara 4, Warszawa

Konferencja
(hybrydowo)
Ochrona danych w robotyce medycznej w dobie AI Act i EHDS
15 października 2024 r.
siedziba UODO, budynek Intraco,
ul. Stawki 2, sala konferencyjna na 38. piętrze, Warszawa

Konferencja
(online)
Dwudniowe szkolenie dla koordynatorów – uczestników XV edycji programu „Twoje dane – Twoja sprawa"
24-25 października 2024 r.

Zapraszamy do udziału w wydarzeniach.

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl