URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 07_08/07_08/24

www.uodo.gov.pl

SPIS TREŚCI

SPIS TREŚCI

Szanowni Państwo,

mimo wakacji w sprawach dotyczących ochrony danych osobowych dzieje się wiele. Wchodzą w życie ważne przepisy, których nie da się dobrze stosować bez prawidłowego przetwarzania danych osobowych. Pojawiają się nowe problemy, które musimy odpowiednio interpretować, by nie tworzyć niepotrzebnego ryzyka dla procesów przetwarzania danych osobowych.

Poradniki

Postanowiliśmy przygotować nowy poradnik – „Prowadzenie działalności związkowej zgodnie z RODO". To efekt wniosków, jakie nasunęły się po zorganizowanym perz UODO seminarium „Przetwarzanie danych osobowych przez związki zawodowe". Jednak pierwsze pomysły na ten poradnik zrodziły się w ramach konsultacji społecznych poradnika „Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców".

Nowy poradnik, który będzie adresowany do związków zawodowych, podobnie jak inne tego rodzaju materiały, powstanie we współpracy ze Społecznym Zespołem Ekspertów przy PUODO.

W tej chwili analizujemy zgłoszone w toku konsultacji uwagi do dwóch pierwszych poradników poddanych konsultacjom: o zatrudnieniu oraz o zgłaszaniu naruszeń ochrony danych. Wszystkie przesłane uwagi są opublikowane na stronie urzędu.

Ochrona sygnalistów

Nowym wielkim wyzwaniem, jakie staje przed nami wszystkimi, będzie przetwarzanie i ochrona danych osobowych przy zgłaszaniu nieprawidłowości zgodnie z nową ustawą o sygnalistach. Ma ona zapewnić bezpieczeństwo osobom, które w związku z pracą zauważają naruszenia prawa i w interesie publicznym chcą o nich poinformować.

Ustawa, przyjęta przez parlament wiosną, wdraża do polskiego porządku prawnego unijną dyrektywę 2019/1937. Jej celem jest m.in. ułatwienie prowadzenia działalności gospodarczej i inwestycji transgranicznych poprzez wzmocnienie praworządności. Chodzi o to, by praktyka działania nie rozmijała się z literą prawa – z tego powodu zgłoszenia sygnalistów są ważne dla instytucji, których dotyczą. Jednak system nie zadziała bez odpowiedniej ochrony danych sygnalistów. Więcej na ten temat

Ustawa Kamilka i prawa dzieci

Kolejnym ważnym prawem, które teraz wchodzi w życie, jest „ustawa Kamilka" – przepisy wzmacniające ochronę dzieci przed przemocą i wykorzystaniem seksualnym. Z punktu widzenia danych osobowych ma dwa newralgiczne punkty: placówki pracujące z dziećmi muszą tworzyć warunki do tego, by dzieci mogły przekazywać sygnały o krzywdzie w bezpieczny dla nich i poufny sposób. Po drugie – ustawa wymaga, by sprawdzać dokładnie dane osób, które mogą się z dziećmi kontaktować. Zwracamy uwagę, że obu tych zadań nie da się wykonać poprawnie bez przeprowadzenia analizy ryzyka, tak jak wskazuje RODO. Aby ułatwić przygotowania do wdrożenia tych przepisów, przygotowaliśmy wskazówki: co zrobić, by chroniąc dzieci nie narazić na niepotrzebne ryzyko ich danych, a także danych osób, które z dziećmi pracują.

Lepszej ochronie dzieci w świecie cyfrowym służy też nasz poradnik „Wizerunek dziecka w internecie. Publikować czy nie?". Urząd Ochrony Danych Osobowych przygotował go wspólnie z Fundacją Orange z myślą o osobach pracujących w organizacjach i placówkach, których zadaniem jest troska o dobro i bezpieczeństwo dzieci. Poradnik opisuje, jakiej ochronie podlega wizerunek, jak poprawnie skonstruować zgodę na jego rozpowszechnianie i obala najpopularniejsze mity z tym związane. Zawiera też listę potencjalnych ryzyk, które wiążą się z publikowaniem wizerunków dzieci w internecie. Materiał zawiera też listę pytań, które warto sobie zadać przed udostępnianiem online treści z udziałem dzieci oraz inspiracje do poszukiwania bezpiecznych dla dzieci rozwiązań.

Precedensowe decyzje PUODO

Pragnę także zwrócić Państwa uwagę na dwie ważne, precedensowe sprawy: postanowienia zabezpieczające nakazujące spółce Meta wstrzymać publikację w Polsce fałszywych reklam wykorzystujących wizerunek Pani Omeny Mensah oraz Pana Rafała Brzoski.

Nie zrobiliśmy sobie wakacji od promowania wiedzy o prawie do prywatności i potrzebie ochrony danych. W tym roku wraz ze współpracownikami byłem obecny na festiwalu Pol'and'Rock, o czym można więcej przeczytać na naszej stronie internetowej. Tej imprezie muzycznej towarzyszy wiele spotkań na tematy ważne dla szczególnie młodych osób. Jest to świetne miejsce do przekazywania wiedzy o przysługujących nam prawach, ale też o wymaganiach, jakie stawia przed nami cyfrowa teraźniejszość.

Formą kontaktu z odbiorcami w każdym wieku są organizowane w całym kraju spotkania Tour de Konstytucja. Także tam Urząd Ochrony Danych Osobowych jest obecny.

Dla młodszych, mam na myśli uczniów szkół podstawowych i ponadpodstawowych, przygotowaliśmy kolejną, już piętnastą edycję programu „Twoje dane – Twoja sprawa". Nabór do programu rusza 2 września. Serdecznie zapraszamy.

Mirosław Wróblewski
Prezes UODO

Drodzy Czytelnicy!

Mam nadzieję, że tylko dla nielicznych z Was będzie to ostatni egzemplarz „Biuletynu UODO”. Jak zapowiadaliśmy w poprzednim numerze, aktualizujemy bazę subskrybentów. Co się z tym łączy – od nowa tworzymy listę jego subskrybentów.

Ci z Was, którzy nie zapiszą się do nowej bazy danych do 31 sierpnia 2024 r., od września przestaną otrzymywać Biuletyn. Dlatego serdecznie zachęcam do dołączenia do grona stałych czytelników i potwierdzenia zapisu poprzez kliknięcie w link, jaki otrzymacie w mailu zwrotnym. Procedura jest jasna i prosta, a przejście przez nią pozwoli Wam mieć dostęp do przygotowanych przez nas cyklicznie informacji z zakresu ochrony danych.

Przed Wami specjalny, podwójny numer, a w nim wywiad z Mirosławem Gumularzem, przewodniczącym Społecznego Zespołu Ekspertów przy PUODO, radcą prawnym, byłym kandydatem na stanowisko Prezesa Urzędu Ochrony Danych Osobowych. Mowa w nim o tym, jak członkowie SZE dzielą się zadaniami, jak wygląda komunikacja w grupie ekspertów oraz dlaczego zespół chce nasycić dyskusję o ochronie danych kwestiami ryzyk dla praw lub wolności. Z rozmowy dowiecie się, czemu warto pisać prostym językiem oraz które z działań innych organów nadzorczych należy, zdaniem dr Gumularza wdrożyć w UODO.

Zapraszam też do zapoznania się z relacją z seminarium UODO dotyczącego przepisów ustawy o ochronie sygnalistów, podczas którego omówiono uwagi przesłane w ramach konsultacji społecznych. W trakcie spotkania eksperci Urzędu wraz z przedstawicielami Społecznego Zespołu Ekspertów oraz specjalistami z zewnątrz zaproponowali wykładnię przepisów w zakresie dotyczącym danych osobowych. Przepisy ustawy budzą wiele wątpliwości, tym bardziej ich interpretacja przez profesjonalistów może zawierać cenne wskazówki dla osób, które będą uczestniczyć we wdrażaniu dyrektywy.

W tym numerze piszemy o tym, że tylko zgoda uprawnia szkołę wyższą do publikacji imion i nazwisk absolwentów oraz roku ukończenia przez nich studiów w księdze pamiątkowej wydawanej z okazji jubileuszu uczelni.

Nowoczesne pojazdy są wyposażane w zaawansowane systemy elektroniczne, sztuczną inteligencję oraz technologie komunikacyjne. Jednak wraz z postępem technologicznym pojawiają się również wyzwania związane z ochroną danych i prywatności użytkowników. W artykule w dziale „Nowe Technologie” podkreślamy konieczność wypracowania nowych standardów i regulacji, które

zagwarantują bezpieczeństwo informacji, nie hamując jednocześnie innowacyjnego rozwoju.

Z pewnością zainteresuje Was jedna z opisanych decyzji Prezesa UODO. Sprawa dotyczyła korespondencji w sprawie psów biegających po drodze. Wniosek jest taki, że gdy obywatel zgłasza sprawę i instytucja publiczna podejmuje ją z urzędu, nie ma żadnego powodu, by w swojej korespondencji ujawniała dane zgłaszającego.

Jeśli chcecie wiedzieć, co się dzieje w innych europejskich organach nadzorczych, w podwójnym numerze przypominamy m.in., że hiszpański odpowiednik UODO przyjął środek tymczasowy, który uniemożliwił Meta wdrożenie funkcji wyborczych. Z kolei francuski organ właściwy ds. ochrony danych nadzorczy (CNIL) kontynuuje prace nad opracowaniem innowacyjnej i chroniącej prywatność sztucznej inteligencji.

Z końcem lata zachęcam również do przeczytania relacji z udziału reprezentantów Urzędu w 30. Pol'and'Rock Festival. W tym roku mieliśmy tam swój stacjonarny punkt porad, w którym uczestnicy festiwalu mogli zasięgnąć pomocy w zakresie ochrony danych osobowych. Warto poczuć odrobinę tej niezwykłej festiwalowej atmosfery i zobaczyć, co się działo na tym wyjątkowym wydarzeniu – przeczytajcie sprawozdanie Izy Maryańskiej, na co dzień głównej specjalistki infolinii Urzędu, która na początku sierpnia prowadziła punkt porad dla uczestników Festiwalu.

Nadchodzi sezon chorobowy. Pamiętajcie więc, że wezwanie pacjenta do gabinetu powinno odbywać się tak, by zapewnić poufność jego danych osobowych. Do przestrzegania tej zasady personel medyczny zobowiązują zarówno ogólne rozporządzenie o ochronie danych (RODO), jak i przepisy branżowe.

Trzymajcie się zdrowo i pamiętajcie o prawach, jakie Wam przysługują.

Karol Witowski
p.o. Rzecznika Prasowego UODO

URZĄD OCHRONY DANYCH OSOBOWYCH

Drodzy Subskrybenci „Biuletynu UODO”,

jedną z zasad ogólnych przetwarzania danych osobowych, jest zasada prawidłowości danych.
Dziś baza subskrybentów „**Biuletynu UODO**” liczy kilka tysięcy osób, zauważyliśmy jednak, że wiele adresów e-mail, na który wysyłamy Biuletyn jest już nieaktualnych.

Od 1 września br. zaczynamy proces gromadzenia nowych subskrybentów od podstaw. Ci, którzy nie zapiszą się do bazy danych do **31 sierpnia br**., przestaną otrzymywać prenumeratę Biuletynu.

Dlatego, jeśli tematy dotyczące ochrony danych osobowych są Wam bliskie, serdecznie zachęcamy do ponownej subskrypcji.

Robert Miętkowski,
Inspektor Ochrony Danych w UODO

Zapisz się!

1 ROZMOWA Z EKSPERTEM

ISTOTNE JEST NIE TYLKO CO ROBIMY, ALE TEŻ JAK PRACUJEMY WSPÓLNIE Z URZĘDEM

Z Mirosławem Gumularzem, Przewodniczącym Społecznego Zespołu Ekspertów przy PUODO rozmawiał Karol Witowski, p.o. Rzecznika Prasowego UODO

7 miesięcy temu był Pan jednym z kandydatów na stanowisko Prezesa UODO. Widzimy, że współpraca między Panem i prezesem Mirosławem Wróblewskim układa się dobrze. Jest Pan przewodniczącym Społecznego Zespołu Ekspertów przy Prezesie Urzędu Ochrony Danych Osobowych.

Kilka słów na temat samego wyboru nowej osoby na funkcję Prezesa UODO. Sam fakt, że pojawiłem się w gronie osób, które były brane pod uwagę i mogły zaprezentować pomysł na zmianę w urzędzie był dużym zaszczytem, w szczególności uwzględniając to, że powstała petycja podpisana przez prawie dwa tysiące osób dotycząca poparcia. Dodatkowo proces wyboru nowego Prezesa UODO był niezwykle transparentny.

Wydaje mi się, że pierwszy raz piastun tak istotnego organu został wybrany w tak przejrzystej formule. Wiele osób mówiło wtedy, że przecieramy szlaki i mam nadzieję, że tak będzie. Należy zwrócić uwagę, że obecny prezes UODO – Mirosław Wróblewski został wybrany spośród osób, które brały udział w publicznym wysłuchaniu w Sejmie pod koniec zeszłego roku. Czyli był to realnie jawny proces. Szerokie grono osób (nie tylko specjalistów) miało szansę zadać pytania i wysłuchać kandydatów.

Istotnym czynnikiem był udział społeczeństwa, które mogło zapoznać się z propozycjami kandydatów w trakcie transmisji w mediach społecznościowych. Zwracam na to uwagę, ponieważ ta sama idea transparentności przyświecała powołaniu Społecznego Zespołu Ekspertów. Chodziło o to, żeby głos strony społecznej był brany pod uwagę w ramach aktywności Urzędu. Był to zresztą nasz wspólny pomysł, który pojawił się w czasie tego kandydowania. Nie będę zresztą ukrywał – bo to żadna tajemnica – że z obecnym Prezesem UODO miałem możliwość wcześniej współpracować przy okazji aktywności naukowej. Jesteśmy współautorami wielu publikacji, m.in. ostatnio komentarza do rozporządzenia UE – akt o usługach cyfrowych, nad którym zakończyliśmy pracę dosłownie kilka dni przed tym, jak został wybrany na nowego Prezesa UODO.

1 ROZMOWA Z EKSPERTEM

Warto zwrócić uwagę, że w składzie zespołu mamy też innego kandydata na Prezesa UODO – dyr. Andrzeja Rybusa-Tołłoczko.

SZE to społeczne ciało opiniodawczo-doradcze Prezesa Urzędu. Poza Panem w jego skład wchodzi jeszcze 14 ekspertów. Jak dzielicie się zadaniami? Czy jest tu jakiś podział na grupy, które rozwiązują konkretne problemy?

W pierwszej kolejności chciałbym odnieść się do liczby 15 osób. Biorąc pod uwagę przykłady grup roboczych, które funkcjonują przy różnych ministerstwach to trzeba przyznać, że nie jest to liczna grupa. Po prostu uznaliśmy z Prezesem, że Społeczny Zespół Ekspertów przy PUODO nie może być przesadnie liczny, bo nie będzie mógł działać "zwinnie". Oczywiście będziemy zapraszać do poszczególnych zagadnień ekspertów spoza naszego zespołu tak, żeby paleta poglądów i argumentów mogła być odpowiednio reprezentatywna. Przykładem takiej sytuacji było ostatnie seminarium dotyczące kwestii ochrony sygnalistów, gdzie oprócz pracowników urzędu i członków naszego zespołu, obecni byli także "zewnętrzni" przedstawiciele nauki i praktyki.

Co do organizacji pracy przyjęliśmy założenie, że pracować nad danym tematem powinny osoby, które czują, że to ich zakres specjalizacji. Dlatego przy okazji każdego projektu tworzymy ad hoc podgrupę roboczą, która będzie się nim zajmowała. I muszę przyznać, że nie ma do tej pory problemu z chętnymi do pracy w zespołach projektowych.

Członkowie zespołu pracują z różnych miejsc w Polsce. Jak wygląda komunikacja, kiedy nie wszyscy mogą się spotkać w jednej przestrzeni?

Staramy się działać elastycznie, ale oczywiście przy zapewnieniu reguł bezpieczeństwa. O ile jest to możliwe, staramy się spotykać w urzędzie z jego pracownikami. Na takich roboczych spotkaniach omawialiśmy m.in. do tej pory zgłoszone uwagi w ramach konsultacji dotyczących ustawy o ochronie sygnalistów czy dotyczące poradników w zakresie kwestii pracowniczych oraz naruszeń. Osoby, które nie są w stanie z różnych względów uczestniczyć offline, łączą się zdalnie (czyli jest to formuła hybrydowa). Co tydzień organizujemy także spotkania statusowe, gdzie omawiamy bieżące kwestie m.in. stan prac nad danym tematem, czy np. potrzebę pilnego zajęcia się jakimś zagadnieniem. Ustalamy także priorytety co do nowych tematów.

Natomiast taka hybrydowa praca daje nam dużą elastyczność. Przykładem jest seminarium dotyczące sygnalistów, gdzie w ciągu kilku tygodni udało się zebrać uwagi, opracować je, przedyskutować w ramach naszego zespołu oraz w dialogu z urzędem i zorganizować wspólnie z UODO spotkanie, które odbiło się dużym (mam wrażenie – bardzo pozytywnym) echem.

1 ROZMOWA Z EKSPERTEM

Na stronie urzędu, w zakładce dotyczącej naszego zespołu, będziemy starali się na bieżąco publikować kalendarium naszych prac. Zależy nam na tym, żeby także w tym aspekcie zapewnić przejrzystość naszych działań. Podkreślę jednak, że tam publikowane są wyłącznie najważniejsze spotkania, wydarzenia, etc. Pomiędzy nimi odbywa się cała masa czynności, analiz, dyskusji.

Zespół nie ma uprawnień do wydania stanowisk, jednak może wychodzić z własnymi inicjatywami i wskazywać na problemy, którymi warto się zająć. Wyobrażam sobie, że z tak różnorodnym doświadczeniem jego członków powstają ciekawe burze mózgów

To prawda. Zespół nie ma kompetencji do wydawania formalnych stanowisk, ale cel jego powołania był inny – wspieranie urzędu poprzez prezentowanie stanowisk i różnych kierunków argumentacji. Brak formalnego uprawnienia do wydawania stanowisk traktuję jako szansę, a nie jako problem. Dzięki temu współpraca z urzędem ma charakter synergii, a nie działania "obok". Staramy się być dla pracowników urzędu partnerem do dyskusji, a nie konkurencją. Zależy nam na tym, żeby stanowisko zespołu było istotne nie ze względu na jego formalny charakter, ale dlatego że jest przekonujące, dobrze uzasadnione, z odwołaniem do piśmiennictwa i orzecznictwa sądowego.

Dlatego tak istotny był dobór składu naszego zespołu. Są to eksperci z dużym dorobkiem zarówno praktycznym, jak i teoretycznym. Nie brakuje w naszym składzie naukowców, ale i praktyków. Dodatkowo skład zespołu budowaliśmy w ten sposób, aby znaleźli się w nim nie tylko prawnicy, ale także eksperci z różnych dziedzin. Dlatego możemy brać udział w dyskusji nie tylko w kwestiach prawnych, ale i technicznych. Przykładowo mamy w składzie osoby specjalizujące się w obszarze stosunków pracy, e-commerce, kwestiach publicznoprawnych, nowych technologii, usług finansowych, kwestii medycznych. W skład zespołu wchodzą także osoby związane z NGO czy organizacjami zrzeszającymi inspektorów ochrony danych. Ta mieszanka zapewnia ciekawą dyskusję i jest na ogół bardzo – że się tak wyrażę – "dynamiczna". Mamy w zespole osoby, które nie unikają sporu na argumenty, bo to dla nich codzienność w ramach pracy naukowej czy praktyki prawniczej.

A co do nowych pomysłów to nie pamiętam tygodnia od momentu powstania zespołu, żeby nie pojawił się pomysł na nową aktywność.

Wspomniana synergia nie polega tylko na tym, że my staramy się przekonać na siłę do czegoś pracowników UODO, np. do jakiegoś pomysłu na interpretację przepisów. Mam przekonanie, że prowadzone pomiędzy naszym zespołem a pracownikami Urzędu dyskusje i spieranie się na argumenty pomagają zrozumieć drugiej stronie inny kontekst tj. osób stosujących w praktyce przepisy. To oczywiście działa też w drugą stronę. Czasem przedstawienie kontekstu funkcjonowania organu sprawia, że my także rozumiemy lepiej, z czego wynika prezentowane podejście.

1 ROZMOWA Z EKSPERTEM

Zespół może już się pochwalić udanymi konsultacjami do dwóch poradników: o przetwarzaniu danych przy zatrudnianiu oraz o reagowaniu na naruszenia danych osobowych. Jak przebiegały prace nad poradnikami?

Już na pierwszym spotkaniu organizacyjnym zespołu założyliśmy, że praca nad aktualizacją poradników będzie jedną z pierwszych aktywności i form współpracy z urzędem. Co istotne, chcemy żeby aktualizacja poradnika dotyczącego zatrudnienia została poprzedzona szerszą dyskusją problematycznych kwestii, jak np. dotyczących testów psychometrycznych. Te prace trwają. Jesteśmy na etapie przygotowywania odpowiedzi na zgłoszone uwagi w toku konsultacji społecznych i przedstawiania propozycji naszego Zespołu na zmiany. Natomiast jeszcze raz podkreślę, że rolą zespołu jest przedstawianie stanowisk, możliwych rozwiązań problematycznych kwestii. Ostatecznym autorem dokumentów jest Urząd Ochrony Danych Osobowych, który w tym zakresie jest wyłącznie właściwy.

Oprócz tego w międzyczasie udało się wspólnie z Urzędem zorganizować konsultacje społeczne dotyczące wdrożenia przepisów dotyczących ochrony sygnalistów. Na ich podstawie przeprowadziliśmy seminarium, które cieszyło się bardzo dużym zainteresowaniem. W oparciu o to seminarium i wnioski, które tam zostały przedstawione, Urząd będzie teraz systematycznie publikował informacje dotyczące wdrożenia tych przepisów. W międzyczasie uruchomiliśmy kilka innych projektów. W szczególności, projekt dotyczący poradnika dla związków zawodowych, przeglądu podstawowych pojęć i ich interpretacji (jak administrator danych, podmiot przetwarzający).

Istotne jest nie tylko co robimy, ale też jak pracujemy wspólnie z Urzędem. Te formy współpracy zawsze ustalamy w odniesieniu do danego zagadnienia. Oprócz konsultacji dokumentów i stanowisk Urzędu (np. poradników) najpewniej będziemy też tworzyć nasze stanowiska, które będą stanowić punkt wyjścia dla UODO do opracowania własnych stanowisk.

Ustaliliśmy we współpracy z Urzędem, że będzie to wyraźnie komunikowane i oznaczone m.in. na stronie Urzędu, w jakim charakterze w danym kontekście występuje Społeczny Zespół Ekspertów przy PUODO. Jednym z takich pomysłów jest stworzenie rejestru ryzyk. Zależy mi bardzo na tym, aby powstał i był wsparciem dla administratorów. Ma być pomocą dla organizacji przy stosowaniu RODO. Ocena ryzyka to jedna z najważniejszych kwestii na gruncie RODO, a jednocześnie najpewniej najtrudniejsza. I właśnie rejestr ryzyk powstanie prawdopodobnie jako nasz (tj. zespołu) autorski projekt, który zostanie poddany konsultacjom i dyskusji. Zobaczymy jaki będzie odzew, zwłaszcza ze strony inspektorów ochrony danych. Chcemy zobaczyć, czy będzie on pomocny i ewentualnie jakie pytania zrodzi.

1 ROZMOWA Z EKSPERTEM

Niezależnie od tego, staramy się, żeby w ramach każdej aktywności naszego zespołu, kłaść nacisk na podejście skoncentrowane wokół realnych ryzyk dla praw lub wolności osób, których dane są przetwarzane. Chcemy jako zespół nasycić dyskusję o ochronie danych kwestiami ryzyk dla praw lub wolności. Mam wrażenie, że czasem jest ona za bardzo formalna w tym sensie, że dotyczy głównie interpretacji przepisów, a czasem nam umyka, że te przepisy dotyczą konkretnych procesów przetwarzania, które mają swoje cechy (operacje na danych) i ryzyka.

W tym zakresie niezwykle ciekawa była dyskusja na ostatnim seminarium dotyczącym ochrony sygnalistów, która dotyczyła m.in. ryzyk dla praw lub wolności. Podobnie było na spotkaniu dotyczącym związków zawodowych i ochrony danych osobowych. Jeżeli omawiane były kwestie formalne, to zawsze staraliśmy się, aby dyskusja, mimo wszystko, koncentrowała się wokół ryzyk dla ludzi, których dane są przetwarzane.

Apelował Pan o powołanie jednostki prostego języka wspierającej polski biznes w tworzeniu klauzul z RODO. Tymczasem w maju br. w UODO został powołany Zespół ds. opracowania i wdrożenia zasad prostego języka. Doszliśmy do takiego momentu, w którym zaczynamy komunikować w sposób zbyt skomplikowany czy może komunikatów jest tak dużo, że tylko te proste docierają do odbiorców?

Prosty język i jasna komunikacja to bardzo złożony i wielowymiarowy problem. Z jednej strony język ochrony danych jest wypełniony żargonem prawniczym, jest bardzo formalny i na dodatek ma swoją specyficzną siatkę pojęciową (administrator danych, podmiot danych, etc.), która nie jest zrozumiała nawet dla prawników, którzy nie specjalizują się w tej dziedzinie. Pamiętam jeszcze jak za czasów studiów doktoranckich trudno było mi wytłumaczyć kolegom cywilistom, że zgoda w rozumieniu przepisów o ochronie danych, to coś innego niż akceptacja warunków umowy (np. akceptacja regulaminu usługi), chociaż w tym drugim przypadku potocznie mówimy o “zgodzie”.

Z drugiej strony pojawiają się pojęcia techniczne (szyfrowanie, usługi chmurowe, autoryzacja, etc.). Na to nakłada się wielość zainteresowanych stron: inspektorzy ochrony danych, administratorzy, osoby, których dane są przetwarzane, dostawcy usług, pracownicy IT, etc.

Dla mnie prawidłowy komunikat to komunikat dostosowany do adresata. Inaczej mówimy na konferencji, na której są sami specjaliści, a inaczej szkoląc osoby, które muszą znać podstawowe zagadnienia. Przy tworzeniu komunikatu należy zawsze na początku zadać sobie

pytanie, do kogo jest kierowany, jakie cele ma osiągnąć i jak powinien być sformułowany, żeby tak się stało.

Pierwszym testem takiego podejścia będzie aktualizacja poradników.

Podkreśla Pan, że każdy komunikat powinien być dostosowany do odbiorcy. Od czasu, kiedy prezesem UODO został Mirosław Wróblewski komunikacja na stronie Urzędu przeszła duże zmiany. Widzi Pan tę różnicę w treści komunikatów? Jesteśmy otwarci na uwagi.

Różnica jest bardzo odczuwalna. Przede wszystkim Prezes i jego Zastępcy spotykają się i rozmawiają ze środowiskami inspektorów ochrony danych, biznesu, grup społecznych, czy branżowych. To jest nowa jakość w komunikacji, wsłuchiwania się w stronę społeczną.

Obecny Prezes UODO prężnie działa na rzecz ochrony danych dzieci. Edukacja dzieci to też temat, który Pana bardzo interesuje.

Jeżeli chodzi o ochronę dzieci, których dane są przetwarzane, problem jest wielopłaszczyznowy. Po pierwsze chodzi o edukację samych dzieci. Przykładowo: uświadamianie, że jeżeli ktoś z nimi "czatuje" i podaje się za daną osobę (np. nauczyciela), to wcale nie musi oznaczać, że nią jest.

Druga kwestia to edukacja rodziców. To oni, w pierwszej kolejności, powinni zwracać uwagę dzieciom na ryzyka związane np. z korzystaniem z mediów społecznościowych. Niestety często problem wynika z działań samych rodziców, którzy bez opamiętania rozpowszechniają np. wizerunek dziecka. Oczywiście oprócz rodziców istotną rolę ma także szkoła czy instytucje szeroko pojętej edukacji. Trzeba pamiętać, że niestety źródłem zagrożeń mogą być także same dzieci. Ostatnio głośno było o sprawie jednego z liceów, gdzie sami uczniowie rozpowszechniali zdjęcie uczennicy zmienione przy wykorzystaniu technologii AI (deep fake). Jest to tzw. cyberprzemoc pomiędzy rówieśnikami.

Uważam, że wydany poradnik dotyczący wizerunku dziecka jest bardzo dobrym krokiem w tym zakresie. To, co moim zdaniem jest teraz najważniejsze, to utrzymanie zainteresowania i edukacja w tym zakresie. Tak, żeby kwestia ochrony dzieci (ale także innych grup szczególnie narażonych, np. osób starszych) była procesem, a nie jednostkowym zdarzeniem. Pamiętajmy, że ochrona dzieci w internecie to nie tylko ochrona danych osobowych, ale także szeroko rozumiana edukacja związana z korzystaniem z internetu, a w szczególności mediów społecznościowych. Przykładowo w jednym ze stanów w USA wprowadzone zostały przepisy wprowadzające do edukacji w szkołach obowiązkową naukę w zakresie korzystania z mediów społecznościowych przez dzieci.

W pierwszej kolejności pilnie zajęliśmy się kwestią tzw. ustawy Kamilka i planujemy działania we współpracy z innymi ekspertami od edukacji dzieci w internecie. W tym zakresie, moim zdaniem,

istotny z punktu widzenia edukacji będzie wskazany powyżej rejestr ryzyk. Powinien on uwzględniać specyficzne ryzyka dla małoletnich.

W zakresie swojej praktyki zawodowej oraz naukowej specjalizuje się Pan w szeroko pojętym prawie nowych technologii. To gałąź, która bardzo dynamicznie się rozwija.

Formalnie nie ma czegoś takiego jak prawo nowych technologii. Natomiast to określenie zakorzeniło się w dyskusji i jest powszechnie stosowane przez praktyków. Pytanie oczywiście, czy osoby które się nim posługują rozumieją je w podobny sposób. Dla mnie to pojęcie oznacza regulacje, które dotyczą najbardziej aktualnych technologii, problemów i ryzyk z nimi związanych. Oczywiście nie jest tak, że przepisy muszą zawsze wskazywać z nazwy te technologie. Przykładowo: RODO jest neutralne technologicznie. Dotyczy zarówno przetwarzania danych w sposób tradycyjny (np. segregator z dokumentami), jak i przy wykorzystaniu algorytmów sztucznej inteligencji. Często głównym problemem w ramach prawa nowych technologii jest właśnie ustalenie, jak te "stare" lub właśnie neutralne technologicznie regulacje dotyczą nowych zjawisk. Pamiętam szeroką dyskusję, gdy RODO rozpoczynało swoje stosowanie, nad tym, które rozwiązania technologiczne podlegają pod pojęcie podejmowania decyzji w sposób całkowicie zautomatyzowany w rozumieniu art. 22 RODO.

Kolejna istotna i specyficzna kwestia to rozumienie samych technologii. Oczywiście w każdej dziedzinie prawa, istotne jest rozumienie stanów faktycznych, które podlegają pod jej przepisy. Tutaj jest to dużo bardziej zniuansowane. Niestety bardzo często czyta się wypowiedzi przedstawicieli nauki, którzy stwierdzają, że z daną technologią łączą się te, a nie inne konsekwencje prawne. Później okazuje się, że sprawa jest dużo bardziej skomplikowana. Dlatego w tej dziedzinie prawa trzeba być bardzo ostrożnym co do generalnych ocen, ponieważ często ocena prawna jest osadzona w bardzo specyficznym stanie faktycznym. Świetnym przykładem jest ostatnia dyskusja odnośnie AI i wypowiedzi niemieckiego (z Hamburga) organu, co do tego, czy w ramach dużych modeli językowych dochodzi do przetwarzania danych osobowych. Jeśli ktoś nie rozumie jak działa dana technologia, a nawet dany algorytm czy aplikacja, nie będzie w stanie ocenić jej od strony prawnej.

Jako doradca społeczny ds. ochrony danych osobowych w Ministerstwie Cyfryzacji brał Pan udział w pracach nad wdrożeniem RODO do polskiego porządku prawnego. Z perspektywy czasu jak Pan ocenia ten proces? Co się udało zrobić, a z czego nie jest Pan zadowolony?

Uważam, że zrobiliśmy jako społeczeństwo bardzo dużo, zwłaszcza na początku stosowania RODO,

aby rosła świadomość potrzeby ochrony ludzi, których dane są przetwarzane. Jednocześnie uważam, że za dużo było narracji o karach, a za mało o tym, dlaczego te przepisy wchodzą. Nie twierdzę, że źródłem tej narracji o karach był sam UODO, ale może w tym zakresie dało się zrobić więcej, żeby dyskusję skoncentrować na ryzykach i potrzebie ochrony nie tyle danych, a ludzi, których te informacje dotyczą.

Natomiast patrząc na ostatni przegląd RODO i ocenę jego stosowania przez Komisję Europejską, Polska klasyfikuje się dość wysoko wśród społeczeństw, które świadome są istnienia przepisów i funkcjonowania krajowego organu ochrony danych. Teraz musimy, moim zdaniem, skupić się na ryzykach dla praw lub wolności m.in. wynikających ze stosowania nowych technologii, nowych procesów przetwarzania danych, czy stosowania "starych" technologii w nowych kontekstach.

I tutaj ważna kwestia dotycząca uprzednich konsultacji. Uważam, że nie sprzyjają im bardzo ogólne przepisy ustawy z 10 maja 2018 r. o ochronie danych osobowych. Myślę, że jest to jedna z tych kwestii, której należy przyjrzeć się bliżej. Być może jest przestrzeń, aby ten mechanizm stał się bardziej powszechny. Coroczne sprawozdania UODO wskazują, że niewielu administratorów składa wnioski o przeprowadzenie tych konsultacji. Chciałbym, aby i ta kwestia stała się przedmiotem dyskusji w naszym zespole i dialogu z Urzędem.

Co z działań innych organów nadzorczych uważa Pan za warte do wdrożenia w UODO?

Uważam, że powinniśmy znaleźć własną drogę. I zastanowić się co faktycznie – w naszej specyficznej sytuacji – może wpłynąć na poziom stosowania przepisów. Oczywiście czerpiąc wzorce z innych organów. Sądzę, że powinniśmy eliminować przeszkody "formalne" w stosowaniu przepisów. W naszym kraju niestety bardzo dużo czasu poświęca się, np. w sektorze publicznym, na kwestie formalne m.in. identyfikacji administratora danych. Zamiast skupić się na ryzykach dla praw lub wolności ludzi, których dane są przetwarzane. Dlatego ważne jest wyjaśnianie tych kwestii, które siłą rzeczy są bardzo "lokalne", ponieważ na ogół wynikają z niedostatecznego poziomu krajowej legalizacji. Świetnym przykładem jest implementacja przepisów dyrektywy o ochronie sygnalistów, która rodzi wiele kwalifikacyjnych problemów, np. co do grup kapitałowych, które niestety trzeba przesądzić, zanim przejdzie się do wdrażania realnych mechanizmów ochrony. Mam wrażenie, że w naszym kraju cały czas pokutuje podejście, że przyjęcie procedur w magiczny sposób samo w sobie załatwi problem ochrony danych.

Uważam, że powinniśmy także publikować więcej przykładów i wzorów dokumentów, np. w zakresie oceny ryzyka. Podoba mi się także podejście hiszpańskiego organu nadzorczego (AEPD), który stworzył osobny portal dotyczący innowacji i technologii.

1 ROZMOWA Z EKSPERTEM

Jest też kilka pomysłów, które dotyczą wzmacniania aspektu cyberbezpieczeństwa, które powstały w ramach dyskusji pomiędzy naszym zespołem i Prezesem oraz pracownikami Urzędu. Nie chcę na razie ujawniać szczegółów, ponieważ to jest jeszcze wczesna faza koncepcyjna, ale w ciągu kilku tygodni taka informacja z pewnością pojawi się na stronie internetowej Urzędu.

Podczas konferencji z udziałem kandydatów na funkcję Prezesa UODO powiedział Pan, że: „skupiamy się na abstrakcyjnych pojęciach danych osobowych, natomiast zapominamy o tym, że cały czas mówimy o ludziach". Jednocześnie jako czynny radca prawny stoi Pan niekiedy po drugiej stronie barykady reprezentując w sądach interesy biznesu. Jak można pogodzić te dwa interesy?

Takie stwierdzenie pojawiało się w czasie kandydowania jako zarzut nie tylko w stosunku do mnie, ale też innych kandydatów. To jest oczywiste, że radca prawny czy adwokat występujący jako pełnomocnik swojego klienta, musi działać w jego interesie. I to nie jest "widzimisię" pełnomocnika, tylko jego obowiązek, który wynika z zasad etyki i którego naruszenie stanowić może podstawę odpowiedzialności. W swojej praktyce zajmuję się nie tylko reprezentowaniem administratorów, ale także podmiotów danych w ramach postępowań dotyczących zgłaszanych skarg. To pozwala zrozumieć obie strony potencjalnych sporów.

Studia prawnicze i kolejne szczeble edukacji, czy aplikacja potrzebne są, żeby rozumieć swoją rolę w różnych kontekstach. Czym innym jest reprezentacja klientów, a czym innym działalność, np. naukowa czy doradcza w ramach zespołów, które działają – jak nasz – jako doradcy społeczni.

To oczywiście nie wyklucza całkowicie możliwości wystąpienia konfliktu interesów. Dlatego uznaliśmy razem z prezesem Wróblewskim, że w zarządzeniu o powołaniu naszego zespołu powinien się pojawić zapis wskazujący na konieczność unikania takich sytuacji. Każdy z członków zespołu zobowiązał się do tego, aby ich unikać, a jeżeli mogą wystąpić, to jasno o nich komunikować.

Dziękuję za rozmowę.

PUBLIKACJA DANYCH OSOBOWYCH ABSOLWENTÓW UCZELNI W KSIĘDZE JUBILEUSZOWEJ

Tylko zgoda uprawnia szkołę wyższą do publikacji imion i nazwisk absolwentów oraz roku ukończenia przez nich studiów w księdze pamiątkowej wydawanej z okazji jubileuszu uczelni.

Trudności z pozyskaniem zgody absolwentów – zwłaszcza ze względu na upływ czasu – powodują, że szkoły wyższe starają się znaleźć inną podstawę uprawniającą je do publikacji wymienionych danych.

Podnoszą np., że jednymi z realizowanych przez uczelnie oraz inne instytucje badawcze celów wskazanych w preambule do ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce są przyczynianie się do rozwoju kultury i współkształtowanie standardów moralnych obowiązujących w życiu publicznym. Przyjmują, że promocja dorobku uczelni i prezentacja jej absolwentów służy tym celom. Zatem publikacja informacji o absolwentach to działanie w interesie publicznym, a więc z zastosowaniem przesłanki, o której mowa w art. 6 ust. 1 lit. e ogólnego rozporządzenia o ochronie danych (RODO). Tymczasem…

… nie tędy droga.

Prawo o szkolnictwie wyższym i nauce, stanowiące podstawę funkcjonowania szkół wyższych, nie przewiduje możliwości publikacji danych osobowych absolwentów. Tym samym uczelnia nie może powołać się na przesłankę, o której mowa w art. 6 ust. 1 lit. c RODO, która zezwala na przetwarzanie danych, jeśli jest to niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.

Zastosowania nie ma również przesłanka określona w art. 6 ust. 1 lit. e RODO, umożliwiająca przetwarzanie danych, gdy jest ono niezbędne do wykonania zadania realizowanego w interesie publicznym. Nie są bowiem spełnione odpowiednie warunki. Kluczowe w tym przypadku jest bowiem ustalenie, czy zachodzi kryterium „niezbędności" przetwarzania danych osobowych dla wykonania zadania realizowanego w interesie publicznym. Przesłanka „interesu publicznego" musi być rozpatrywana w powiązaniu z określoną w art. 51 ust. 2 Konstytucji RP zasadą pozyskiwania przez władze publiczne informacji od obywateli tylko w takim zakresie, w jakim jest to niezbędne w demokratycznym państwie prawa. Kryterium interesu publicznego musi być więc zawsze powiązane i wyważone z interesem poszczególnych osób, których dane dotyczą.

W tym kontekście warto odwołać się zarówno do wyroku Trybunału Sprawiedliwości Unii Europejskiej (TSUE) z 16 grudnia 2008 r. w sprawie C-524/06, Heinz Huber v. Bundesrepublik Deutschland, jak i do stanowiska doktryny odnoszącego się do omawianego zagadnienia.

Wynika z nich, że „przesłanki niezbędności w relacji do realizacji zadań publicznych nie można interpretować rozszerzająco, zaś sposób przetwarzania powinien być adekwatny do realizowanego celu i będzie taki wyłącznie wówczas, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami.” (D. Lubasz, W. Chomiczewski [w:] RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. E. Bielak-Jomaa, Warszawa 2018, art. 6. (dostęp: 2024-05-23 11:29).

Promocja osiągnięć szkoły wyższej jest ogólnym celem przetwarzania danych wywiedzionym z preambuły Prawa o szkolnictwie wyższym.

Cel ten może zostać osiągnięty na wiele sposobów

- bez użycia danych osobowych absolwentów - albo za zgodą absolwentów na przetwarzanie danych osobowych. Dlatego nie można uznać zamieszczenia w przestrzeni publicznej bez wiedzy i zgody absolwentów ich danych osobowych w postaci imienia i nazwiska oraz roku ukończenia szkoły wyższej za działanie niezbędne dla promowania osiągnięć szkoły wyższej, i co za tym idzie za działanie adekwatne w myśl zasady minimalizacji danych (art. 5 ust. 1 lit. c RODO).

Należy również dodać, że TSUE w swoich stanowiskach wielokrotnie wskazywał na ryzyka związane z pozostawianiem danych osobowych w przestrzeni publicznie dostępnej, jaką jest internet. Wielokrotnie podkreślał konieczność ważenia niezbędności takich działań ze względu na liczne ryzyka, jakie wiążą się z ponownym wykorzystaniem tych danych poza kontrolą dotychczasowego administratora w różnych celach. Jako przykłady można wskazać:

- wyrok TSUE z 8 grudnia 2022 r. w sprawie C-460/20 U, RE v. Google LLC czy też
- wyrok TSUE z 14 grudnia 2023 r. w sprawie C-456/22 VX, AT v. Gemeinde Ummendorf.

Warto też podkreślić, że informacja o dacie ukończenia szkoły wyższej może w pośredni sposób wskazywać na wiek absolwenta – tak więc publikacja danych osobowych wiązałaby się z możliwością udostępnienia dodatkowych danych osobowych.

Należy również zaznaczyć, że problem z dotarciem do absolwentów w celu pozyskania zgody, będzie również rodził

problem z realizacją wobec tych osób obowiązku informacyjnego,

o którym mowa w art. 13 i 14 RODO.

2 UODO SYGNALIZUJE

Warunki, które muszą być spełnione, by możliwe było ograniczenie praw osób, których dane dotyczą, są ściśle określone w art. 23 ust. 1 RODO. Nie można uznać, że w omawianym przypadku będziemy mieli do czynienia z przesłanką z art. 23 ust. 1 lit. e RODO – przetwarzanie służy innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu.

Upublicznienie danych osobowych absolwentów należy również uznać za

zmianę celu przetwarzania

danych osobowych, gdyż zostały one pierwotnie pozyskane w celu prowadzenia kształcenia na określonym kierunku studiów. Zmiana celu przetwarzania jest dopuszczalna na zasadach określonych w art. 6 ust. 4 RODO. Wyraźnie podkreśla się w nim konieczność powiązania nowego celu przetwarzania z celami określonymi w art. 23 ust. 1 RODO, w przypadku gdy przesłanką zmiany celu nie jest zgoda osoby.

Pod uwagę trzeba wziąć też rozporządzenie Rady Ministrów z dnia 22 czerwca 2011 r. w sprawie sposobu i trybu udostępniania materiałów archiwalnych znajdujących się w archiwach wyodrębnionych. Wyraźnie wynika z niego, że

nie ma podstaw do automatycznego udostępniania danych osobowych znajdujących się w archiwach wyodrębnionych.

Udostępnienie tych danych musi być powiązane ze spełnieniem ściśle określonych warunków określonych w tym akcie prawnym.

Reasumując,

w związku z unormowaniami ustawy – Prawo o szkolnictwie wyższym i nauce, a także w obliczu zmiany pierwotnych celów, w jakich dane absolwentów miałyby być wykorzystywane, przesłanką uzasadniającą upublicznienie danych absolwentów uczelni wyższej z okazji jej jubileuszu może być wyłącznie zgoda osoby w rozumieniu art. 6 ust. 1 lit. a RODO.

JAK LEKARZ POWINIEN WYWOŁYWAĆ PACJENTÓW OCZEKUJĄCYCH NA WIZYTĘ?

Wezwanie pacjenta do gabinetu powinno odbywać się tak, by zapewnić poufność jego danych osobowych. Do przestrzegania tej zasady personel medyczny zobowiązują zarówno ogólne rozporządzenie o ochronie danych (RODO), jak i przepisy branżowe.

Przepisy ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta oraz przepisy szczególne odnoszące się do sektora medycznego nie regulują kwestii sposobu wywoływania pacjenta przed wizytą lekarską. W związku z tym stosować należy ogólne zasady ochrony danych osobowych określone w RODO. Jedną z nich jest zasada integralności i poufności (art. 5 ust. 1 lit. f RODO). Stanowi ona, że dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie ich bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. Wezwanie pacjenta do gabinetu powinno więc odbywać się tak, by zapewnić poufność jego danych osobowych.

Tajemnica zawodowa

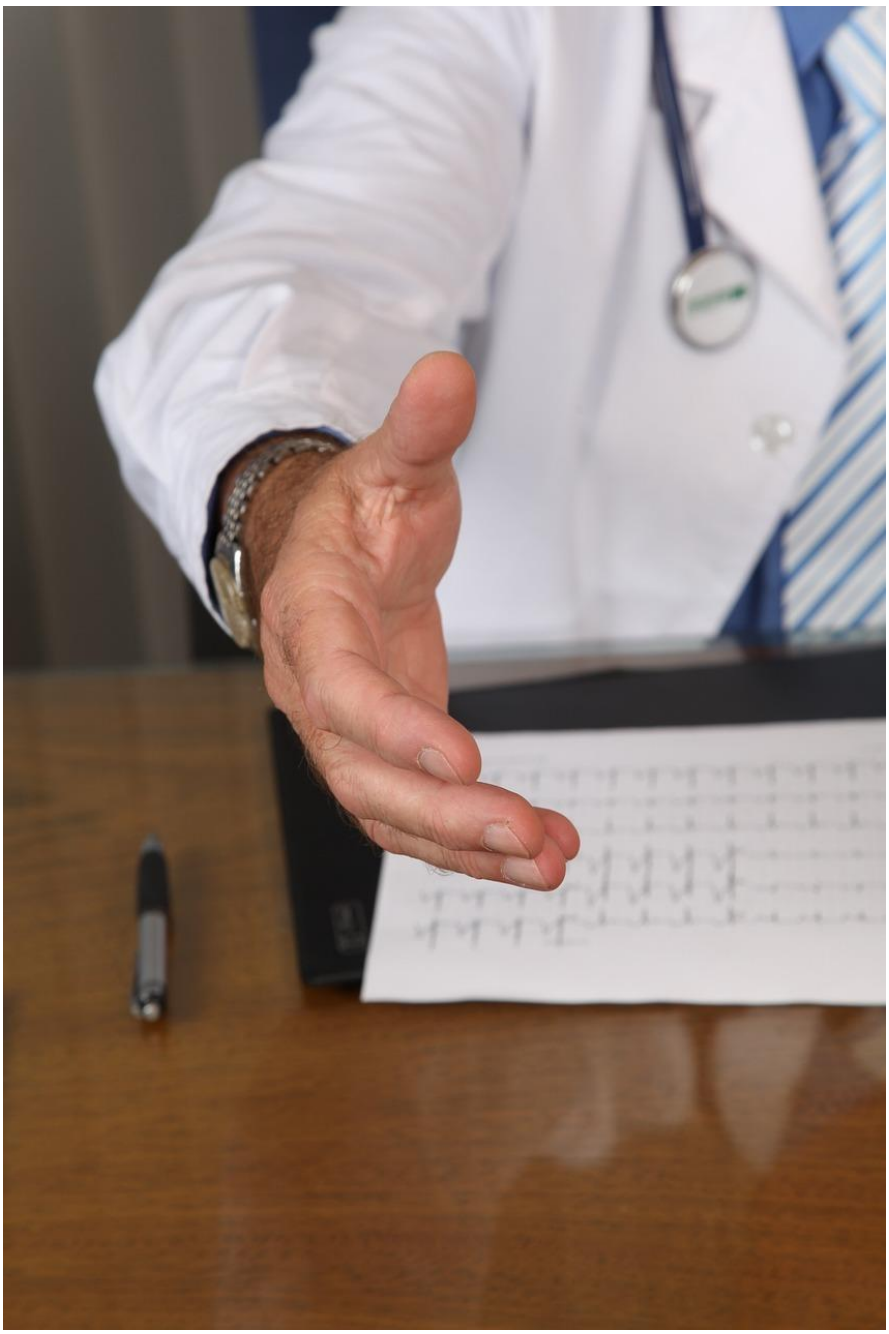
Jednocześnie pod uwagę należy brać przepisy ustanawiające tajemnicę zawodową obowiązującą osoby wykonujące zawody medyczne oraz ustanawiające prawo pacjenta do prywatności. Zgodnie z art. 40 ust. 1 ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty, lekarz ma obowiązek zachowania w tajemnicy informacji związanych z pacjentem, a uzyskanych w związku z wykonywaniem zawodu. Podobnie regulacje zawiera ustawa z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej. Stosownie do jej art. 17 ust. 1, pielęgniarka i położna są obowiązane do zachowania w tajemnicy informacji związanych z pacjentem, uzyskanych w związku z wykonywaniem zawodu.

Prawo pacjenta do prywatności

Istotne znaczenie mają także przepisy ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. Stanowią one (art. 20 ust. 1), że pacjent ma prawo do poszanowania intymności i godności, w szczególności w czasie udzielania mu świadczeń zdrowotnych.

Reguły obowiązujące placówki, które przystąpiły do kodeksu postępowania

W sektorze opieki zdrowotnej niektóre placówki udzielające świadczeń medycznych zobowiązały się do stosowania kodeksów postępowania regulujących przetwarzanie danych osobowych. Są one zatwierdzone przez Prezesa UODO i dostępne m.in. na stronie internetowej Urzędu. W jednym z nich, tj. w Kodeksie postępowania dla sektora ochrony zdrowia, można znaleźć wytyczne dotyczące sposobu wywoływania pacjenta do gabinetu przed wizytą lekarską (załącznik nr 3, s. 74). Należy jednak podkreślić, że postanowienia wymienionego kodeksu nie są wiążące dla wszystkich podmiotów medycznych, lecz tylko tych, które zobowiązały się do jego stosowania.



fot. pixabay

WE WRZEŚNIU KOLEJNE WEBINARIUM NA TEMAT CERTYFIKACJI

Podsumowaniu dotychczasowych sześciu webinariów z serii „Certyfikacja w ochronie danych" i wyjaśnieniu pojawiających się wątpliwości w tym zakresie służyć ma kolejne tego typu spotkanie zaplanowane na wrzesień br.

Od grudnia 2023 r. do maja 2024 r. UODO co miesiąc organizował webinaria, których celem jest promowanie certyfikacji i zachęcanie rynku do tworzenia mechanizmów certyfikacji zgodnie z art. 42 RODO.

Certyfikacja to nowe i niezwykle ważne narzędzie, które może ułatwić administratorom i podmiotom przetwarzającym wykazanie zgodności z ogólnym rozporządzeniem o ochronie danych, a osobom, których dane osobowe będą przetwarzane, szybko ocenić stopień ich ochrony.

Zanim jednak administratorzy i podmioty przetwarzające będą mogli uzyskać certyfikaty potwierdzające zgodność ich procesów przetwarzania danych z RODO, musi powstać rynek, na którym będzie można się o nie ubiegać.

Przybliżeniu wszystkich aspektów związanych procesem certyfikacji służą prowadzone przez UODO webinaria. Nagrania z odbytych już spotkań, podczas których zostały omówione m.in. podstawowe przepisy i pojęcia dotyczące certyfikacji, a także wyjaśniono, czym jest mechanizm certyfikacji i jak przebiega procedura zatwierdzania kryteriów certyfikacji, dostępne są na stronie internetowej Urzędu w zakładce Działania edukacyjne UODO w zakresie certyfikacji.

O tym, jakie kwestie powinny być poruszone podczas kolejnego spotkania, mogą Państwo zdecydować, przesyłając – do 31 sierpnia br. – e-mail z pytaniami/tematami do sekretariatu Departamentu Orzecznictwa i Legislacji (dol@uodo.gov.pl), w temacie wiadomości wpisując „Certyfikacja – wrześniowe webinarium".

Szczegółowe informacje na temat daty oraz agendy wrześniowego webinarium z serii „Certyfikacja w ochronie danych" – odbywającego się tradycyjnie w formule online – zostaną opublikowane w terminie późniejszym na stronie internetowej UODO.

Zapraszamy do zapoznania się z nagraniami z dotychczasowych spotkań, zgłaszania zagadnień wymagających omówienia oraz do udziału we wrześniowym webinarium.

SPRAWA KORESPONDENCJI W SPRAWIE PSÓW BIEGAJĄCYCH PO DRODZE. UPOMNIENIE PUODO

Jeśli obywatel zgłasza sprawę i instytucja publiczna podejmuje ją z urzędu, nie ma żadnego powodu, by w swojej korespondencji ujawniała dane zgłaszającego.

Mieszkanka gminy C. poskarżyła się Prezesowi UODO na swojego wójta za to, że w korespondencji z jej sąsiadem użył jej danych (nazwiska i adresu).

Wójt przetwarzał dane osobowe Skarżącej w związku z jej licznymi zgłoszeniami dotyczącymi nieprawidłowości w realizacji ustawy o ochronie zwierząt.

Chodziło o psy tego sąsiada. Mieszkanka gminy C. uważała, że jej zagrażają, bo chodzą po drodze bez opieki. Wójt uznał, że mogło dojść do złamania przepisów ustawy o ochronie zwierząt. Zabrania ona puszczania psów bez możliwości ich kontroli i bez oznakowania umożliwiającego identyfikację właściciela lub opiekuna. Wójt napisał więc do właściciela psów, podając w dopisku, że pismo to dostaje też do wiadomości pani, która się na psy skarżyła (i podał tam jej adres).

Wyjaśnił, że przetwarzanie danych osobowych Skarżącej odbyło się w celu wypełnienia obowiązku prawnego wynikającego z art. 11 ust. 1 ustawy o ochronie zwierząt, zgodnie z którym zapobieganie bezdomności zwierząt należy do zadań własnych gminy. Przetwarzanie danych osobowych Skarżącej służyło ponadto ochronie jej żywotnych interesów. Celem przetwarzania było pouczenie sąsiada Skarżącej o jego obowiązkach jako właściciela psów.

Wójt dodał: „Nadto umieszczenie rozdzielnika, co być może było niewłaściwe i dokonane wskutek przeoczenia, mogło uwiarygodniać informację o tym, iż [obywatel] narusza zakaz wynikający z art. 10a ust. 3 ustawy o ochronie zwierząt".

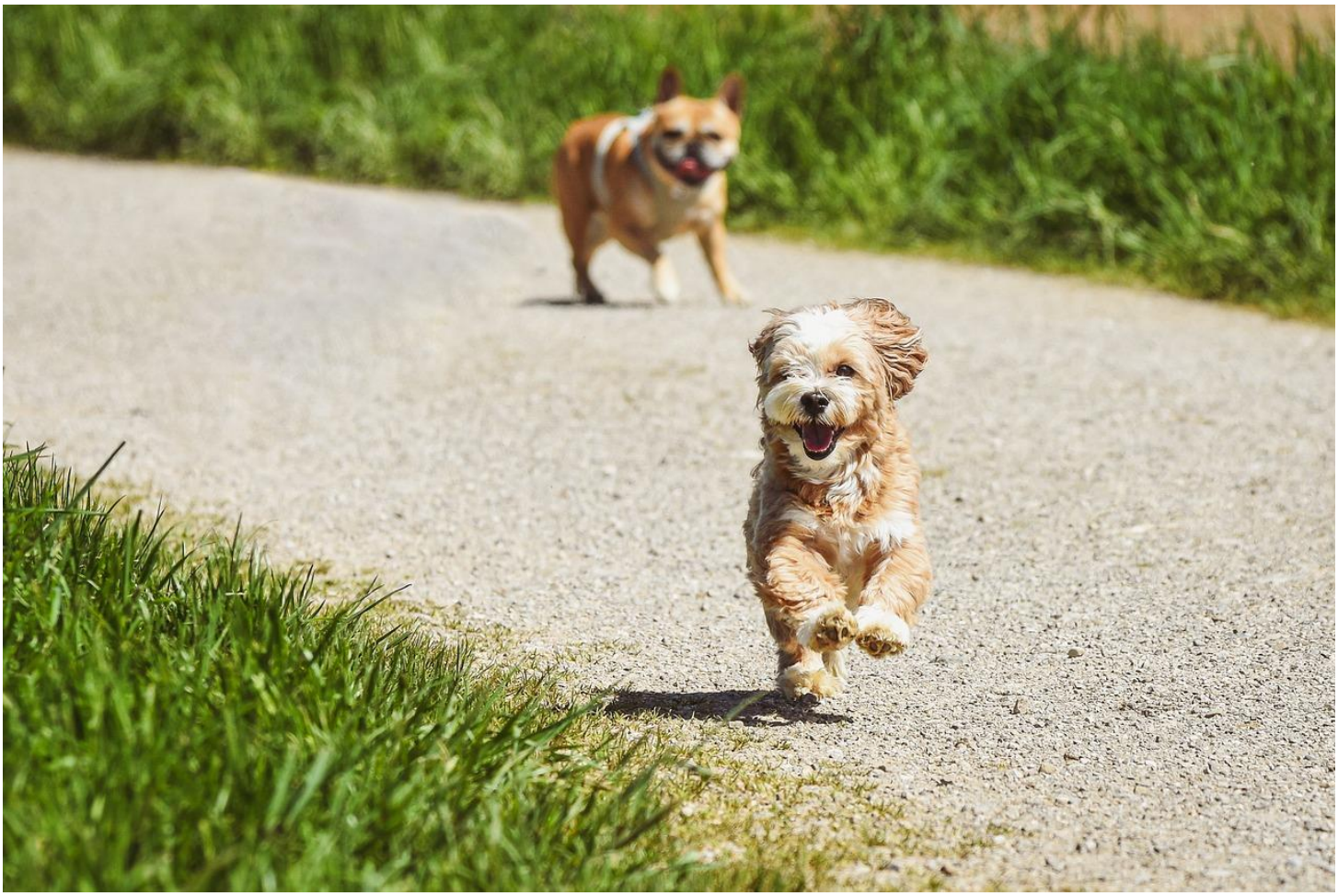
Podjęcie przez Skarżącą działań, które zainicjowały realizację obowiązków gminy wynikających z ustawy o ochronie praw zwierząt, nie uzasadniało późniejszego zamieszczenia jej danych w piśmie skierowanym do właściciela zwierząt, który zdaniem gminy nie wypełniał tych obowiązków. Wskazać należy, że działania Skarżącej stanowiły realizację jej uprawnień obywatelskich i nie wykluczały ochrony prawa do prywatności, ani też jej praw wynikających z przepisów o ochronie danych osobowych.

3 WYBRANE DECYZJE UODO

Prezes UODO zauważył, że pouczenie właściciela psów o obowiązkach nie wymagało, by uzupełniać go o dane Skarżącej. Także żaden z przepisów Kpa nie nakazuje umieszczania w korespondencji rozdzielnika z danymi osób, do których kierowane jest pismo.

Ujawniając dane osobowe Skarżącej wójt postąpił więc niewłaściwie. Stąd upomnienie.

Sygnatura sprawy: DS.523.4084.2022



fot. pixabay

RUSZYŁY PRACE NAD NOWYM PORADNIKIEM DOTYCZĄCYM NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

21 czerwca 2024 r. zakończyły się otwarte konsultacje w sprawie poradnika „Obowiązki administratorów związane z naruszeniami ochrony danych osobowych". Uwagi do jego treści zgłosiło aż 21 podmiotów. Przedstawiciele UODO oraz Społecznego Zespołu Ekspertów przy Prezesie UODO rozpoczęli już wspólne prace, których celem jest aktualizacja poradnika.

Wskazówki dla administratorów

W połowie 2019 r. UODO opublikował specjalny materiał informacyjny mający wesprzeć administratorów w realizacji nowych obowiązków związanych z naruszeniami ochrony danych osobowych. Zawierał on szereg wskazówek przygotowanych przez pracowników organu nadzorczego na podstawie doświadczeń z pierwszego roku stosowania RODO.

Poradnik okazał się przydatnym narzędziem dla wielu zainteresowanych. Pomógł on uporządkować dostępną wówczas wiedzę na temat tego typu zdarzeń oraz rozwiać liczne wątpliwości związane ze stosowaniem rozporządzenia w praktyce.

Czas na zmiany

Po pięciu latach od publikacji, UODO przeprowadził otwarte konsultacje, zachęcając wszystkich interesariuszy do wyrażenia swoich opinii na temat materiału. Decyzja ta spotkała się z szerokim zainteresowaniem, które zaowocowało zaangażowaniem się w dyskusję zarówno osób fizycznych, jak i przedstawicieli administracji, organizacji pozarządowych oraz biznesu.

Zaprezentowane spostrzeżenia i sugestie pokazują, że rewizja poradnika jest potrzebna i oczekiwana. Rozwój technologii, zmiany w prawie oraz wiele wciąż aktualnych wątpliwości interpretacyjnych przyczyniają się do konieczności ponownego sformułowania przez organ nadzorczy wskazówek dotyczących postępowania w przypadku naruszeń ochrony danych osobowych.

Prace nad poradnikiem ruszyły

Chcąc wyjść naprzeciw potrzebom administratorów, przedstawiciele UODO we współpracy z członkami Społecznego Zespołu Ekspertów przy Prezesie UODO rozpoczęli prace nad analizą

otrzymanych wiadomości oraz dostosowaniem treści poradnika do współczesnych wyzwań.

Organ nadzorczy odniesie się także do zgromadzonych uwag w nadchodzącym komunikacie.

fot. Spotkanie przedstawicieli Społecznego Zespołu Ekspertów przy PUODO, który wspiera Urząd w pracach nad aktualizacją poradników
materiał własny UODO

NOWE TECHNOLOGIE W MOTORYZACJI: PRZYSZŁOŚĆ MOBILNOŚCI A OCHRONA DANYCH

Motoryzacja przechodzi rewolucyjne zmiany napędzane dynamicznym rozwojem nowych technologii. Nowoczesne pojazdy są teraz wyposażone w zaawansowane systemy elektroniczne, sztuczną inteligencję oraz technologie komunikacyjne, które nie tylko podnoszą komfort i bezpieczeństwo jazdy, ale także kształtują przyszłość mobilności. Jednak wraz z postępem technologicznym pojawiają się również wyzwania związane z ochroną danych i prywatności użytkowników. W erze cyfryzacji i globalnej sieci konieczne staje się wypracowanie nowych standardów i regulacji, które zagwarantują bezpieczeństwo informacji, nie hamując jednocześnie innowacyjnego rozwoju.

„Connected car" krokiem w stronę rewolucji w motoryzacji?

Aby dzieci były bezpieczne, dorośli powinni zdobyć podstawową wiedzę o ich funkcjonowaniu w sieci. Pierwszym krokiem jest zrozumienie potencjalnych zagrożeń. Cyberprzestępczość, cyberprzemoc, niewłaściwe treści, czy narażenie na nadmierną reklamę to tylko niektóre z nich. Ważne jest, by rodzice

Współczesne samochody zbierają ogromne ilości danych, często przekraczające pół miliona gigabajtów na godzinę. Dane te mogą obejmować lokalizację, zachowania kierowcy, parametry techniczne pojazdu, informacje z kamer i czujników, szczegóły dotyczące podróży, a także dane z systemów połączonych, takie jak historia wyszukiwania, połączeń czy polecenia głosowe.

Może to znacząco zwiększyć bezpieczeństwo, efektywność i komfort jazdy. Dzięki wymianie danych z otoczeniem samochody mogą ostrzegać kierowców o zagrożeniach, optymalizować trasy oraz oferować różnorodne usługi, jak rezerwacje parkingów czy płatności bezgotówkowe. Jednak wraz z tymi możliwościami pojawia się istotne wyzwanie: ochrona danych osobowych.

„Pojazdy podłączone do internetu generują coraz większe ilości danych, z których większość można uznać za dane osobowe, gdyż dotyczą kierowców lub pasażerów. Nawet jeśli dane zgromadzone przez samochód podłączony do internetu nie są bezpośrednio powiązane z nazwiskiem danej osoby, z technicznymi aspektami i funkcjami pojazdu, będą one dotyczyły kierowcy lub pasażerów samochodu. Na przykład dane odnoszące się do stylu jazdy lub pokonanej odległości, dane związane

z zużyciem części pojazdu, dane dotyczące lokalizacji lub dane gromadzone przez kamery mogą dotyczyć zachowania kierowcy, a także informacji o innych osobach, które mogą znajdować się w pojeździe lub przechodzić obok. Takie dane techniczne generuje osoba fizyczna i umożliwiają jej bezpośrednią lub pośrednią identyfikację przez administratora danych lub przez inną osobę."

Źródło: Wytyczne EROD 01/2020 dotyczące przetwarzania danych osobowych w kontekście pojazdów podłączonych do Internetu i aplikacji związanych z mobilnością

A co z danymi biometrycznymi?

Niektóre dane wygenerowane przez pojazdy podłączone do internetu mogą również wymagać szczególnej uwagi ze względu na ich wrażliwy charakter lub potencjalny wpływ na prawa i interesy osób, których dane dotyczą. Wśród nich wymienia się

- dane dotyczące lokalizacji,
- dane, które mogłyby ujawniać popełnienie przestępstwa lub naruszenie przepisów ruchu drogowego,
- a także dane biometryczne (oraz wszelkie szczególne kategorie danych osobowych określone w art. 9 RODO).

Te ostatnie stają się coraz bardziej powszechne, w miarę jak producenci samochodów wprowadzają nowe technologie. Mogą one obejmować informacje takie jak

- odciski palców,
- rozpoznawanie twarzy,
- skanowanie tęczówki oka,
- oraz monitorowanie pulsu i oddechu.

Te zaawansowane systemy oferują szereg korzyści, ale również niosą ze sobą istotne wyzwania i ryzyka, zwłaszcza w kontekście prywatności i bezpieczeństwa danych.

Po pierwsze, technologie biometryczne są w stanie znacznie poprawić bezpieczeństwo pojazdów. Na przykład, systemy rozpoznawania twarzy mogą być używane do autoryzacji dostępu do pojazdu, co zmniejsza ryzyko kradzieży.

Skanery linii papilarnych mogą być używane do uruchamiania silnika, a monitorowanie biometryczne może wykrywać oznaki zmęczenia lub złego samopoczucia kierowcy, ostrzegając go o potrzebie odpoczynku.

Jednak wprowadzenie danych biometrycznych do samochodów wiąże się również z poważnymi wyzwaniami. Głównym problemem jest ochrona prywatności. Dane biometryczne są wyjątkowo wrażliwe i unikalne dla każdej osoby, co oznacza, że ich wyciek może mieć poważne konsekwencje. Niewystarczające zabezpieczenia danych biometrycznych mogą prowadzić do ich kradzieży

.

i nieuprawnionego użycia, co może skutkować kradzieżą tożsamości lub innymi formami nadużyć.

Dlatego niezwykle ważne jest, aby producenci samochodów stosowali zaawansowane metody szyfrowania, które skutecznie chronią nasze dane.

Pojawia się też pytanie o to, kto ma dostęp do tych danych i w jaki sposób są one przechowywane oraz wykorzystywane. Kierowcy powinni mieć pełną kontrolę nad swoimi danymi i możliwość ich usunięcia, jeśli zdecydują się zmienić pojazd lub po prostu nie chcą już korzystać z technologii biometrycznych.

Niestety, wielu producentów samochodów oferuje kierowcom ograniczoną kontrolę nad swoimi danymi, co jest niepokojące. Istotne jest, abyśmy dokładnie zapoznawali się z politykami prywatności producentów i wybierali tych, którzy zapewniają większą transparentność oraz możliwość zarządzania naszymi danymi.

Konieczne jest również zapewnienie alternatywnej metody dostępu, która nie opiera się na biometrii (np. fizyczny klucz lub kod), bez wprowadzania dodatkowych ograniczeń, co oznacza, że użycie danych biometrycznych nie powinno być obowiązkowe.

Należy również podkreślić, że producenci samochodów mają różne podejścia do ochrony danych. Istnieją znaczące różnice w zakresie zabezpieczeń i polityk prywatności – jako użytkownicy powinniśmy być świadomi tych różnic i wybierać pojazdy, które najlepiej odpowiadają naszym oczekiwaniom w zakresie ochrony prywatności.

RODO i inne regulacje

W Europie ochrona danych osobowych jest regulowana przez Rozporządzenie Ogólne o Ochronie Danych Osobowych (RODO). Wprowadza ono wymogi dotyczące gromadzenia, przetwarzania i przechowywania danych osobowych, co ma na celu ochronę prywatności użytkowników i zapewnienie im większej kontroli nad swoimi danymi.

Przede wszystkim administratorzy danych muszą zapewnić, aby cele przetwarzania danych były konkretne, wyraźne i prawnie uzasadnione. Dane nie mogą być przetwarzane w sposób niezgodny z pierwotnym celem ich zbierania, a każda operacja przetwarzania musi opierać się na ważnej podstawie prawnej.

Użytkownicy muszą wyrazić zgodę na przetwarzanie ich danych osobowych. Tylko wtedy dane mogą być legalnie przetwarzane. Ważne jest, aby ta zgoda była dobrowolna, świadoma i jednoznaczna.

5 NOWE TECHNOLOGIE

Zaleca się również, aby przetwarzanie danych odbywało się lokalnie, a więc dane powinny być przetwarzane wewnątrz pojazdu, bez przekazywania ich na zewnątrz, o ile to możliwe. Ma to na celu minimalizowanie ryzyka związanego z transferem danych.

Użytkownicy mają również prawo do bycia zapomnianymi, co oznacza, że mogą zażądać usunięcia swoich danych osobowych. Firmy muszą respektować te żądania i usuwać dane, gdy tylko nie są już potrzebne do pierwotnego celu.

Kluczowe jest również bezpieczeństwo danych, co oznacza, że firmy muszą stosować odpowiednie środki techniczne i organizacyjne, takie jak szyfrowanie kanałów komunikacyjnych, unikalne klucze kryptograficzne dla każdego pojazdu, regularne odnawianie tych kluczy oraz uwierzytelnianie urządzeń odbierających dane. Wszystko to ma na celu ochronę danych przed nieautoryzowanym dostępem, utratą czy zniszczeniem.

Równie ważna jest przejrzystość. Firmy muszą jasno informować użytkowników, jakie dane są zbierane i w jakim celu. Użytkownicy powinni mieć również bezpośredni dostęp do danych generowanych przez aplikacje w pojazdach.

Ochronę danych trzeba uwzględniać już na etapie projektowania systemów, a dane powinny być anonimizowane lub pseudonimizowane, zwłaszcza gdy są przekazywane poza pojazd. Minimalizacja danych, czyli ograniczenie zbierania danych do niezbędnego minimum, to kolejna ważna zasada.

Wreszcie w przypadku przetwarzania danych, które może wiązać się z wysokim ryzykiem naruszenia praw i wolności osób, konieczne jest przeprowadzenie oceny skutków dla ochrony danych.

Należy również wspomnieć, że Komisja Europejska pracuje nad stworzeniem solidnych i odpornych ram bezpieczeństwa dla urządzeń IoT i sieci, wprowadzając rygorystyczne standardy ochrony danych oraz mechanizmy szyfrowania. Współpracując z producentami i ekspertami ds. cyberbezpieczeństwa, dąży do ustanowienia jednolitych wytycznych na terenie całej Unii Europejskiej, aby zapewnić wysoki poziom ochrony konsumentów i zbudować zaufanie użytkowników do nowych technologii.

Rozwój technologii w motoryzacji niesie ze sobą ogromny potencjał, ale również wyzwania, zwłaszcza w kontekście ochrony danych. Wprowadzenie odpowiednich regulacji i standardów jest kluczowe dla zrównoważenia innowacji i prywatności. Jako użytkownicy nowoczesnych pojazdów, musimy być proaktywni w zarządzaniu naszymi danymi osobowymi. Powinniśmy edukować się na temat technologii używanych w naszych samochodach, regularnie aktualizować oprogramowanie pojazdów oraz wymagać od producentów lepszych standardów ochrony danych. Tylko w ten sposób możemy zapewnić sobie pełne bezpieczeństwo i ochronę naszej prywatności w dynamicznie rozwijającym się świecie motoryzacji.

EROD URUCHAMIA FRANCUSKĄ I NIEMIECKĄ WERSJĘ PRZEWODNIKA PO OCHRONIE DANYCH OSOBOWYCH DLA MAŁYCH PRZEDSIĘBIORSTW

Przewodnik zawiera praktyczne informacje dla MŚP na temat zgodności z RODO i korzyści z niej płynących w przystępnym i zrozumiałym języku.

Opracowanie narzędzi zapewniających praktyczne, łatwe do zrozumienia i przystępne wskazówki dotyczące ochrony danych jest kluczem do dotarcia do odbiorców niebędących ekspertami i strategicznym celem EROD.

Przewodnik EROD obejmuje różne aspekty RODO, od podstaw ochrony danych, po prawa osób, których dane dotyczą i środki zabezpieczające dane osobowe. Zawiera on filmy, infografiki, interaktywne schematy blokowe i inne praktyczne materiały, które mają pomóc MŚP w osiągnięciu zgodności z RODO.

W przyszłości przewodnik będzie dostępny w 15 kolejnych językach europejskich.

Źródło: komunikat EROD

fot. pexels

HISZPAŃSKI ORGAN NADZORCZY PRZYJĄŁ ŚRODEK TYMCZASOWY, KTÓRY UNIEMOŻLIWIŁ META WDROŻENIE FUNKCJI WYBORCZYCH

Hiszpański organ nadzorczy (AEPD) przyjął środek tymczasowy wobec Meta Platforms Ireland Limited, aby w związku z wyborami do Parlamentu Europejskiego, Meta natychmiastowo zawiesiła na terytorium Hiszpanii wdrażanie funkcji Election Day Information (EDI) i Voter Information Unit (VIU) oraz gromadzenie i przetwarzanie danych związanych z ich wykorzystaniem.

Za pośrednictwem tych dwóch funkcji, które polegają na dostarczaniu użytkownikom Facebooka i Instagrama informacji o wyborach do Parlamentu Europejskiego, Meta zamierzała przetwarzać dane osobowe, takie jak m.in. imię i nazwisko użytkownika, adres IP, wiek i płeć, czy informacje o sposobie interakcji z tymi funkcjami.

Funkcje te miały zostać uruchomione dla wszystkich użytkowników Meta, którym przysługuje prawo do głosowania w wyborach do Parlamentu Europejskiego w czerwcu 2024 r. (z wyjątkiem Włoch, których organ nadzorczy prowadzi już postępowanie w tej sprawie).

AEPD nakazał Meta zastosowanie się do środka tymczasowego, ponieważ uważa, że przetwarzanie danych przewidziane przez Meta jest sprzeczne z ogólnym rozporządzeniem o ochronie danych (RODO) i co najmniej naruszałoby zasady ochrony danych dotyczące zgodności z prawem, minimalizacji danych i zasady ograniczenia przechowywania.

AEPD uważa, że planowane przez Meta gromadzenie i przechowywanie danych stanowiłoby poważne zagrożenie dla praw i wolności użytkowników Instagrama i Facebooka, którzy odczuliby wzrost ilości gromadzonych na ich temat danych, co pozwoliłoby na tworzenie bardziej złożonych, szczegółowych i wyczerpujących profili oraz spowodowałoby bardziej inwazyjne przetwarzanie.

Udostępnienie danych osobowych osobom trzecim stanowiłoby nieproporcjonalną ingerencję w prawa i wolności osób, których dane dotyczą. Utrata kontroli pociąga za sobą wysokie ryzyko, że takie dane mogą zostać wykorzystane przez nieznanych administratorów i do celów, które nie zostały wyraźnie określone.

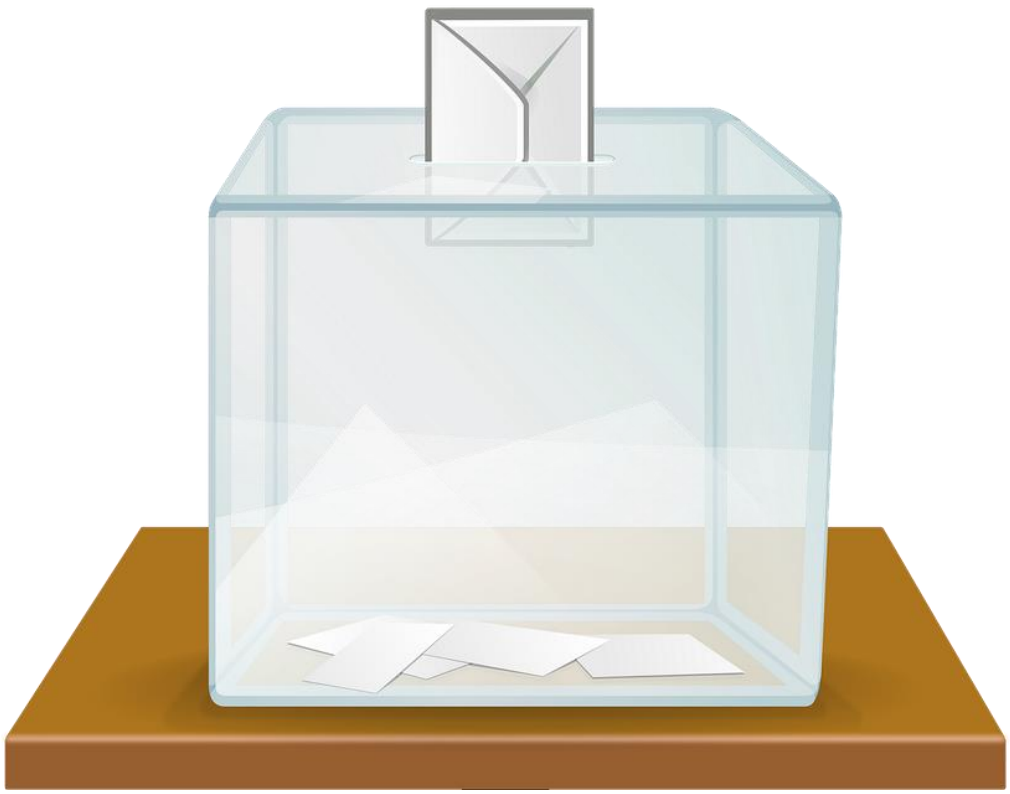
Komisja Europejska ogłosiła pod koniec kwietnia 2024 r., że wszczyna procedurę przeciwko Meta i zamierza przeanalizować między innymi takie aspekty jak dezinformacja, widoczność treści

politycznych i narzędzi monitorowania w okresie poprzedzającym wspomniane wybory, w ramach rozporządzenia o usługach cyfrowych.

Działanie AEPD odbywa się w ramach procedury ustanowionej w art. 66 ust. 1 RODO, która stanowi, że w wyjątkowych okolicznościach, gdy organ nadzorczy, którego sprawa dotyczy – w tym przypadku AEPD – uzna, że istnieje pilna potrzeba podjęcia działań w celu ochrony praw i wolności osób, których dane dotyczą, niezwłocznie przyjąć środki tymczasowe mające na terytorium jego państwa członkowskiego wywołać skutki prawne przez określony okres, nieprzekraczający trzech miesięcy.

W tym kontekście AEPD uznała, że przyjęcie pilnych środków tymczasowo zakazujących tych funkcji jest uzasadnione, aby zapobiec gromadzeniu danych, profilowaniu użytkowników i przekazywaniu ich danych stronom trzecim, zapobiegając w ten sposób wykorzystywaniu danych osobowych przez nieznanych administratorów i do celów, które nie zostały wyraźnie określone.

Źródło: komunikat hiszpańskiego organu nadzorczego



fot. pixabay

WORLDCOIN ZOBOWIĄZUJE SIĘ DO ZAPRZESTANIA DZIAŁALNOŚCI W HISZPANII

Po upływie okresu obowiązywania środka tymczasowego nałożonego przez hiszpański organ nadzorczy (AEPD), spółka zobowiązała się w sposób prawnie wiążący do niewznawiania działalności w Hiszpanii do końca roku lub do czasu wydania ostatecznej decyzji przez bawarski organ ochrony danych.

AEPD w marcu 2023 r. przyjęła środek tymczasowy, aby Tools for Humanity Corporation zaprzestała gromadzenia i przetwarzania danych osobowych, które prowadziła w Hiszpanii w ramach swojego projektu Worldcoin.

Tymczasem postępowania prowadzone przez Bayerisches Landesamt für Datenschutzaufsicht, niemiecki organ nadzorczy (Bawaria), gdzie spółka ma swoją główną jednostkę organizacyjną w Europie, są w toku i oczekuje się, że wkrótce zakończą się ostateczną decyzją dostosowaną do wszystkich organów nadzorczych, których sprawa dotyczy. W tym kontekście spółka podjęła prawnie wiążące zobowiązanie do niewznawiania działalności w Hiszpanii do końca roku lub do czasu przyjęcia przez niemiecki organ nadzorczy (Bawaria) ostatecznej decyzji w sprawie przetwarzania danych przez spółkę.

Środek tymczasowy, ustanowiony w art. 66 ust. 1 ogólnego rozporządzenia o ochronie danych (RODO) w celu ochrony praw i wolności osób, których dane dotyczą, został utrzymany w mocy przez hiszpański sąd Audiencia Nacional, uznając, że "zabezpieczenie interesu ogólnego polegającego na ochronie prawa do ochrony danych osobowych osób, których dane dotyczą, przeważało nad interesem spółki".

W następstwie środka tymczasowego nałożonego przez AEPD, spółka Tools for Humanity Corporation ogłosiła zmiany w swojej działalności, takie jak wprowadzenie kontroli weryfikacji wieku lub możliwość usunięcia kodu tęczówki.

AEPD współpracuje w tym zakresie z niemieckim organem nadzorczym (Bawaria), ponieważ ten ostatni jest organem wiodącym w tej sprawie, a AEPD jest organem którego sprawa dotyczy, zgodnie z RODO.

Źródło: komunikat hiszpańskiego organu nadzorczego

SZTUCZNA INTELIGENCJA: WSKAZÓWKI OD WŁOSKIEGO ORGANU NADZORCZEGO DOTYCZĄCE OCHRONY DANYCH OSOBOWYCH PRZED ZBIERANIEM DANYCH Z INTERNETU

Włoski organ nadzorczy opublikował wytyczne dotyczące ochrony danych osobowych przed zjawiskiem web scrapingu, czyli masowego zbierania danych osobowych z internetu. Dane te są publikowane przez administratorów danych w podmiotach publicznych i prywatnych, a zbierane przez osoby trzecie w celu szkolenia generatywnych modeli sztucznej inteligencji.

Dokument uwzględnia uwagi otrzymane przez organ w ramach postępowania, które zostało przeprowadzone w grudniu ubiegłego roku.

Oczekując na decyzję, w wyniku szeregu toczących się już postępowań, w tym przeciwko OpenAI (w sprawie legalności web scrapingu danych osobowych prowadzonego na podstawie uzasadnionego interesu), organ nadzorczy uznał za konieczne, przekazanie podmiotom publikującym dane osobowe w internecie w charakterze administratorów danych, pewnych wstępnych wskazówek dotyczących konieczności dokonania oceny potrzeby przyjęcia odpowiednich środków w celu zapobiegania lub przynajmniej utrudniania web scrapingu.

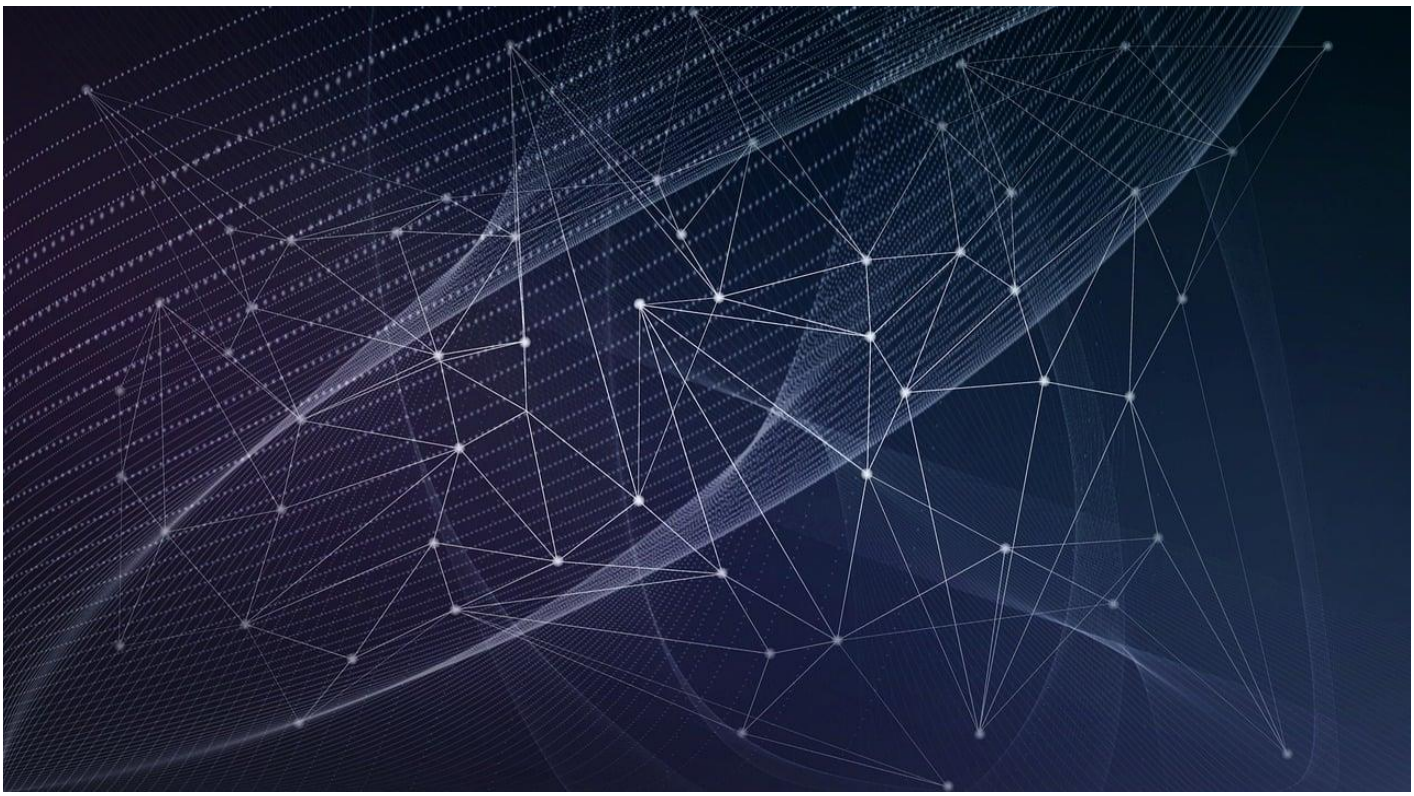
W dokumencie organ sugeruje konkretne środki, które należy podjąć. To:

- utworzenie obszarów zastrzeżonych, dostępnych tylko po rejestracji, w celu usunięcia danych z publicznej dostępności;
- włączenie klauzul zapobiegających zbieraniu danych do warunków świadczenia usług na stronach internetowych;
- monitorowanie ruchu na stronach internetowych w celu zidentyfikowania wszelkich nieprawidłowych przepływów danych przychodzących i wychodzących;
- konkretne interwencje dotyczące botów przy użyciu, między innymi, rozwiązań technologicznych udostępnianych przez te same firmy odpowiedzialne za web scraping.

Są to nieobowiązkowe środki, które administratorzy danych będą musieli ocenić, w oparciu o zasadę rozliczalności, czy wdrożyć w celu zapobiegania lub łagodzenia, w sposób selektywny,

skutków web scrapingu, biorąc pod uwagę szereg elementów: stan techniki, koszty wdrożenia, zwłaszcza dla MŚP.

Źródło: komunikat włoskiego organu nadzorczego



fot. pixabay

KOMISJA WYZNACZA TEMU JAKO BARDZO DUŻĄ PLATFORMĘ INTERNETOWĄ (VERY LARGE ONLINE PLATFORM – VLOP) ZGODNIE Z AKTEM O USŁUGACH CYFROWYCH

Temu to platforma sprzedażowa ze średnią liczbą ponad 45 milionów użytkowników miesięcznie w Unii Europejskiej (dane Temu). Ta liczba użytkowników zgodnie z Aktem o usługach cyfrowych (DSA) oznacza, że Temu będzie traktowana w Europie jak duża platforma internetowa (VLOP).

Po wskazaniu jako VLOP, Temu będzie musiało przestrzegać najbardziej rygorystycznych zasad wynikających z DSA. Obowiązek ten wejdzie w życie w ciągu czterech miesięcy od powiadomienia (tj. do końca września 2024 r.). Zasady dla VLOP to: obowiązek należytej oceny i ograniczenia wszelkich ryzyk systemowych wynikających z ich usług, w tym wystawiania na sprzedaż i sprzedaży podrobionych towarów, niebezpiecznych lub nielegalnych produktów oraz przedmiotów naruszających prawa własności intelektualnej.

Te dodatkowe obowiązki obejmują w szczególności:

Bardziej staranny nadzór nad nielegalnymi produktami

- Temu musi starannie przeanalizować konkretne ryzyko systemowe w odniesieniu do rozpowszechniania nielegalnych treści i produktów oraz projektowania lub funkcjonowania swojej usługi i powiązanych z nią systemów. Sprawozdania z oceny ryzyka będą musiały być dostarczane Komisji 4 miesiące po powiadomieniu o formalnym wyznaczeniu, a następnie raz w roku.
- Temu musi wdrożyć środki ograniczające ryzyko, takie jak wystawianie na sprzedaż i sprzedaż podrobionych towarów, niebezpiecznych produktów i przedmiotów naruszających prawa własności intelektualnej. Środki te mogą obejmować dostosowanie warunków świadczenia usług, ulepszenie projektu interfejsu użytkownika w celu lepszego zgłaszania i wykrywania podejrzanych ofert, usprawnienie procesów moderacji w celu szybkiego usuwania nielegalnych przedmiotów oraz udoskonalenie algorytmów w celu zapobiegania promocji i sprzedaży zabronionych towarów.
- Temu musi wzmocnić swoje wewnętrzne procesy, zasoby, testy, dokumentację i nadzór nad wszelkimi działaniami związanymi z wykrywaniem ryzyka systemowego.

6 SPRAWY MIĘDZYNARODOWE

Wzmocnione środki ochrony konsumentów

- Coroczne raporty oceny ryzyka sporządzane przez Temu muszą oceniać wszelkie potencjalne negatywne skutki dla zdrowia i bezpieczeństwa konsumentów, z naciskiem na fizyczne i psychiczne samopoczucie nieletnich użytkowników.

- Temu będzie zobowiązane do ustrukturyzowania swojej platformy, w tym interfejsów użytkownika, algorytmów rekomendacji i warunków świadczenia usług, w celu złagodzenia i zapobiegania zagrożeniom dla bezpieczeństwa i dobrego samopoczucia konsumentów. Należy wdrożyć środki mające na celu ochronę konsumentów przed zakupem niebezpiecznych lub nielegalnych towarów, ze szczególnym naciskiem na zapobieganie sprzedaży i dystrybucji produktów, które mogą być szkodliwe dla nieletnich. Obejmuje to włączenie solidnych systemów kontroli wieku w celu ograniczenia zakupu produktów dla osób poniżej pewnego wieku.

Większa przejrzystość i rozliczalność

- Temu musi zapewnić, że jego oceny ryzyka i zgodność ze wszystkimi zobowiązaniami DSA są co roku poddawane zewnętrznym i niezależnym audytom.

- Temu musi publikować repozytoria wszystkich reklam wyświetlanych na swoim interfejsie.

- Temu będzie musiało zapewnić dostęp do publicznie dostępnych danych badaczom, w tym zweryfikowanym badaczom wyznaczonym przez koordynatorów usług cyfrowych.

- Temu musi spełniać wymogi dotyczące przejrzystości, w tym publikować co sześć miesięcy raporty odnoszące się do decyzji w zakresie moderowania treści i zarządzania ryzykiem, a także raz w roku raporty na temat ryzyka systemowego i wyników audytów.

- Temu musi wyznaczyć osobę odpowiedzialną za zgodność z przepisami i co roku poddawać się niezależnemu audytowi zewnętrznemu.

Ogólne zastosowanie DSA do platform internetowych i platform sprzedażowych

Od 17 lutego 2024 r. wszystkie platformy internetowe, w tym Temu, muszą już przestrzegać ogólnych obowiązków wynikających z DSA. Te ogólne przepisy obejmują obowiązki internetowych platform sprzedażowych w zakresie:

- zapewnienia identyfikowalności sprzedawców na swoich platformach;

- zaprojektowanie interfejsu w sposób ułatwiający sprzedawcom przestrzeganie ich zobowiązań prawnych wynikających z prawa UE;

- informowania konsumentów o zakupie nielegalnego produktu w momencie, gdy dowiedzą się o jego nielegalności.

Od 17 lutego 2024 r. DSA wymaga również od wszystkich platform internetowych, w tym platform sprzedażowych:

- zapewnienia przyjaznych dla użytkownika mechanizmów umożliwiających użytkownikom lub podmiotom zgłaszanie nielegalnych treści;
- priorytetowego traktowania powiadomień składanych przez tzw. "zaufane podmioty zgłaszające";
- dostarczania użytkownikom uzasadnień, gdy ich treści są ograniczane lub usuwane;
- zapewnienia wewnętrznego systemu rozpatrywania skarg dla użytkowników w celu odwołania się od decyzji dotyczących moderowania treści;
- przeprojektowania swoich systemów w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony nieletnich;
- upewnienia się, że ich interfejsy nie są zaprojektowane w sposób, który oszukuje lub manipuluje użytkownikami;
- wyraźnego oznaczania reklamy w swoich interfejsach;
- zaprzestania prezentowania ukierunkowanych reklam opartych na profilowaniu danych wrażliwych (takich jak pochodzenie etniczne, poglądy polityczne lub orientacja seksualna) lub skierowanych do nieletnich;
- działania na jasnych warunkach, w sposób staranny, obiektywny i proporcjonalny przy ich stosowaniu;
- publikacji raz w roku raportów przejrzystości dotyczących procesów moderowania treści.

Kolejne kroki

Po przejściu procedury wyznaczenia Temu jako VLOP Komisja będzie właściwa do nadzorowania zgodności Temu z DSA we współpracy z irlandzkim koordynatorem ds. usług cyfrowych.

Służby Komisji będą uważnie monitorować stosowanie zasad i obowiązków DSA przez platformę, w szczególności w odniesieniu do środków mających na celu zagwarantowanie ochrony konsumentów i przeciwdziałanie rozpowszechnianiu nielegalnych produktów. Służby Komisji są gotowe do ścisłej współpracy z Temu w celu zapewnienia, że kwestie te zostaną odpowiednio rozwiązane.

Kontekst

Procedura ta (procedura wyznaczenia jako VLOP) ilustruje, w jaki sposób Komisja nadal uważnie

monitoruje rozwój rynku. Komisja wyznaczyła już 24 bardzo duże platformy internetowe i wyszukiwarki w ramach umowy o partnerstwie w sprawie usług cyfrowych.

25 kwietnia 2023 r. Komisja wyznaczyła pierwsze 19 bardzo dużych platform operacyjnych (VLOP) i bardzo dużych wyszukiwarek internetowych (VLOSE). Począwszy od końca sierpnia VLOP i VLOSE będą musiały spełniać dodatkowe obowiązki wynikające z sekcji 5 DSA. W dniu 20 grudnia 2023 r. wyznaczono trzy dodatkowe VLOP. W dniu 26 kwietnia 2024 r. Komisja wyznaczyła Shein jako VLOP, dla którego dodatkowe zobowiązanie stanie się wiążące w sierpniu 2024 r.

Nadzór i egzekwowanie DSA są dzielone między Komisję i koordynatorów ds. usług cyfrowych, którzy musieli zostać wyznaczeni przez państwa członkowskie do 17 lutego 2024 r.

Źródło: informacja prasowa Komisji Europejskiej

fot. pexels

EROD: KOMITET SKOORDYNOWANEGO NADZORU POWOŁUJE NOWEGO KOORDYNATORA

Komitet Skoordynowanego Nadzoru (CSC) wybrał Fanny Coudert z biura Europejskiego Inspektora Ochrony Danych (EIOD), na nową koordynatorkę CSC, na dwuletnią kadencję. Fanny Coudert zastąpi Clarę Guerrę z portugalskiego organu nadzorczego.

Fanny Coudert będzie kierować pracami Komitetu przy wsparciu zastępców: Sebastiana Hümmelera z federalnego niemieckiego organu nadzorczego i Mateja Sironica ze słoweńskiego organu nadzorczego.

CSC zapewnia skoordynowany nadzór nad dużymi systemami informacyjnymi UE oraz organami, urzędami i agencjami UE zgodnie z art. 62 rozporządzenia 2018/1725 lub z aktem prawnym UE ustanawiającym wielkoskalowy system informatyczny lub organ, urząd lub agencję UE. Komitet powstał w ramach Europejskiej Rady Ochrony Danych (EROD) i skupia unijne organy nadzorcze oraz Europejskiego Inspektora Ochrony Danych (EIOD), a także organy nadzorcze państw nienależących do strefy Schengen, gdy jest to przewidziane w prawie UE.

CSC obecnie obejmuje system wymiany informacji na rynku wewnętrznym (IMI), Eurojust, Prokuraturę Europejską (EPPO), Europol i system informacyjny Schengen (SIS). Stopniowo Komitet obejmie również inne systemy informatyczne, organy, urzędy i agencje w dziedzinie granic, azylu i migracji (EES, Eurodac, ETIAS, VIS i ich interoperacyjność), współpracy policyjnej i wymiaru sprawiedliwości (ECRIS-TCN) oraz Prüm nowej generacji.

Informacje o mandacie Koordynatora CSC i zastępców:

Koordynator i zastępcy są wyznaczani na dwuletnią kadencję rozpoczynającą się w dniu ich wyboru i mogą zostać ponownie wybrani na kolejne dwa lata.

Zastępca Sebastian Hümmeler został wybrany po raz drugi 29 listopada 2023 r., a zastępca Matej Sironic został wybrany 10 kwietnia 2024 r.

Źródło: komunikat EROD

ROZPORZĄDZENIE PROCEDURALNE RODO WCHODZI W DECYDUJĄCĄ FAZĘ

Parlament Europejski i Rada Unii Europejskiej (Rada UE) opublikowały poprawki do projektu rozporządzenia proceduralnego RODO Komisji Europejskiej. NOYB, czyli Europejskie Centrum Praw Cyfrowych (organizacja non-profit) przeanalizowała obie wersje i przygotowała wstępny przegląd (wideo i prezentacja).

Kontekst

Zgodnie z RODO organy nadzorcze z różnych państw członkowskich mają współpracować przy rozpatrywaniu skarg użytkowników i egzekwowaniu prawa wobec międzynarodowych firm. Poszczególne organy działają jednak na podstawie bardzo różnych krajowych przepisów proceduralnych. Niektóre państwa członkowskie nie mają nawet skodyfikowanej procedury. Samo RODO również nie zawiera zbyt wielu wyjaśnień dotyczących tych aspektów proceduralnych.

W 2023 r. Komisja Europejska zaproponowała nowe rozporządzenie w celu usunięcia przeszkód we współpracy. Można jednak powiedzieć, że wniosek ten został w dużej mierze skrytykowany za brak jakości prawnej, przeniesienie uprawnień z organów nadzorczych, których sprawa dotyczy, na organy wiodące i tak naprawdę nie zajęcie się wieloma podstawowymi kwestiami.

Pierwotny wniosek i poprawki

W normalnym procesie legislacyjnym UE, Parlament Europejski (kierowany przez komisję LIBE) i Rada (z przedstawicielami każdego państwa członkowskiego UE) przedstawiły obecnie dwie zmienione wersje wniosku Komisji:

- Tekst Komisji Europejskiej
- Poprawki Parlamentu Europejskiego
- Poprawki Rady Unii Europejskiej

Slajdy z filmu można również znaleźć tutaj.

Następnym krokiem jest pogodzenie tych dwóch wersji w jeden tekst – jest to ogromne wyzwanie, które zostanie wykonane w tak zwanych „trialogach”.

NOYB uważa, że wersje Parlamentu i Rady UE wydają się zmierzać w tym samym kierunku

z politycznego punktu widzenia. Jednak wersja Parlamentu ma bardziej przejrzyste podejście na wysokim szczeblu, a także usunęła niepotrzebne kroki, podczas gdy Rada UE dodała głównie elementy do wniosku Komisji, co częściowo jeszcze bardziej komplikuje jego czytanie.

W nadchodzących tygodniach NOYB opublikuje drugi materiał wideo na temat procedury art. 65/66 oraz pełne pisemne porównanie.

Źródło: materiał NOYB

fot. pixabay

META OTRZYMAŁA WSTĘPNE USTALENIA KOMISJI EUROPEJSKIEJ DOTYCZĄCE MODELU „PAY OR CONSENT", KTÓRY NARUSZA PRZEPISY AKTU O RYNKACH CYFROWYCH

Komisja poinformowała Metę, że według wstępnych ustaleń jej model reklamy „pay or consent" („zapłać lub wyraź zgodę") jest niezgodny z DMA. Komisja stoi na wstępnym stanowisku, że model wymusza na użytkownikach zgodę na łączenie danych osobowych, nie oferując jednocześnie mniej spersonalizowanej, lecz równoważnej alternatywy dla mediów społecznościowych dostarczanych przez Meta.

Wstępne ustalenia Komisji w sprawie modelu Meta „pay or consent" („zapłata lub zgoda")

Wiele platform internetowych przetwarza do celów reklamy dane osobowe użytkowników, którzy korzystają z ich usług i usług świadczonych przez osoby trzecie. Dzięki dominującej pozycji na rynkach cyfrowych strażnicy dostępu mogą narzucać warunki świadczenia usług dużej liczbie użytkowników, co umożliwia im gromadzenie ogromnych ilości danych osobowych. Zyskują w ten sposób potencjalną przewagę nad konkurencją, która nie ma dostępu do tak dużej ilości danych. To z kolei bardzo ogranicza możliwości w świadczeniu internetowych usług reklamowych i usług w zakresie serwisów społecznościowych.

Zgodnie z art. 5 ust. 2 DMA strażnicy dostępu muszą uzyskać zgodę użytkowników na łączenie danych osobowych pochodzących z danej podstawowej usługi platformowej z danymi osobowymi pochodzącymi z innych usług. Jeżeli użytkownik odmówi wyrażenia takiej zgody, powinien on otrzymać dostęp do mniej spersonalizowanego, lecz równoważnego rozwiązania alternatywnego. Strażnicy dostępu nie mogą uzależniać korzystania z usługi lub niektórych jej funkcji od zgody użytkownika.

W odpowiedzi na zmiany unijnych przepisów Meta wprowadziła w listopadzie 2023 r. model „zapłata lub zgoda", zgodnie z którym unijni użytkownicy Facebooka i Instagrama mają do wyboru dwie opcje: (i) opłacanie miesięcznego abonamentu za dostęp do serwisów społecznościowych w wersji bez reklam lub (ii) darmowy dostęp do serwisów społecznościowych w wersji ze spersonalizowanymi reklamami.

Komisja stoi na wstępnym stanowisku, że model reklamy „zapłać lub wyraź zgodę" stosowany przez Meta nie jest zgodny z DMA, ponieważ nie spełnia niezbędnych wymogów określonych w art. 5
ust. 2. Model Meta:

- nie oferuje użytkownikom wersji usługi, która wykorzystuje mniejszą ilość danych osobowych i jest równoważną alternatywną dla usługi opartej na spersonalizowanych reklamach;
- nie gwarantuje użytkownikom prawa do wyrażenia dobrowolnej zgody na łączenie ich danych osobowych pochodzących z różnych usług.

Aby model był zgodny z DMA, powinien on oferować użytkownikom, którzy nie wyrażają zgody na łączenie danych osobowych, równoważną usługę wykorzystującą mniejszą ilość danych – w tym przypadku do celów personalizacji reklam.

Komisja współpracuje w trakcie postępowania z odpowiednimi organami nadzorczymi.

Co dalej?

Przekazanie wstępnych ustaleń Komisji do Meta jest równoznaczne z poinformowaniem przedsiębiorstwa, że jego działania naruszają przepisy DMA. Wstępna opinia nie determinuje jednocześnie wyniku postępowania. Meta może teraz skorzystać z prawa do obrony i przeanalizować dokumenty zawarte w aktach Komisji, a następnie udzielić pisemnej odpowiedzi na zastrzeżenia. Komisja zakończy postępowanie po upływie 12 miesięcy, licząc od 25 marca 2024 r., czyli daty jego wszczęcia.

Jeżeli wstępne ustalenia potwierdzą się, Komisja przyjmie decyzję stwierdzającą niezgodność modelu Meta z art. 5 ust. 2 DMA.

W drodze decyzji stwierdzającej niewypełnianie obowiązków Komisja może nałożyć na strażnika dostępu kary pieniężne, których wysokość nie może przekraczać 10 % jego łącznego światowego obrotu. W przypadku stwierdzenia ponownego naruszenia obowiązku kary mogą wzrosnąć do 20%. Jeżeli naruszenia staną się systematyczne, Komisja jest ponadto uprawniona do przyjęcia dodatkowych środków zaradczych, takich jak zobowiązanie strażnika dostępu do sprzedaży przedsiębiorstwa lub jego części lub zakazanie strażnikowi dostępu nabywania dodatkowych usług związanych z systemowym nieprzestrzeganiem przepisów.

Komisja kontynuuje konstruktywny dialog z Meta, aby wypracować rozwiązanie, które umożliwi przedsiębiorstwu skuteczne przestrzeganie przepisów.

Źródło: nota prasowa Komisji Europejskiej

W DRUGIM SPRAWOZDANIU NA TEMAT STANU CYFROWEJ DEKADY WEZWANO DO ZINTENSYFIKOWANIA WSPÓLNYCH DZIAŁAŃ NA RZECZ TRANSFORMACJI CYFROWEJ UNII EUROPEJSKIEJ

2 lipca Komisja Europejska opublikowała drugie sprawozdanie na temat stanu cyfrowej dekady, zawierające kompleksowy przegląd postępów poczynionych w dążeniu do osiągnięcia celów cyfrowych określonych na 2030 r. w programie polityki „Droga ku cyfrowej dekadzie".

W tym roku po raz pierwszy sprawozdaniu towarzyszy analiza krajowych strategicznych planów działania dotyczących cyfrowej dekady przedstawionych przez państwa członkowskie, w których wyszczególniono planowane krajowe środki, działania i finansowanie mające przyczynić się do transformacji cyfrowej UE.

Z analizy Komisji wynika, że w obecnym scenariuszu wspólne wysiłki państw członkowskich nie osiągną poziomu ambicji UE. Zidentyfikowane luki obejmują potrzebę dodatkowych inwestycji, zarówno na szczeblu unijnym, jak i krajowym, w szczególności w obszarach umiejętności cyfrowych, wysokiej jakości łączności, wykorzystania sztucznej inteligencji (AI) i analizy danych przez przedsiębiorstwa, produkcji półprzewodników i ekosystemów przedsiębiorstw typu startup.

Zarówno UE, jak i państwa członkowskie mają do odegrania ważną rolę w egzekwowaniu nowych ram prawnych, podejmowaniu działań na rzecz promowania rozpowszechniania technologii cyfrowych i zapewnieniu swoim obywatelom odpowiednich umiejętności cyfrowych, aby w pełni korzystać z transformacji cyfrowej.

Dlatego tegoroczne sprawozdanie jest apelem o bardziej ambitne działania wobec państw członkowskich, ponieważ osiągnięcie celów cyfrowej dekady w zakresie infrastruktury cyfrowej, przedsiębiorstw, umiejętności i usług publicznych ma kluczowe znaczenie dla przyszłego dobrobytu gospodarczego i spójności społecznej UE.

W tym kontekście Komisja zaktualizowała również zalecenia dla poszczególnych krajów i przekrojowe zalecenia dla każdego państwa członkowskiego UE w celu wyeliminowania

stwierdzonych luk.

Konkurencyjna, suwerenna i odporna UE: infrastruktura cyfrowa i przedsiębiorstwa

Przyjęcie i rozwój innowacyjnych technologii ma kluczowe znaczenie dla konkurencyjności Europy, zwłaszcza w obecnym krajobrazie geopolitycznym i ze względu na rosnące zagrożenia dla cyberbezpieczeństwa, wymagające większej odporności i solidnych środków bezpieczeństwa.

W sprawozdaniu podkreślono, że UE jest daleka od osiągnięcia celów w zakresie łączności określonych w DDPP: Sieci światłowodowe, które mają kluczowe znaczenie dla zapewnienia łączności gigabitowej i umożliwiają korzystanie z najnowocześniejszych technologii, takich jak sztuczna inteligencja, chmura obliczeniowa i internet rzeczy, docierają do zaledwie 64% gospodarstw domowych. Wysokiej jakości sieci 5G docierają obecnie jedynie do 50% terytorium UE, a ich wydajność jest nadal niewystarczająca do świadczenia zaawansowanych usług 5G. Aby sprostać tym wyzwaniom, państwa członkowskie i Komisja powinny współpracować na rzecz wspierania prawdziwie funkcjonalnego jednolitego rynku cyfrowego.

W 2023 r. wykorzystanie sztucznej inteligencji, chmury obliczeniowej lub dużych zbiorów danych przez przedsiębiorstwa europejskie było również znacznie poniżej celu cyfrowej dekady wynoszącego 75%. Zgodnie z obecnymi tendencjami do 2030 r. tylko 64% przedsiębiorstw będzie korzystać z chmury obliczeniowej, 50% – z dużych zbiorów danych, a jedynie 17% – ze sztucznej inteligencji.

Aby osiągnąć cyfryzację sektora przedsiębiorstw, zasadnicze znaczenie ma zachęcanie MŚP do korzystania z innowacyjnych narzędzi cyfrowych, w szczególności chmury obliczeniowej i sztucznej inteligencji, a także mobilizowanie dalszych inwestycji prywatnych w przedsiębiorstwa typu start-up o dużym wzroście. Ma to kluczowe znaczenie dla utrzymania konkurencyjności Europy w odniesieniu do innowacji, wydajności i wzrostu opartych na danych.

Innym poważnym wyzwaniem, przed którym stoi transformacja cyfrowa UE, pozostaje ograniczone rozpowszechnienie technologii cyfrowych poza dużymi miastami. Aby zlikwidować tę przepaść cyfrową, zasadnicze znaczenie ma wspieranie współpracy między podmiotami europejskimi na szczeblu transgranicznym i lokalnym, na przykład poprzez projekty wielokrajowe, europejskie centra innowacji cyfrowych (EDIH) i konsorcja na rzecz europejskiej infrastruktury cyfrowej (EDIC). Od ubiegłego roku osiągnięto szereg sukcesów w tym zakresie, przy czym do końca maja 2024 r. utworzono trzy EDIC.

Polityka cyfrowa dla ludzi i społeczeństwa: umiejętności cyfrowe i usługi publiczne

Umieszczenie ludzi w centrum transformacji cyfrowej naszych społeczeństw i gospodarek jest

cyfrowej dekady i pierwszej zasady Deklaracji praw i zasad cyfrowych.

Obecnie cele w zakresie umiejętności cyfrowych określone w cyfrowej dekadzie są nadal dalekie od osiągnięcia, a jedynie 55,6% ludności UE posiada co najmniej podstawowe umiejętności cyfrowe. Zgodnie z obecną tendencją liczba specjalistów w dziedzinie ICT w UE wyniesie w 2030 r. około 12 mln, przy utrzymującym się braku równowagi płci. Aby osiągnąć te cele, państwa członkowskie powinny stosować wieloaspektowe podejście do wspierania umiejętności cyfrowych na wszystkich poziomach edukacji oraz zachęcać młodych ludzi, w szczególności dziewczęta, do zainteresowania się dyscyplinami nauk ścisłych, technologii, inżynierii i matematyki (STEM).

Państwa członkowskie czynią postępy w realizacji celu, jakim jest zapewnienie obywatelom i przedsiębiorstwom dostępu do wszystkich kluczowych usług publicznych i elektronicznej dokumentacji medycznej w internecie, a także zapewnienie im bezpiecznej identyfikacji elektronicznej (eID). Pomimo nierównego wykorzystania w państwach członkowskich identyfikacja elektroniczna jest obecnie dostępna dla 93% ludności UE i oczekuje się, że unijny portfel tożsamości cyfrowej będzie zachęcać do korzystania z niej. W dotychczasowym scenariuszu postępowania osiągnięcie 100% cyfrowych usług publicznych dla obywateli i przedsiębiorstw do 2030 r. pozostaje jednak wyzwaniem.

Kolejne kroki

Państwa członkowskie będą teraz musiały dokonać przeglądu i dostosowania swoich krajowych planów działania, aby dostosować je do ambicji programu polityki „Droga ku cyfrowej dekadzie” przed 2 grudnia 2024 r. Jak określono w DDPP, Komisja będzie monitorować i oceniać wdrażanie tych zaleceń oraz przedstawi sprawozdanie z postępów w kolejnym sprawozdaniu na temat stanu cyfrowej dekady w 2025 r.

Kontekst ogólny

Zaproponowany we wrześniu 2021 r. Droga ku cyfrowej dekadzie wyznacza jasny sposób na osiągnięcie transformacji cyfrowej w Unii Europejskiej. W grudniu 2022 r. Europejska deklaracja praw i zasad cyfrowych uzupełniła ją poprzez ustanowienie zasad i zobowiązań, które powinna przyświecać transformacji cyfrowej UE. Pierwsze sprawozdanie na temat stanu cyfrowej dekady opublikowano we wrześniu 2023 r.

Tegorocznemu sprawozdaniu towarzyszy kompleksowy pakiet dokumentów roboczych, sprawozdań i analiz służb Komisji, w których przedstawiono postępy w różnych wymiarach DDPP. Wspólne Centrum Badawcze Komisji (JRC) również przyczyniło się do tego monitorowania, zapewniając metodykę agregowania krajowych celów cyfrowych na szczeblu UE oraz mapując

kwotę inwestycji z unijnych instrumentów finansowania przeznaczonych na inicjatywy obejmujące komponent cyfrowy.

W trakcie obecnej kadencji UE podjęła istotne działania, aby osiągnąć postępy w realizacji celów i założeń cyfrowej dekady. Dzięki wnioskowi i przyjęciu kluczowych przepisów Komisja aktywnie promowała bezpieczniejszą przestrzeń internetową dla obywateli europejskich i wspierała ochronę konsumentów, zachowując jednocześnie potencjał innowacyjny europejskich przedsiębiorstw. Znaczne środki finansowe UE udostępniono również na wspieranie transformacji cyfrowej, w szczególności za pośrednictwem Instrumentu na rzecz Odbudowy i Zwiększania Odporności (150 mld EUR), DIGITAL Europa (7,9 mld EUR) oraz instrumentu „Łącząc Europę" 2 – technologie cyfrowe (1,7 mld EUR).

Źródło: komunikat prasowy Komisji Europejskiej

fot. pixabay

SZTUCZNA INTELIGENCJA: FRANCUSKI ORGAN NADZORCZY (CNIL) KONTYNUUJE PRACE NAD OPRACOWANIEM INNOWACYJNEJ I CHRONIĄCEJ PRYWATNOŚĆ SZTUCZNEJ INTELIGENCJI

Rok 2022 odznaczył się zmianą podejścia do wdrażania i wykorzystywania systemów sztucznej inteligencji dla ogółu społeczeństwa. Od tego czasu CNIL zauważył rosnącą chęć przyjęcia technologii we wszystkich sektorach: zdrowia, usług publicznych, bezpieczeństwa publicznego itp. CNIL uważa, że przyjęcie sztucznej inteligencji jest głównym czynnikiem dla Francji w zakresie konkurencyjności, innowacji i suwerenności w nadchodzących latach.

Niemniej jednak europejskie ramy prawne mają również na celu zapewnienie wysokiego poziomu ochrony praw podstawowych: pojawia się wiele pytań dotyczących ram prawnych dla tych technologii i ich wpływu na jednostki. Potrzeba odpowiedzi jest zatem coraz bardziej nagląca, tak aby umożliwić rozwój tych technologii w ramach zasady zaufania.

Tworzenie powiązań między RODO a AI Act

Podczas gdy europejskie rozporządzenie w sprawie sztucznej inteligencji zostało niedawno przyjęte i wejdzie w życie stopniowo w nadchodzących miesiącach, CNIL pragnie zapewnić pewność prawną podmiotom działającym w tym sektorze, przewidując związek między AI Act a RODO. RODO ma bowiem zastosowanie do dostawców systemów, niezależnie od aktu o sztucznej inteligencji, gdyż wykorzystują oni dane osobowe do ich opracowywania.

W tym kontekście CNIL po raz drugi otwiera publiczne konsultacje dla wszystkich podmiotów w celu opracowania swoich zaleceń:

- przedstawione do konsultacji arkusze instruktażowe mają na celu zajęcie się kilkoma głównymi kwestiami związanymi z innowacjami i ochroną: wykorzystanie webscrapingu (gromadzenie danych ze stron internetowych), które jest powszechną praktyką, w szczególności do tworzenia dużych modeli językowych, publikacja modeli sztucznej inteligencji w otwartym oprogramowaniu, ale także zarządzaniem prawami osób, co jest kamieniem węgielnym ram prawnych dotyczących danych

osobowych.

- a także kwestionariusz na temat stosowania RODO do modeli sztucznej inteligencji szkolonych na bazie danych osobowych.

Konsultacje i wymiana w celu tworzenia innowacyjnych i odpowiedzialnych modeli sztucznej inteligencji

CNIL przeprowadził liczne rozmowy z zainteresowanymi stronami zaangażowanymi w projektowanie i rozwój systemów sztucznej inteligencji. Są nimi firmy, ośrodki badawcze, władze publiczne, związki zawodowe pracowników, federacje zawodowe itp. Podnieśli oni potrzebę wyjaśnienia obowiązujących ram prawnych dla najbardziej rozpowszechnionych praktyk w celu stworzenia innowacyjnej i opartej na odpowiedzialności sztucznej inteligencji.

Rozwój systemów sztucznej inteligencji można pogodzić z wyzwaniami związanymi z ochroną prywatności. Co więcej, uwzględnienie tego imperatywu umożliwi stworzenie urządzeń, narzędzi i aplikacji, które będą etyczne i wierne europejskim wartościom. Jest to warunek zaufania obywateli do tych technologii.

Źródło: komunikat francuskiego organu nadzorczego (CNIL)

fot. pexels

AEPD PRZEDSTAWIA RAPORT NA TEMAT WPŁYWU UZALEŻNIAJĄCYCH WZORCÓW W INTERNECIE, ZWŁASZCZA W STOSUNKU DO NIELETNICH

10 lipca 2024 r. Hiszpańska Agencja Ochrony Danych (AEPD) przedstawiła raport, w którym analizuje, w jaki sposób przetwarzanie danych osobowych użytkowników na wielu platformach, aplikacjach i usługach obejmuje mechanizmy uzależniające w celu wydłużenia czasu korzystania z internetu.

W raporcie podkreślono, że w wielu przypadkach dostawcy ci wdrażają wprowadzające w błąd i uzależniające wzorce projektowe, aby przedłużyć czas pozostawania użytkowników w ich serwisach lub zwiększyć ich poziom zaangażowania i ilość gromadzonych o nich danych osobowych. Negatywny wpływ uzależniających strategii jest znacznie większy, gdy są one wykorzystywane do przetwarzania danych osobowych osób szczególnie wrażliwych, takich jak dzieci i młodzież, wpływając na preferencje i zainteresowania małoletnich, a ostatecznie wpływając na ich autonomię i prawo do rozwoju.

Raport klasyfikuje modele uzależnień na trzech poziomach: wysokim, średnim i niskim. Tak zwane wzorce wysokiego poziomu to ogólne strategie, niezależne od kontekstu i zastosowania. Cztery z nich zostały zidentyfikowane. Są to: wymuszone działanie, inżynieria społeczna, ingerencja w interfejs i trwałość. Wzorce średniego poziomu opisują bardziej szczegółowe podejścia, które wykorzystują psychologiczne słabości lub luki użytkowników. Wreszcie, wzorce niskiego poziomu odpowiadają konkretnemu wykonaniu różnych podejść i często są specyficzne dla kontekstu lub aplikacji.

Uwzględnienie uzależniających modeli w przetwarzaniu danych osobowych ma istotne konsekwencje dla ochrony danych użytkowników, takie jak proaktywna odpowiedzialność, skuteczne stosowanie obowiązków w zakresie ochrony danych w fazie projektowania, przejrzystość, zgodność z prawem, rzetelność, ograniczenie celu, minimalizacja danych lub przetwarzanie szczególnych kategorii danych.

Wiąże się to również z ryzykiem dla praw i wolności wszystkich użytkowników, a w szczególności

6 SPRAWY MIĘDZYNARODOWE

Dla prawa do integralności fizycznej i psychicznej dzieci i młodzieży.

Postępowania wszczęte przez Komisję Europejską

W związku z uzależniającymi modelami, Komisja Europejska wszczęła dwa postępowania w sprawie sankcji za możliwą niezgodność z DSA, przeciwko TikTok i Meta. Ponadto sama firma ogłosiła zawieszenie TikTok Lite po tym, jak Komisja upubliczniła swój zamiar nałożenia tymczasowych środków zawieszających funkcję, która finansowo nagradzała dodatkowy czas spędzony przed ekranem.

Źródło: komunikat hiszpańskiego organu nadzorczego (AEPD)

fot. pexels

AEPD I EUROPEJSKI INSPEKTOR OCHRONY DANYCH OMAWIAJĄ WYZWANIA W ZAKRESIE OCHRONY DANYCH ZWIĄZANE Z PRZETWARZANIEM NEURODANYCH

Hiszpańska Agencja Ochrony Danych (AEPD) i Europejski Inspektor Ochrony Danych (EIOD) opublikowali wspólny raport analizujący wyzwania związane z przetwarzaniem neurodanych dla praw i wolności osób fizycznych. Dokument, który analizuje to pojawiające się zjawisko, zawiera przegląd neurodanych i ocenia ich wpływ na prywatność i ochronę danych osobowych, w tym analizę konkretnych przypadków.

Raport określa, w jaki sposób niektóre zastosowania neurodanych mogą znacząco ingerować w podstawowe prawa i wolności jednostek, proponując jednocześnie analizę potrzeby stworzenia nowych praw człowieka, takich jak neuroprawa.

Ostatnie postępy w neurotechnologii umożliwiają pojawienie się rosnącej liczby połączonych urządzeń, które monitorują aktywność mózgu w różnych celach. Mózg odgrywa kluczową rolę między innymi w ludzkich zdolnościach poznawczych, decyzjach, emocjach i zachowaniach. W raporcie wyjaśniono, że techniki obrazowania mózgu zostały pierwotnie opracowane w kontekście medycyny klinicznej i badań neurobiologicznych, okazując się skuteczne w różnych metodach leczenia.

Jednak w ostatnich latach obserwuje się trend w kierunku zastosowań związanych z marketingiem. Na przykład do pomiaru reakcji ludzkiego mózgu na reklamy lub produkty w celu badania, analizowania i przewidywania zachowań konsumentów.

Neurotechnologie zostały również wykorzystane w urządzeniach do noszenia na ciele do szeregu codziennych czynności, takich jak edukacja i rozrywka. Ponadto implanty mózgu oferują możliwość wpływania na aktywność mózgu ludzi i jej zmiany. Ta dostępność, wraz z możliwościami sztucznej inteligencji w zakresie łączenia danych z różnych źródeł, może znacząco ingerować w podstawowe prawa i wolności.

Raport analizuje, co wiąże się z przetwarzaniem neurodanych w różnych kontekstach

i na przykładach przypadków użycia, takich jak środowisko edukacyjne lub gry wideo, a także zagrożenia stwarzane przez niektóre z nich. Następnie określono wymogi i zasady ochrony danych, których należy przestrzegać przy przetwarzaniu tego rodzaju danych osobowych, które często stanowią szczególne kategorie danych (np. dane biometryczne lub dane dotyczące zdrowia). Co do zasady, przetwarzanie szczególnych kategorii danych jest zabronione, z zastrzeżeniem wyjątków w pewnych okolicznościach. Tam, gdzie jest to dozwolone, przetwarzanie neurodanych musi być zgodne ze wszystkimi innymi wymogami i zasadami ochrony danych, takimi jak proporcjonalność, dokładność, przejrzystość i uczciwość.

W raporcie stwierdzono, że osoby rozważające przetwarzanie neurodanych powinny zawsze brać pod uwagę inwazyjny charakter przetwarzania neurodanych i dokładnie ocenić, czy zamierzony cel w pełni uzasadnia to „niezwykle inwazyjne i wrażliwe przetwarzanie danych, które dotyka najbardziej intymnego aspektu życia ludzi". Ponadto podkreśla, że kluczowe jest przeprowadzenie dogłębnej analizy neurodanych i ocena wpływu ich przetwarzania na prawa podstawowe, w tym potrzebę stworzenia neuropraw.

Karta Praw Podstawowych Unii Europejskiej wyraźnie uznaje podstawowe prawo do integralności psychicznej (art. 3), jako jeden z przejawów podstawowego prawa do godności ludzkiej (art. 1), które jest również podstawą prawa do prywatności i ochrony danych osobowych (art. 7 i 8 Karty).

Agencja ustanowiła wśród swoich strategicznych kierunków promowanie regulacji przetwarzania neurodanych i powiązanych z nimi neuropraw, zwłaszcza w dziedzinie usług skierowanych do nieletnich.

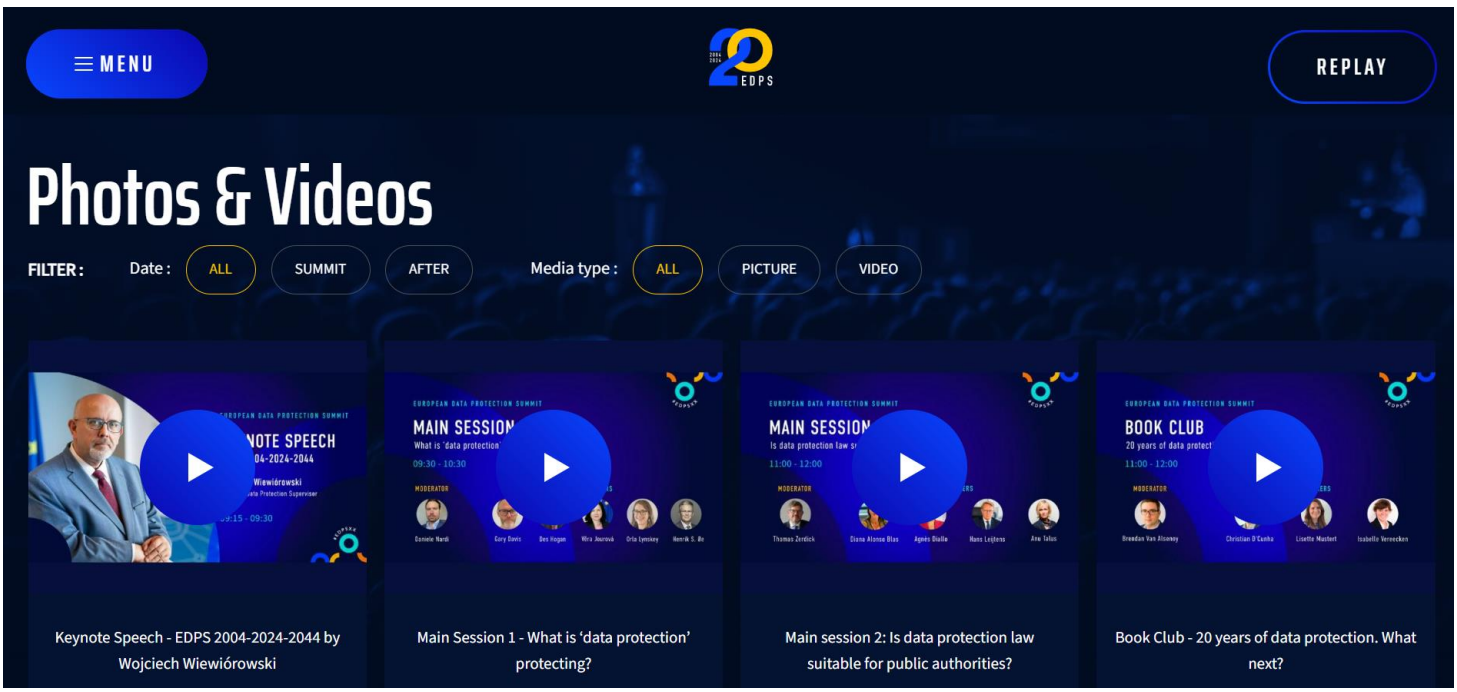
Źródło: komunikat hiszpańskiego organu nadzorczego (AEPD)

NAGRANIA Z KONFERENCJI EIOD PT. „RETHINKING DATA IN A DEMOCRATIC SOCIETY”

W jednym z ostatnich numerów biuletynu informowaliśmy o obchodach 20-lecia istnienia instytucji Europejskiego Inspektora Ochrony Danych. Z tej okazji zorganizowano szereg wydarzeń.

Dostępne są już nagrania wszystkich paneli konferencji EIOD pt. „Rethinking Data in a Democratic Society”, zorganizowanej z okazji 20-lecia organu, która odbyła się 20 czerwca br.

Poniżej link do materiałów foto i wideo:
https://20years.edps.europa.eu/en/summit/media



fot. strona główna 20years.edps.europa.eu

USTAWA O OCHRONIE SYGNALISTÓW Z PERSPEKTYWY RODO – RELACJA Z SEMINARIUM

7 sierpnia w Urzędzie Ochrony Danych Osobowych odbyło się seminarium, podczas którego prezes UODO Mirosław Wróblewski wspólnie z przedstawicielami Społecznego Zespołu Ekspertów przy PUODO oraz zewnętrznymi ekspertami zastanawiali się nad interpretacją przepisów tej ustawy.

Wątpliwości Urzędu

Ustawa o ochronie sygnalistów została przyjęta przez Sejm RP w dniu 14.06.2024. Prezes UODO przewidując, że stosowanie ustawy może zrodzić poważne wątpliwości w praktyce, wraz ze Społecznym Zespołem Ekspertów przy PUODO oraz ekspertami Urzędu podjęli inicjatywę konsultacji społecznych. W ramach konsultacji można było zgłaszać pytania i obiekcje, dotyczące stosowania tych przepisów w zakresie ochrony danych osobowych.

Na podstawie przesłanych uwag UODO przygotował wyjaśnienia, które zostały przedstawione w ramach otwartego spotkania w formie seminarium. Jego celem było zidentyfikowanie i omówienie obszarów, które mogą generować największe wątpliwości interpretacyjne.

Uwagi UODO do ustawy

Mirosław Wróblewski na początku spotkania, przypomniał o kilku uwagach, które Urząd zgłaszał w toku prac legislacyjnych. Chodziło o wątpliwości dotyczące przepisów w odniesieniu do katalogów danych zawartych w rejestrach zgłoszeń. Ich zakres nie został dostosowany do możliwości anonimowego dokonania zgłoszenia naruszenia. Jak podkreślił: „Ustawa wymaga przejrzystego i konsekwentnego przyjęcia pewnych przepisów kształtujących prawa i obowiązki sygnalistów, chcących dokonać zgłoszenia zarówno w trybie imiennym, jak i w trybie anonimowym, jeśli organizacja dopuści takie anonimowe zgłoszenia”.

Prezes UODO zaznaczył, że organ nadzorczy postulował o wyraźne określenie w ustawie poprzez jakie dane osobowe możliwa będzie identyfikacja tożsamości sygnalisty:

– „Dobór zakresu danych powinien następować z uwzględnieniem celu regulacji, czyli identyfikacji tożsamości zgłaszającego oraz osoby, której dotyczy zgłoszenie z uszanowaniem jednoczesnym

zasady minimalizacji danych". Mamy bowiem w art. 17 dyrektywy 2019/1937 założenie zgodności i poszanowania przepisów RODO.

Mirosław Wróblewski zaakcentował, że „kluczowym elementem ochrony sygnalisty jest obowiązek zapewnienia poufności jego tożsamości, wynikający z art. 16 ust. 1 dyrektywy. Tutaj warto odnieść się do art. 8 ust. 5 i ust. 6 ustawy o sygnalistach, gdzie ograniczane są prawa wynikające z RODO". Natomiast w opinii UODO spełnienie tych wymogów zgodnie z art. 23 RODO powinno nastąpić w treści przepisów ustawowych.

Prezes UODO wspomniał również o wątpliwościach odnoszących się do art. 6 ustawy – do kogo należeć będzie ocena przesłanki uzasadnionych podstaw utwierdzających sygnalistę w przekonaniu o prawdziwości informacji ujętej w zgłoszeniu. Podkreślił również, że siatka pojęciowa ustawy przysparza trudności w interpretacji przepisów.

Dr Mirosław Gumularz, przewodniczący Społecznego Zespołu Ekspertów przy PUODO podziękował za przesłanie licznych uwag i aktywny udział w konsultacjach społecznych. Zapewnił jednocześnie, że każda uwaga została wnikliwie przeanalizowana przez Społeczny Zespół Ekspertów w dialogu z Urzędem oraz zaprezentował najbardziej problematyczne kwestie, jakie pojawiły się w ramach konsultacji społecznych. Omawiano je w kolejnych panelach.

Obowiązki informacyjne oraz retencja danych

W panelu poświęconym obowiązkom informacyjnych i retencji danych podkreślono, że w kontekście realizacji obowiązku informacyjnego wskazanego w art. 13 RODO (tj. gdy dane są pozyskiwane bezpośrednio od podmiotu danych) należy:

- uwzględnić, że w procesie przyjmowania zgłoszeń sygnalistów będzie dochodziło do przetwarzania danych osobowych różnych kategorii podmiotów danych, tj. m.in. sygnalistów, osób których dotyczy zgłoszenie, świadków, etc.;
- stosować warstwowe podejście do wykonania obowiązku informacyjnego, odsyłając np. do procedury zgłoszeń wewnętrznych (klauzula informacyjna może się pojawić jednocześnie także na stronie www w miejscu, gdzie będzie informacja o kanałach przyjmowania zgłoszeń);
- obowiązek informacyjny można spełnić także np. przy pierwszym kontakcie z osobą, która potencjalnie może być sygnalistą, np. na etapie rekrutacji, zatrudniania, ofertowania, zawierania umów cywilnych czy innych stosunków z osobami, które będą wykonywały pracę na rzecz podmiotu prawnego.

Paneliści rozważali scenariusze problemów ze spełnieniem obowiązku informacyjnego.

Zastanawiali się też, od kiedy należy liczyć okres retencji. Ustalono, że okres retencji należy liczyć

od momentu wpłynięcia zgłoszenia.

Zwrócono uwagę, że (co podkreślał m.in. dr Paweł Litwiński) art. 8 ust. 3 ustawy o ochronie sygnalistów nie jest do końca jasny, gdy uświadomimy sobie, że jedno zgłoszenie może zawierać informacje o kilku naruszeniach prawa – wtedy okresy retencji danych liczone oddzielnie dla każdej z informacji o naruszeniu prawa mogą być różne. Mimo tego wydaje się, że 3-letni okres retencji danych powinien być zawsze liczony od daty przyjęcia zgłoszenia. Dotyczy to także danych zawartych w rejestrze zgłoszeń (art. 29 ust. 5 ustawy o ochronie sygnalistów) – rejestr zgłoszeń jest bowiem konstruowany w oparciu o zgłoszenie (w rejestrze odnotowujemy numer zgłoszenia itd., a więc informacje związane ze zgłoszeniem), a w konsekwencji, to data dokonania zgłoszenia będzie miała podstawowe znaczenia dla obliczania okresu retencji danych.

Zakaz ujawniania tożsamości sygnalisty (który pojawia się m.in. w art. 8 ust. 1 ustawy) należy rozumieć szeroko, w świetle art. 16 ust. 1 dyrektywy o ochronie sygnalistów (dyrektywa 2019/1937 z dnia 23 października 2019 r.). Prowadzący panel mocno zaakcentowali, że nie wolno informować o tożsamości sygnalisty ponieważ zgodnie z art. 16 ust. 1 dyrektywy (implementowany do art. 27 ustawy krajowej) „Państwa członkowskie zapewniają, by tożsamość osoby dokonującej zgłoszenia nie została ujawniona – bez wyraźnej zgody tej osoby – żadnej osobie, która nie jest upoważnionym członkiem personelu właściwym do przyjmowania zgłoszeń i podejmowania w związku z nimi działań następczych. Ma to również zastosowanie do wszelkich innych informacji, na podstawie których można bezpośrednio lub pośrednio zidentyfikować tożsamość osoby dokonującej zgłoszenia” . Przypomnieli słuchaczom, że tożsamość sygnalisty to nie tylko imię i nazwisko, ale też np. jego miejsce i stanowisko pracy.

W kontekście art. 8 ust. 1 ustawy dyskutanci wskazali argumenty przemawiające za tym, że zgoda, o której mowa w tym przepisie jest zgodą w rozumieniu RODO, niemniej dotyczy jednej specyficznej operacji na danych (tj. ujawnienia danych sygnalisty). Zgoda musi spełniać wymagania RODO, a więc być dobrowolnym, konkretnym, świadomym i jednoznacznym okazaniem woli, jak również kryteria wskazane w art. 8 ust. 1 ustawy o ochronie sygnalistów, tj. musi być wyraźna.

Przypomniano, że zgodnie z art. 7 ust. 3 RODO wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem, o czym sygnalistę należy poinformować.

Prelegenci podkreślili, że sygnalista musi też zostać poinformowany co się wydarzy, gdy jego tożsamość zostanie ujawniona.

Jeśli chodzi o osoby, których dotyczą dane podawane w zgłoszeniu sygnalisty (np. sprawcy, tj. osoby, której dotyczy zgłoszenie) i obowiązków informacyjnych z art. 14 RODO, należy pamiętać

o wyłączeniu z art. 14 ust. 5 lit. b) RODO, a nie tylko o wyłączeniu wynikającym bezpośrednio z ustawy z 14 czerwca 2024 o ochronie sygnalistów.

Przepisy ustawy nie uwzględniły jak wyłączyć obowiązek w przypadku przekazania kopii danych, by nie przekazywać informacji o sygnaliście, świadku i wszystkich, których prawa mogłyby na tym ucierpieć. W związku z tym zasadne wydaje się być zastosowanie art. 15 ust. 4 RODO, by w efekcie nie uwzględniać w kopii takich danych, których ujawnienie mogłoby niekorzystnie wpłynąć na prawa i wolności innych (tu: głównie sygnalisty).

Przetwarzać dane osobowe sygnalisty (oraz innych osób wskazanych w art. 27 ustawy) wewnątrz organizacji (podmiotu prawnego) mogą wyłącznie osoby wskazane w art. 27 ust. 1 ustawy, tj. zajmujące się przyjmowaniem zgłoszeń i prowadzeniem działań następczych. Nie wyklucza to outsourcingu, ale wyłącznie w zakresie wskazanym w art. 28 ust. 1 ustawy.

Jak zostało wskazane w ustawie: 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.

Jednocześnie należy zwrócić uwagę, że art. 27 ust. 2 ustawy nie może być rozumiany w ten sposób, że jedyną przesłanką legalnego dostępu i przetwarzania danych tam wskazanych jest tylko formalne nadanie upoważnienia (o którym mowa w treści art. 27 ust. 2 ustawy).

Nadanie upoważnienia, o którym mowa w art. 27 ust. 2 ustawy jest tylko formalnym potwierdzeniem tego, że wskazane osoby (zgodnie z postanowieniami procedury zgłoszeń wewnętrznych) są uprawnione do dostępu do danych osobowych (i w konsekwencji ich przetwarzania). Przepis art. 27 ust. 2 ustawy, który dotyczy zgłoszeń wewnętrznych należy czytać w kontekście art. 25 ust. 1 ustawy, który wymienia obligatoryjne elementy procedury zgłoszeń wewnętrznych m.in. wymaga wskazania, kto będzie uprawniony do przyjmowania zgłoszeń i prowadzenia działań następczych. Należy go interpretować także zgodnie z art. 16 ust. 1 dyrektywy o ochronie sygnalistów, który wskazuje, że tożsamość osoby dokonującej zgłoszenia nie może zostać ujawniona – bez wyraźnej zgody tej osoby – żadnej osobie, która nie jest upoważnionym członkiem personelu właściwym do przyjmowania zgłoszeń i podejmowania w związku z nimi działań następczych.

Upoważnienie powinno być szczegółowe, tj. na tyle, aby wyłączyć możliwe wątpliwości co do jego zakresu. Musi wskazywać do wykonywania jakich czynności na danych osobowych upoważnia daną osobę.

Wskazano również na brak kompleksowej regulacji ustawy. Podkreślono, by nie ograniczać się do samej ustawy o sygnalistach. Niezbędne jest korzystanie również z RODO, przy równoczesnym zachowaniu ostrożności w tym aspekcie.

Każdy przypadek trzeba będzie oceniać indywidualnie – które informacje przekazać, a które nie. Jest to kwestia oceny i należy tu również wziąć pod uwagę zasadę rozliczalności.

Procedura przyjmowania zgłoszeń wewnętrznych i prowadzenia postępowań wyjaśniających

W drugim panelu uczestnicy seminarium omawiali procedury przyjmowania zgłoszeń wewnętrznych i prowadzenia postępowań wyjaśniających z perspektywy zasad przetwarzania danych osobowych.

Wiele pytań, które wpłynęły do Społecznego Zespołu Ekspertów oraz UODO dotyczyło możliwości zgłoszeń anonimowych oraz sposobów przekazywania zgłoszeń (kontrowersje wzbudziło ustne zgłaszanie naruszeń).

Poruszono również zagadnienie tzw. „fałszywego sygnalisty" – dopiero na zaawansowanym etapie postępowania można stwierdzić, czy sygnalista mieści się w ustawowych ramach definicji. Należy ostrożnie podchodzić do stwierdzenia, że ktoś nie jest sygnalistą.

Dużą część dyskusji poświęcono grupom kapitałowym w kontekście sygnalistów, kanałów zgłoszeń i tego, jak powinno wyglądać zgłoszenie. W kontekście kanałów zgłoszeń rozważano różne możliwości ich wdrażania przez grupy kapitałowe z perspektywy praktycznej oraz zgodności z prawem. Przede wszystkim zwrócono uwagę na ryzyko, jakie niesie za sobą pozostawienie jedynie kanałów korporacyjnych. Eksperci podkreślili, że ustawa – w art. 28 – posługuje się różnymi pojęciami „wspólnych zasad" czy „wspólnych procedur". Jak zauważyli prelegenci, są to pojęcia odmienne od tych użytych w dyrektywie, gdzie jest mowa np. o możliwości łączenia zasobów w przypadku niektórych kategorii podmiotów. Ustawa krajowa nie mówi o łączeniu zasobów co do przyjmowania zgłoszeń i ich rozpatrywania. Jednocześnie zaznaczono, że nie wyklucza to oczywiście powierzenia czynności np. jednej ze spółek w grupie na ogólnych zasadach wynikających z art. 28 ust. 1 ustawy.

UODO interesowały również grupy kapitałowe o zasięgu międzynarodowym, rozmówcy zastanawiali się, co robić w sytuacji, gdy grupa kapitałowa jest tak skonstruowana, że występuje w niej relacja „spółka-matka". Próba zmierzenia się z wyzwaniem, jakie działania podjąć w danej sytuacji nie była łatwa, padły różne propozycje reakcji ze strony prelegentów.

Przede wszystkim zwrócono uwagę, że „spółka matka" może występować w roli podmiotu, któremu powierzono czynność na podstawie art. 28 ust. 1 ustawy (i w zakresie tam wskazanym), ale jeżeli spółka matka (poza RP) przyjmuje zgłoszenia do własnych celów, to nie jest to przypadek

regulowany ustawą o ochronie sygnalistów (nie wyklucza to oczywiście, że wejdą wtedy w grę przepisy krajowe innego państwa członkowskiego UE).

Zastanawiano się jak podmiot ma realizować ustawę, gdy zadania są przekazywane na zewnątrz – czy podmiot któremu organizacja zdecydowała się powierzyć outsourcing daje gwarancję ochrony danych osobowych i ochrony sygnalisty. W przypadku outsourcingu wewnątrz grupy podmiotów (np. do spółki „matki") należy uwzględnić ryzyka związane np. z nieuprawnionym dostępem do danych.

Dokonano próby rozróżnienia pojęcia zasady od procedury. Przypomniano, że procedury należy przyjmować w sposób przyjęty w danej strukturze, a wraz z rozpoczęciem rekrutacji muszą być one dostępne dla kandydatów w ustalonej przez daną organizację formie.

Poinstruowano słuchaczy jak powinno wyglądać modelowe upoważnienie do procesów przetwarzania danych. Dyskutowano, jaki jest minimalny zakres upoważnienia, by spełniało wymogi prawne. Ustalono, że powinno zawierać informacje, kto upoważnia, kogo, do czego – jakich konkretnie czynności.

Podkreślono, że podczas konsultacji społecznych, często pojawiały się pytania o zgłoszenia anonimowe. Jak ustalono, przyjęcie zgłoszeń anonimowych zależeć będzie w dużej mierze od kultury organizacji. Podmioty, które się na to zdecydują, będą musiały wziąć pod uwagę konsekwencje tej decyzji, równocześnie pamiętając, że anonimowość może być pozorna.

Prelegenci zastanawiali się nad słusznością zgłoszeń telefonicznych – wyrażenie zgody na transkrypcję, utrwalenie zgłoszenia zdaje się być w przepisach. Powinno się jednak zgłaszającego powiadomić, że rozmowa jest nagrywana. Zdaniem prowadzących panel, zgoda może być wyrażona także poprzez wolę kontynuacji rozmowy. Eksperci zastanawiali się, czy jest to zgoda w rozumieniu art. 7 RODO (pojęcie „zgody" pojawiło się w art. 26 ust. 3 ustawy o ochronie sygnalistów). Większość uczestników spotkania przyjęło, że nie jest to zgoda w rozumieniu RODO.

Jak ustalili specjaliści, więcej argumentów przemawia za tym, że – wskazana w ustawie zgoda dotycząca sposobu dokumentowania rozmowy z sygnalistą (art. 26 ust. 3 ustawy o ochronie sygnalistów) nie jest zgodą w rozumieniu RODO.

Zgłoszenia zewnętrzne

Panel trzeci dał możliwość uzyskania informacji, w jaki sposób Biuro Rzecznika Praw Obywatelskich przygotowuje się do wejścia w życie ustawy o sygnalistach. Bowiem polski ustawodawca właśnie RPO powierzył rolę centralnego organu wspierającego sygnalistów w korzystaniu z przysługujących im praw.

7 EDUKACJA

Jak zauważył przedstawiciel Biura RPO dyr. Marcin Malecko, nowo powstający w Biurze Rzecznika Praw Obywatelskich Zespół ds. Sygnalistów wciąż ma więcej pytań niż gotowych odpowiedzi Wyzwaniem dla BRPO jest zorganizowanie systemu zgłoszeń zewnętrznych i odseparowanie go od systemu zgłoszeń wewnętrznych.

Słuchacze mogli się dowiedzieć, że prawdopodobnie powstanie elektroniczny formularz zgłoszeniowy na odrębnej stronie niż BRPO. W założeniu ma być prosty w obsłudze oraz wymagać jedynie niezbędnych danych do procedowania zgłoszenia.

Zakres pozyskiwanych danych – np. tych, które będzie musiał wpisać sygnalista, wypełniając formularz online do dokonywania zgłoszeń – musi być zgodny z zasadą minimalizacji (art. 5 ust. 1 lit. c) RODO) oraz skorelowany z treścią procedury zgłoszeń wewnętrznych i decyzją podmiotu prawnego co do przyjmowania zgłoszeń anonimowych (m.in. art. 25 ust. 1 pkt 4 ustawy wymaga, aby procedura zgłoszeń wewnętrznych określała m.in. tryb postępowania z informacjami o naruszeniach prawa zgłoszonymi anonimowo).

Podobnie treść klauzuli informacyjnej w rozumieniu art. 13-14 RODO musi uwzględniać tę kwestię, tj. m.in. trzeba wyraźnie wskazać czy podanie danych jest dobrowolne czy nie (uwzględniając decyzję co do zgłoszeń anonimowych).

Ustawa nakłada na BRPO obowiązek upowszechniania informacji na temat uprawnień sygnalistów i ich roli w społeczeństwie. Niestety nie definiuje jak tę funkcję poradniczą, edukacyjną Rzecznik ma pełnić. Na razie RPO zastanawia się nad utworzeniem dwóch infolinii – jednej czysto poradniczej, drugiej do zgłaszania sygnałów przez sygnalistów.

Wciąż nie wiadomo jak wyglądać będzie weryfikacja zgłoszeń zewnętrznych – do jakiego stopnia dopuścić weryfikację i w jaki sposób ją przeprowadzić.

Poruszono problem zgłaszania naruszeń przez „nie sygnalistów” – wydaje się, że właściwą praktyką jest przyjmowanie zgłoszeń również przez osoby, które nie wpisują się w definicję sygnalisty, a więc nie mają związku z zatrudnieniem.

Dyskutanci zastanawiali się, czy można takiego zgłoszenia nie przyjąć. Szczególnie, że gdy zgłoszenie jest anonimowe mogą wystąpić trudności w ustaleniu, czy osoba zgłaszająca ma jakieś konotacje z zatrudnieniem, a więc jest sygnalistą w rozumieniu ustawy. Pojawiła się wątpliwość, czy takiej osobie przysługuje ochrona i – jeśli tak – w jaki sposób ją zapewnić.

Zastanawiano się, czy sygnalistą może być aktywista, obserwator, któremu na sercu leży dobro publiczne, ale nie ma powiązania z zatrudnieniem.

Zabezpieczenia techniczne i organizacyjne

W ostatnim panelu dyskutowano o bezpieczeństwie wybranych kanałów zgłaszania naruszeń poprzez zapewnienie odpowiednich zabezpieczeń technicznych i organizacyjnych.

Podkreślono konieczność uwzględnienia, w projektowanych procesach przetwarzania danych, ochrony danych osobowych zgodnie z zasadami privacy by design i privacy by default – przy równoczesnym zadbaniu o integralność i dostępność danych oraz przy zachowaniu ich poufności.

W ramach oceny ryzyka należy uwzględnić m.in. scenariusze związane z nieuprawnionym dostępem do danych sygnalisty i innych osób (wewnątrz organizacji przyjmującej zgłoszenia), co jest szczególnie istotne z perspektywy treści art. 27 ustawy oraz ryzyk dotyczących działań odwetowych.

Zauważono, że komunikacja musi być zaszyfrowana zarówno w transporcie, jak i w procesie składowania informacji. Zaproponowano metody zapobiegania email spoofingu. Rozmawiano o bezpieczeństwie przekazywania zgłoszeń do podmiotu prawnego.

Zastanawiano się nad potrzebą wysyłania zaszyfrowanych maili – choć szyfrowanie zwiększa bezpieczeństwo, może być uznane dla zgłaszających za rozwiązanie zbyt trudne, przez co będą oni rezygnować z wysyłania zgłoszeń.

Dyskutowano o tym, jakie trudności rodzą platformy zgłoszeniowe. Eksperci wskazali, że zanim się na platformę zdecydujemy, należy ją odpowiednio zabezpieczyć, zaszyfrować, zweryfikować zgodnie z RODO, zmierzyć i ocenić.

Prelegenci szukali odpowiedzi na pytanie, jak zadbać o poufność danych, również w kontekście monitoringu stacji roboczej pracowników przyjmujących zgłoszenia.

Zwrócono uwagę na zasadę integralności danych – komunikat wysłany przez system informatyczny, gdy jest źle zabezpieczony, istnieje ryzyko, że zostanie zmieniony przez osobę trzecią.

Ryzyka naruszenia praw lub wolności osób, których dane będą przetwarzane w procesie obsługi zgłoszeń sygnalistów należy rozważać m.in. w kontekście przyjętej przez podmiot prawny procedury zgłoszeń wewnętrznych (odpowiednio dotyczy to zgłoszeń zewnętrznych), a w szczególności w powiązaniu z kanałami komunikacyjnymi przyjęcia zgłoszenia oraz aktywami wspierającymi ten proces – środkami przetwarzania, takimi jak: systemy, sprzęt, aplikacje, personel i inne zasoby.

W trakcie oceny ryzyka należy szczególną uwagę zwrócić na to, kto z personelu organizacji będzie miał (nawet potencjalny) dostęp do danego środka przetwarzania (komputery, serwery, sieci, aplikacje, praformy, pomieszczenie do przyjmowania zgłoszeń ustnych itd.).

Przepisy ustawy zwracają szczególną uwagę na zapobieganie działaniom odwetowym, dlatego w ocenie ryzyka i doborze środków należy przeanalizować, komu z wewnątrz organizacji może

zależeć na uzyskaniu dostępu do treści zgłoszeń naruszeń prawa czy poznaniu tożsamości sygnalistów (czy też innych osób).

Podsumowanie – na co organizacja musi zwrócić uwagę, wdrażając przepisy ustawy o sygnalistach

• Przed przystąpieniem do wdrożenia ustawy, organizacja musi ustalić jakimi kanałami będzie przyjmować zgłoszenia (elektronicznie, telefonicznie, czy dopuszczalne są anonimowe zgłoszenia i czym to będzie skutkowało w ocenie ryzyka formularza).

• Powinna podjąć decyzję, kto będzie przyjmował zgłoszenia i prowadził działania następcze. Mogą to robić wyłącznie osoby bezstronne. W tym kontekście pojawił się również temat outsourcingu – że zakres dopuszczalnego outsourcingu wynika z art.28 ust.1 ustawy o ochronie sygnalistów w powiązaniu w zakresie przetwarzania danych osobowych z RODO.

• Musi przeprowadzić ocenę ryzyka naruszenia praw lub wolności osób fizycznych (z art. 25 RODO i 32 RODO) już w fazie projektowania procesu przyjmowania zgłoszeń sygnalistów uwzględniając także wymagania dotyczące oceny skutków (art. 35 RODO).

• Organizacja powinna również zastanowić się, jak będzie spełniać obowiązki informacyjne - należy je wypełniać warstwowo.

• Jeśli chodzi o informowanie o procedurze kandydatów do pracy, kontrahentów – tu istnieje możliwość spełnienia wprost obowiązku informacyjnego, jak i przekierowania do właściwych dokumentów.

• Klauzule informacyjne muszą być dostosowane w szczególności w zakresie informowania o obowiązku lub też dobrowolności podania danych przez sygnalistę.

• Ustawa o ochronie sygnalistów nie wymaga podania danych do kontaktu przez sygnalistę. Należy to zsynchronizować z kwestią zakresu tych danych, w zależności od tego, czy organizacja dopuści anonimowe zgłoszenia czy też nie.

• Bardzo ważne jest uwzględnienie kwestii powierzenia przekazania danych oraz weryfikacji nadawanych upoważnień.

• Organizacja musi też ustalić jak zarządzać usuwaniem danych i dokonać aktualizacji rejestru czynności, w zależności od typu i zakresu pozyskiwanych danych.

• Niezbędne jest, by wskazała podstawę do przetwarzania danych.

• Musi również uwzględnić konieczność aktualizacji rejestru czynności o nowy proces przetwarzania danych (w tym kontekście warto wspomnieć o tym, że w procesie szeroko pojętej obsługi zgłoszeń sygnalistów pojawiają się różne kategorie osób, których dane są przetwarzane

m.in. sygnalista, osoba, której dotyczy zgłoszenie, świadek, osoba powiązana z sygnalistą).

Co dalej?

Prezes UODO podkreślił, że przepisy tej ustawy budzą liczne wątpliwości. Rolą Urzędu jest nadzór nad przestrzeganiem tej ustawy. Na ile przepisy wymagają dalszych sugestii zmian, pokaże praktyka.

W następstwie dyskusji seminaryjnej na stronie UODO systematycznie będą pojawiać się pisemne wyjaśnienia UODO podpowiadające właściwe kierunki interpretacji przepisów ustawy o sygnalistach w zakresie dotyczącym danych osobowych.

W związku z tym, że bardzo dużo pytań dotyczyło roli kancelarii prawnych w kontekście outsourcingu czynności zgłoszeń sygnalistów Mirosław Wróblewski, prezes UODO, zapowiedział, że zwróci się do samorządów radców prawnych i adwokatów o spotkanie w celu omówienia roli kancelarii prawnych we wspieraniu klientów, biorąc pod uwagę możliwość zawarcia z nimi umowy powierzenia przyjmowania zgłoszeń wewnętrznych w rozumieniu art. 28 ust. 1 ustawy o ochronie sygnalistów.

Na fotografii uczestnicy panelu II. Kolejno od lewej: dr hab. Arwid Mednis, dr Arleta Nerka, dr Dominika Dörre-Kolasa, Weronika Kowalik,UODO, dr hab. Beata Baran-Wesołowska

PORADY PRAWNE URZĘDU OCHRONY DANYCH OSOBOWYCH NA 30. EDYCJI POL'AND'ROCK FESTIVALU

Reprezentanci Urzędu Ochrony Danych Osobowych w pierwszych dniach sierpnia mieli możliwość udziału w niezwykłym wydarzeniu, w 30. Pol'and'Rock Festival w miejscowości Czaplinek-Broczyno.

Pol'and'Rock Festival to coroczna impreza muzyczna, która gromadzi fanów rocka i nie tylko, oferując występy znanych zespołów oraz młodych artystów. Ma na celu promowanie polskiej muzyki oraz integrację społeczności muzycznej. Zazwyczaj odbywa się w malowniczej scenerii (w tym roku na lądowisku samolotów), co sprawia, że jest to nie tylko uczta dla ucha, ale także dla oka. To świetna okazja, aby spędzić czas z przyjaciółmi i cieszyć się muzyką na żywo.

Pol'and'Rock Festival, znany wcześniej jako Przystanek Woodstock to jednak nie tylko festiwal muzyczny, ale także miejsce, gdzie odbywa się wiele innych wydarzeń i atrakcji, takich jak np. warsztaty i panele dyskusyjne, dotyczące prawa, cyberbezpieczeństwa, sztuki, ekologii, zdrowego stylu życia czy aktywizmu społecznego, na których uczestnicy mogą zdobywać nowe umiejętności i wiedzę.

Porady prawne Infolinii biura Urzędu Ochrony Danych Osobowych

Udzielanie porad prawnych na koncercie rockowym, mimo że jest to nietypowe zjawisko, może przynieść korzyści zarówno organizatorom, jak i uczestnikom. W tym roku, na 30. Pol'and'Rock Festival, jako przedstawicielka Infolinii miałam przyjemność udzielać porad i informacji o przepisach o ochronie danych osobowych w punkcie porad zorganizowanym dzięki uprzejmości Krajowej Izby Radców Prawnych.

Stacjonarny punkt porad dotyczących ochrony danych osobowych cieszył się dużym zainteresowaniem gości festiwalu. Porady polegały na udzielaniu fachowych informacji i wskazówek dotyczących kwestii prawnych. Jako prawniczka z Urzędu Ochrony Danych Osobowych, mogłam odpowiedzieć zainteresowanym na pytania odnoszące się do ich praw i obowiązków, a także poinstruować ich, jakie kroki podjąć w konkretnej sytuacji.

8 WSPÓŁPRACA Z UODO

Infolinia Urzędu Ochrony Danych Osobowych (UODO) zajmuje się udzielaniem informacji i wsparcia w zakresie ochrony danych osobowych. Pomaga uzyskać pomoc w kwestiach związanych z przetwarzaniem danych, prawami osób, których dane dotyczą, oraz obowiązkami administratorów danych. Na co dzień, pracownicy Infolinii są dostępni w godzinach 10.00-14.00, aby odpowiedzieć na pytania obywateli, rozwiać ich wątpliwości i pomóc w zrozumieniu przepisów dotyczących ochrony danych.
Porady i informacje o działalności Urzędu Ochrony Danych Osobowych, opierają się na dwóch aktach prawnych dotyczących ochrony danych osobowych, regulujących zasady przetwarzania danych oraz prawa osób, których dane dotyczą. Pierwszym z nich jest Rozporządzenie (UE) 2016/679 (Ogólne rozporządzenie o ochronie danych, znane jako RODO) – podstawowy akt prawny w Unii Europejskiej, który wprowadza zasady dotyczące ochrony danych osobowych. RODO ma na celu zapewnienie większej kontroli obywateli nad ich danymi osobowymi oraz ujednolicenie przepisów w całej UE. Drugim ze wspomnianych aktów jest Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych – która wdraża przepisy RODO w polskim prawodawstwie. Określa m.in. zasady przetwarzania danych osobowych, prawa osób, których dane dotyczą, oraz obowiązki administratorów danych.

Konkretne pytania, jakie zadali goście festiwalu, wymagały między innymi udzielenia informacji na tematy dotyczące przetwarzania danych osobowych cudzoziemców przez organy państwowe, zarówno w sprawie legalizacji pobytu cudzoziemców na terytorium RP, w tym zawierania małżeństw z obywatelami Polski, a także ich rozwiązania; powszechnego problemu, jakim są zasady stosowania monitoringu wizyjnego wraz z możliwością nagrań audio, a także świadomych zgód związanych z monitoringiem na podstawie Kodeksu pracy; zagadnień odnoszących się do praw autorskich, badań naukowych i ochrony danych, a także przyszłych paneli dyskusyjnych. Poruszono kwestie zazębiania się praw o ochronie danych osobowych i prawa kościelnego, np. przy apostazji. Pytania odnosiły się również do prawa do prywatności oraz sposobów na zabezpieczenie się przed cyberprzestępcami.

Konsultacje prawne to często proces rozwiązywania problemów, a satysfakcja ze znalezienia skutecznego rozwiązania jest nie do przecenienia. Z radością udzielałam porad prawnych w niecodziennym, festiwalowym otoczeniu, nawiązując serdeczne relacje z uczestnikami festiwalu.

Co jeszcze oferuje festiwal?

W strefie dla dzieci, dla najmłodszych festiwalowiczów przygotowano specjalne atrakcje, takie jak animacje, warsztaty plastyczne czy zabawy, które pozwoliły im na kreatywne spędzenie czasu.

8 WSPÓŁPRACA Z UODO

Uczestnicy mogli również wziąć udział w akcjach charytatywnych. Festiwal angażuje się w różne inicjatywy charytatywne, organizując zbiórki na rzecz potrzebujących oraz promując działania prospołeczne.

Była też strefa zdrowia, w której udzielano porad dotyczących zdrowego stylu życia, można też było doświadczyć różnych form aktywności fizycznej, takich jak joga czy medytacja.

Nie sposób pominąć strefy sztuki i wystaw. Na festiwalu można poznać artystów prezentujących swoje prace, a także uczestniczyć w wystawach sztuki, które często mają na celu promowanie lokalnych twórców. Spotkania z samymi twórcami – artystami, reżyserami czy pisarzami, są okazją do rozmów o ich pracy i inspiracjach.

W ramach festiwalu odbywają się pokazy filmów, związane z tematyką festiwalu lub promujące wartości bliskie jego idei. To wszystko sprawia, że Pol'and'Rock Festival to nie tylko muzyka, ale także bogate doświadczenie kulturowe i społeczne, które polecam każdemu.

Prosto z sierpniowego weekendu na Pol'and'Rock Festival pozdrawia Państwa autorka artykułu, Izabela Maryańska, Główna Specjalistka Infolinii Urzędu Ochrony Danych Osobowych, działaczka społeczna, prawniczka obojga praw, mediatorka sądowa.

Na fotografii kolejno od lewej: Tomasz Ochmiński, zastępca dyr. Departamentu Nowych Technologii UODO, Mirosław Wróblewski, prezes UODO, Izabela Maryańska, główna specjalistka infolinii w Departamencie Komunikacji Społecznej, UODO podczas Pol'and'Rock Festival.
Zdjęcie pochodzi z zasobów własnych autorki.

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl