URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO

Nr 7–8/07–08/23

SPIS TREŚCI

Szanowni Państwo!

Niemal 3 lata po tzw. wyroku Schrems II, w sprawie C-311/18, w którym Trybunał Sprawiedliwości UE stwierdził nieważność decyzji wykonawczej Komisji Europejskiej (UE) 2016/1250 w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA, 10 lipca br. Komisja Europejska przyjęła nową decyzję stwierdzającą odpowiedni stopień ochrony danych osobowych zapewniony przez tzw. „Ramy ochrony danych UE-USA" (EU-US Data Privacy Framework).
Dla administratorów, którzy przekazują dane poza Europejski Obszar Gospodarczy do USA wydana decyzja oznacza, że organizacje z USA, ujęte w „Wykazie ram ochrony danych" prowadzonym i udostępnianym publicznie przez Departament Handlu USA, zapewniają odpowiedni stopień ochrony przekazywanych danych osobowych. Jest to zatem dobra wiadomość dla wszystkich podmiotów zainteresowanych przekazywaniem danych do państwa trzeciego bez dodatkowych zezwoleń, narzędzi czy środków uzupełniających, a na podstawie tego dokumentu prawnego.
Co wydana decyzja Komisji Europejskiej oznacza dla nas, obywateli? Przede wszystkim stwierdza odpowiedni stopień ochrony danych osobowych przekazywanych za ocean, czyli tam gdzie RODO nie obowiązuje. Ponadto przyznaje ona szereg praw podmiotom danych. Dla przykładu osoby fizyczne, których dane są przekazywane do USA na podstawie decyzji, mają do dyspozycji kilka mechanizmów dochodzenia roszczeń w postaci składania skarg zarówno na rynku europejskim, jak i amerykańskim. Wydana decyzja jest zatem dobrym krokiem w kierunku zapewnienia jednolitego, wysokiego poziomu ochrony danych osobowych zarówno przedsiębiorców europejskich, jak i amerykańskich organizacji. UODO od dawna podkreśla konieczność spójnego podejścia do ochrony danych osobowych oraz niezbędność wspólnych działań w tym zakresie.
Co ważne, decyzja ta zostanie poddana przeglądowi i ocenie już po roku od jej wydania. To bardzo ważne z kilku powodów. Po pierwsze pozwoli to na sprawdzenie, czy obecnie przyjęte przepisy mają faktycznie zastosowanie, a amerykańskie organizacje zapewniają wysoki poziom ochrony danych. Druga sprawa to coraz to nowsze rozwiązania technologiczne, które w wielu przypadkach są oparte na przetwarzaniu danych. W obliczu ciągłego rozwoju nowych technologii należy także mieć na względzie jak ważna jest ochrona danych osobowych i zapewnienie bezpieczeństwa przetwarzanych danych użytkowników, zwłaszcza przez BigTechy. Obserwując to zjawisko, dla lepszego zrozumienia technologii, potencjału jej wykorzystania, korzyści i zagrożeń Urząd podejmuje wiele inicjatyw edukacyjnych i naukowych. Najnowsza inicjatywa, jaką organ nadzorczy zamierza w tym celu zorganizować, to konferencja dotycząca rozwoju nowych technologii, o czym będziemy Państwa na bieżąco informować.

Jakub Groszkowski
Zastępca Prezesa UODO

Drodzy Czytelnicy!

Upowszechnianie w społeczeństwie wiedzy o przepisach ogólnego rozporządzenia o ochronie danych (RODO) jest jednym z podstawowych zadań organu nadzorczego. Edukacja jest wpisana w DNA Urzędu Ochrony Danych Osobowych i wszelkie działania służące jej propagowaniu wypełniamy z pełną powagą i niesłabnącym zaangażowaniem. Po latach prowadzenia z sukcesem programu edukacyjnego dla szkół i uczniów „Twoje Dane – Twoja Sprawa" i budowania wśród najmłodszych nie tylko zasobów wiedzy, ale i pozytywnych nawyków ochrony danych osobowych i prawa do prywatności, przyszedł czas na kolejne inicjatywy. Obecnie prowadzone warsztaty w ramach projektu edukacyjnego „Letnia Akademia Liderów RODO", o którym mogliście Państwo przeczytać w poprzednim wydaniu „Biuletynu UODO", potwierdzają nasze założenia o tym, jak ważna jest nieustanna edukacja w zakresie ochrony danych osobowych i prawa do prywatności. Comiesięczne wydania „Biuletynu UODO", z których każde niesie ze sobą walor edukacyjny, z pewnością można również zaliczyć do działań podnoszących poziom wiedzy o ochronie danych osobowych. Ponadto systematycznie za pośrednictwem strony internetowej www.uodo.gov.pl publikujemy materiały poradnikowe. Nie zapominamy także o organizowaniu szkoleń czy webinariów zarówno dla administracji rządowej, jak i samorządów, administratorów, czy inspektorów ochrony danych (IOD). Więcej o działaniach edukacyjnych UODO przeczytacie Państwo w wywiadzie z Anną Dudkowską, Dyrektor Departamentu Współpracy Międzynarodowej i Edukacji. Biorąc powyższe pod uwagę, organ nadzorczy nie miał żadnych wątpliwości, by objąć patronat nad cyklicznymi badaniami Krajowego Rejestru Długów oraz serwisu ChronPESEL.pl. Jesteśmy przekonani, że uzyskane wyniki z dotychczasowych trzech edycji badań i opracowane na ich podstawie raporty mają wpływ na podniesienie świadomości społecznej w obszarze ochrony danych osobowych. Więcej na temat wyników badań przeczytacie Państwo w dziale „Edukacja" w materiale „Dane osobowe – czy wiemy, jak je chronić? Omówienie wyników raportu".
Wciąż żyjemy w dynamicznie zmieniającej się rzeczywistości, a przed nami jeszcze więcej wyzwań związanych z dalszym rozwojem, już i tak wszechobecnych nowych technologii. W tym numerze zadaliśmy sobie pytanie, czym właściwie jest Internet Rzeczy i w jaki sposób wpływa na bezpieczeństwo danych osobowych użytkowników? Niewątpliwie jest jednym z najbardziej obiecujących kierunków rozwoju i może przynieść wiele korzyści.

Czy są to jednak tylko same korzyści czy może także zagrożenia? Odpowiedzi na te i inne pytania można znaleźć w dziale „Nowe technologie". O sztucznej inteligencji, która udziela odpowiedzi na zapytania przeczytacie Państwo także w materiale mec. Xawerego Konarskiego, Prezesa Stowarzyszenia Prawa Nowych Technologii.

Mówiąc o nowych technologiach, sztucznej inteligencji w kontekście ochrony danych osobowych, nie sposób nie zaprezentować komentarza na temat jakże ważnej decyzji Komisji Europejskiej o nazwie Ramy ochrony danych, która stanowi nową podstawę transferów danych osobowych pomiędzy UE i USA. O tym co wprowadza nowy mechanizm i kto może z niego skorzystać przeczytacie Państwo w materiale Ewy Kurowskiej-Tober, członka Stowarzyszenia Prawa Nowych Technologii.

W tym numerze nie zabraknie także wielu innych materiałów odnoszących się do pytań stawianych Urzędowi zarówno przez administratorów, jak i IOD, takich jak kwestie ustalenia roli w procesie przetwarzania danych osobowych.

Zachęcam Państwa do lektury.

Adam Sanocki
Dyrektor Departamentu
Komunikacji Społecznej,
Rzecznik Prasowy UODO

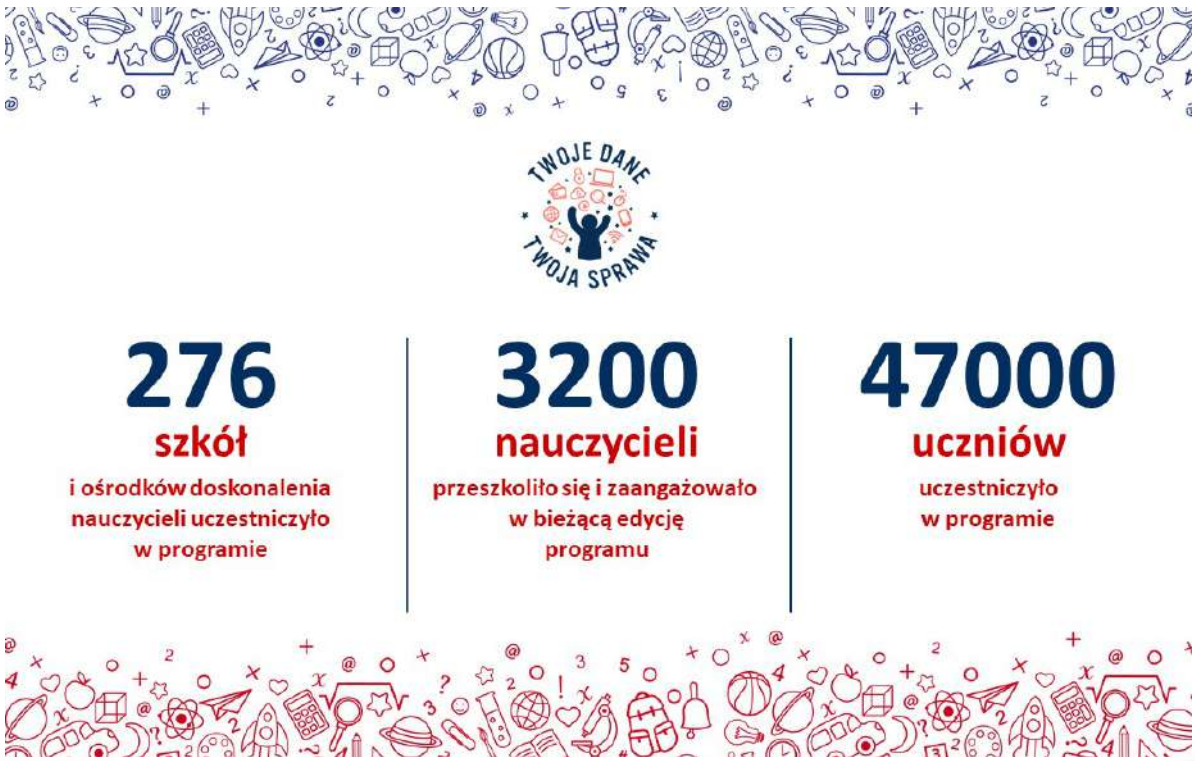
1 ROZMOWA Z EKSPERTEM

WIEDZA, ZROZUMIENIE ZASAD OCHRONY DANYCH OSOBOWYCH I ŚWIADOMOŚĆ SWOICH PRAW TO EFEKT DZIAŁAŃ EDUKACYJNYCH UODO

Anna Dudkowska, Dyrektor Departamentu Współpracy Międzynarodowej i Edukacji na temat działań edukacyjnych UODO rozmawia z Eweliną Janczylik-Foryś.

Za nami XIII edycja programu edukacyjnego UODO dla szkół „Twoje dane – Twoja sprawa". Czy może Pani podsumować tegoroczne osiągnięcia?

Bardzo nas cieszy, że przy tegorocznej edycji programu edukacyjnego „Twoje dane – Twoja sprawa" wzrosła liczba uczniów uczestniczących w inicjatywie. W minionym roku szkolnym ponad 47 tys. uczniów brało udział w zajęciach lekcyjnych, pozalekcyjnych i wydarzeniach tematycznych.
To o trzy tysiące więcej niż w poprzedniej edycji tego Programu. Co więcej ponad 3,2 tys. nauczycieli zostało przeszkolonych i zaangażowanych w działania, aby idea ochrony prywatności i danych osobowych stanowiła ważny element szkolnej edukacji. Tylko w roku szkolnym 2022/2023 zrealizowano ponad 4 tys. inicjatyw związanych z ochroną danych osobowych.



Co powoduje, że każda kolejna edycja różni się od poprzednich?

Podstawowym celem Programu jest upowszechnienie wiedzy o ochronie danych osobowych wśród uczniów i nauczycieli, aby świadomie korzystali z praw gwarantowanych przez RODO, co jest istotne w dobie gwałtowanego rozwoju nowych technologii. Biorąc pod uwagę przytoczone liczby, sądzę, że to nam się udaje. Program ma pewien schemat, dzięki czemu nasze działania są czytelne i konsekwentnie realizujemy z góry założony cel.

1 ROZMOWA Z EKSPERTEM

Działania w ramach Programu są realizowane w dwóch etapach. Po pierwsze UODO dociera z wiedzą o ochronie danych osobowych do dyrektorów placówek oświatowych i nauczycieli. W drugim etapie są edukowani uczniowie oraz całe społeczności szkolne. Pomagamy szkołom realizować ich zadania – wskazujemy drogę, jak żyć bezpiecznie w świecie pełnym wyzwań dla ochrony danych osobowych. Atutem Programu jest profesjonalne wsparcie merytoryczne ekspertów Urzędu Ochrony Danych Osobowych. Oczywiście każda edycja Programu jest inna od poprzednich, ma swój określony harmonogram, wyróżnia ją zakres tematyczny. Robimy wszystko, aby kolejne edycje Programu dostarczały nowych treści, wprowadzamy nowe pomysły. Każda edycja Programu rozpoczyna się kompleksowym szkoleniem dla nauczycieli – szkolnych koordynatorów Programu, które dostarcza im odpowiednią dawkę wiedzy, aby mogli podzielić się nią w gronie pedagogicznym. Wiedzę tę personel pedagogiczny może poszerzać w trakcie roku szkolnego, korzystając z dodatkowych szkoleń tematycznych, np. z cyklu „RODO w szkolnej ławce”. Ponadto wprowadzono porady dla nauczycieli i uczniów w postaci cyklu porad „Warto wiedzieć…”, które systematycznie dostarczają treści na temat ochrony danych oraz prywatności. W trakcie pandemii widzieliśmy potrzebę dostosowania naszego Programu do panujących wówczas warunków, czyli przekazywania wiedzy za pośrednictwem Internetu. Dużą popularnością wśród uczniów cieszył się cykl webinarów tematycznych pt. #ODOlekcje. Tematykę tych spotkań dobrano tak, aby była dla uczestników angażująca i użyteczna. Wzięto pod uwagę różne potrzeby, w tym zadbano, aby treści były dostosowane do uczniów ze szczególnymi potrzebami. W roku szkolnym 2022/2023 informacje o inicjatywach edukacyjnych można było śledzić na interaktywnej mapie inicjatyw. Zatem wprowadzamy do Programu pewne nowości, jednocześnie nie zapominając o dotychczasowych osiągnieciach i sprawdzonych metodach podnoszenia wiedzy nauczycieli i uczniów. Zagadnienia Programu dostosowujemy do bieżących potrzeb i aktualnych problemów. Dla przykładu w dobie coraz bardziej znaczącej roli nowych technologii, sztucznej inteligencji realizowaliśmy spotkania z uczniami wskazujące m.in. jak ważne są nasze dane biometryczne, uświadomiliśmy jak fake news mogą nami manipulować. Nasza oferta tematyczna jest dostosowywana do aktualnych wyzwań. Już pracujemy nad kolejną – XIV – edycją Programu. Przypomnę, nabór rusza, jak zawsze 1 września 2023 r. A widzimy jakie korzyści przynosi uczestnictwo w Programie i placówki edukacyjne także je dostrzegają, dlatego nieustannie zachęcamy szkoły do dołączenia do tej inicjatywy.

Jakie to konkretnie korzyści?

Inicjatywy podejmowane przez szkoły, służą społeczności szkolnej na wielu polach. Dzięki uczestnictwu w Programie dyrektorzy, nauczyciele poszerzają wiedzę o tym, jak poprawnie przetwarzać dane osobowe, skutecznie przeciwdziałać naruszeniom ochrony danych oraz lepiej identyfikować ryzyka związane z tymi zadaniami w placówce edukacyjnej, które wiążą się z przetwarzaniem danych osobowych.

Z kolei uczniom Program pomaga pozyskiwać wiedzę, a przez to również nabywać umiejętności, które

ułatwią im funkcjonowanie nie tylko w społeczności szkolnej, ale także w środowisku lokalnym, a w przyszłości i zawodowym.

Korzyści dla uczniów:

- wykazanie się pomysłami, umiejętnościami, talentami plastycznymi, aktorskimi i sportowymi,
- zdobycie odpowiedniej wiedzy i umiejętności praktycznych dotyczących skutecznej ochrony siebie,
- aktywne spędzenie czasu – uczniowie uczestniczą w konkursach, zabawach, warsztatach, spotkaniach z ekspertami oraz zajęciach terenowych i in.

Korzyści dla nauczycieli:

- uczestniczą w specjalistycznych szkoleniach, podczas których uzyskują wsparcie ekspertów i materiały edukacyjne,
- zdobywają wiedzę na temat realizacji obowiązków wynikających z RODO w sektorze oświaty,
- doskonalą umiejętności i warsztat edukatora w zakresie prowadzenia ciekawych zajęć z uczniami.

Korzyści dla szkół:

- umożliwia podnoszenie kwalifikacji kadrze,
- promuje szkołę w środowisku lokalnym,
- przyczynia się do podniesienia świadomości uczniów na rzecz zwiększenia ich bezpieczeństwa.

Prowadzenie programu „Twoje dane – Twoja sprawa" musi także po tylu latach skłaniać do pewnej refleksji. Czy widzi Pani jakieś tendencje?

Nasze doświadczenia w ramach realizacji programu edukacyjnego „Twoje dane – Twoja sprawa" pokazują, że dzieci i młodzież są coraz bardziej świadomi swoich praw i obowiązków wynikających z przepisów prawa. Natomiast brakuje im nadal refleksji i wiedzy praktycznej w życiu codziennym. Czasami potrzeba więcej rozwagi, mądrości życiowej i przewidywania konsekwencji swojego działania, aby bezpiecznie uczestniczyć w cyfrowej rzeczywistości. Dlatego też edukacja w obszarze ochrony danych osobowych jest taka ważna. Ponad 90 proc. uczestników Programu jest zadowolonych z przeprowadzonych zajęć i uważa, że wiedza nt. ochrony prywatności jest potrzebna w edukacji szkolnej. Uczestnicy wskazują na adekwatność tematyki Programu do realiów społeczeństwa informacyjnego, uniwersalny zakres merytoryczny zajęć. Zainteresowanie realizowaniem Programu i kontynuacją zajęć na temat ochrony danych osobowych jest coraz większe wśród uczniów i nauczycieli. Obserwujemy również bardzo duże zaangażowanie szkół w różnorodne działania dodatkowe i współpracę ze środowiskiem lokalnym. Nabyta podczas Programu wiedza oraz świadomość swoich praw, niewątpliwie ułatwi im sprawne i bezpieczne funkcjonowanie w cyfrowym świecie.

1 ROZMOWA Z EKSPERTEM

Aby kształcić młode pokolenie, świadome swoich praw i obowiązków pod względem ochrony danych osobowych, trzeba docierać z wiedzą na ten temat do dyrektorów szkół, nauczycieli i rodziców. Cele te są realizowane przez program „Twoje dane – Twoja sprawa".

Dużo mówimy o edukacji dzieci, a program „Twoje Dane – Twoja Sprawa" jest takim już sztandarowym działaniem edukacyjnym. Skąd wziął się pomysł na rozpoczęcie kolejnego projektu, jakim jest „Letnia Akademia Liderów RODO"?

„Letnia Akademia Liderów RODO" to inicjatywa edukacyjna skierowana do studentów prawa, administracji, stosunków międzynarodowych i informatyki oraz młodych absolwentów tych kierunków. Powstała ona m.in. w związku z 5. rocznicą stosowania RODO w Polsce. Inicjatywa ta stanowi nowoczesną formę kształcenia, dzięki której młodzi ludzie czerpią z wiedzy i doświadczenia od aktualnych ekspertów z zakresu ochrony danych osobowych. Jak słusznie Pani zauważyła, wiele robimy na rzecz podnoszenia świadomości dzieci. Dostrzegamy jednocześnie, że kiedy młody człowiek kończy szkołę ponadpodstawową, to nauczanie na dalszym etapie o ochronie danych osobowych i prawie do prywatności nie jest wystarczające, a niekiedy nie jest w ogóle kontynuowane. A przecież ochrona danych osobowych to dziedzina, która dotyczy każdego człowieka. Nie zawsze sami możemy dokonać wyboru w jaki sposób i jakie dane są o nas przetwarzane. Często decydują o tym przepisy prawa, interes publiczny. Są jednak sytuacje, w których to my sami decydujemy i mamy wpływ na to, kto i kiedy posługuje się naszymi danymi. Mamy wpływ na ochronę naszej prywatności poprzez ograniczanie udostępniania danych w mediach społecznościowych czy w różnych formularzach zakupowych. Dlatego ważna jest wiedza, zrozumienie zasad ochrony danych osobowych, i świadomość swoich praw.

Proszę powiedzieć, czego dokładnie nauczą się młodzi ludzie podczas zajęć?

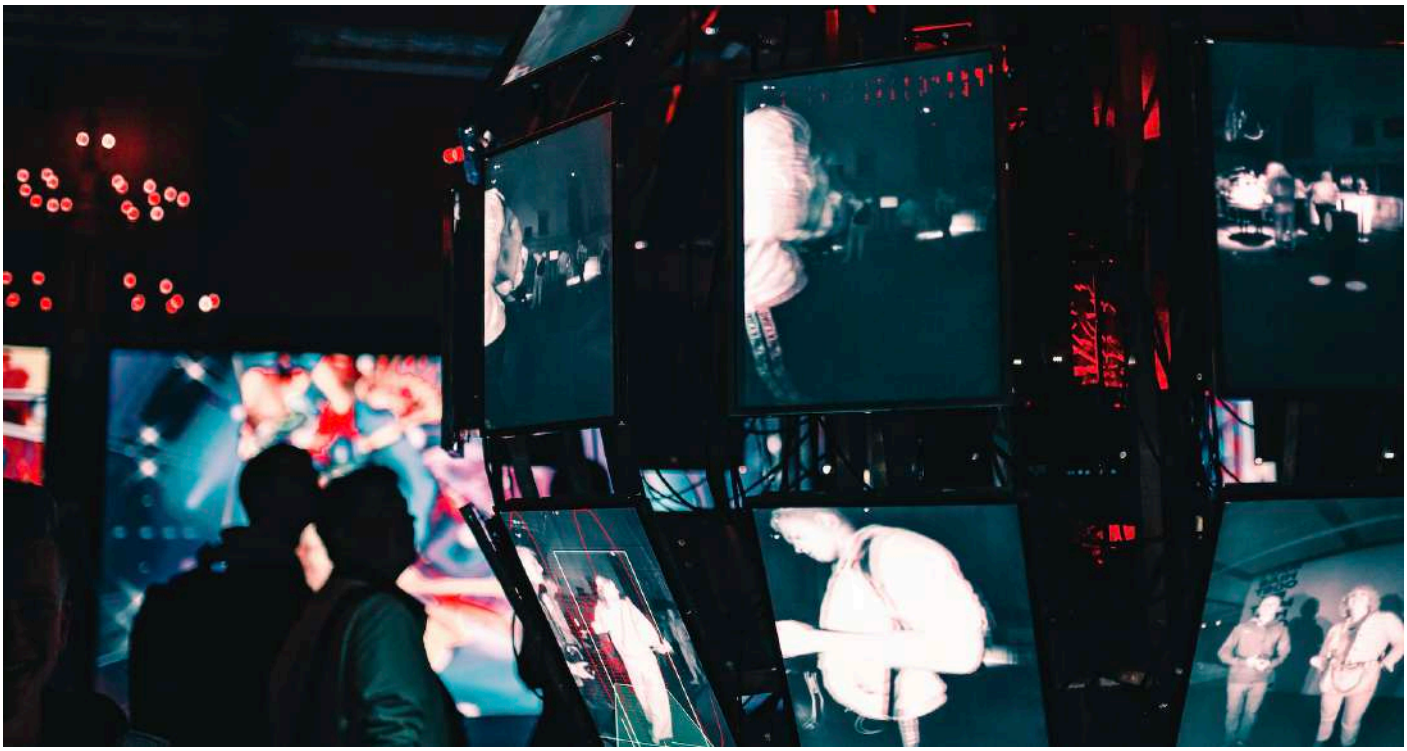
Uczestnicy Akademii, biorą udział w wykładach prowadzonych przez pracowników Urzędu, którzy poruszają między innymi tematy związane z kontrolami i naruszeniami ochrony danych osobowych, zadaniami inspektorów ochrony danych, współpracą UODO z Europejską Radą Ochrony Danych. Dowiedzą się, jak wygląda procedura nakładania administracyjnych kar pieniężnych przez Prezesa Urzędu, jak prawidłowo złożyć skargę do Urzędu Ochrony Danych Osobowych na naruszenie przepisów RODO oraz jak chronić dane osobowe w dobie postępu technologicznego. Zaproszeni eksperci przybliżą zagadnienia związane z ochroną danych osobowych w kontekście cyberbezpieczeństwa i nowych technologii.

Zdajemy sobie sprawę, że ochrona danych osobowych i ochrona prywatności są szczególnie ważne w kontekście przetwarzania ogromnej liczby informacji przez zaawansowane systemy informatyczne. Dlatego UODO przygląda się temu zagadnieniu w trosce o ochronę danych osobowych obywateli.

1 ROZMOWA Z EKSPERTEM

Zwróciłam uwagę, że w naszej rozmowie oprócz edukacji często porusza Pani zagadnienie nowych technologii i cyberbezpieczeństwa.

Zagadnienia dotyczące relacji pomiędzy ochroną danych osobowych a nowymi technologiami, sztuczną inteligencją, od dawna są przedmiotem zainteresowania UODO. Dla lepszego ich zrozumienia, Urząd podejmuje wiele inicjatyw edukacyjnych i naukowych. Oprócz organizowania wydarzeń kierowanych do ekspertów, temat sztucznej inteligencji był także przedstawiany uczniom w ramach programu edukacyjnego UODO „Twoje dane – Twoja sprawa". Uczyliśmy wówczas czym jest SI i jakie może stwarzać wyzwania dla ochrony danych osobowych oraz jak ważne jest zachowanie stosownego umiaru i rozwagi w korzystaniu z dobrodziejstw nowoczesnych technologii.



Dziękuję za rozmowę.

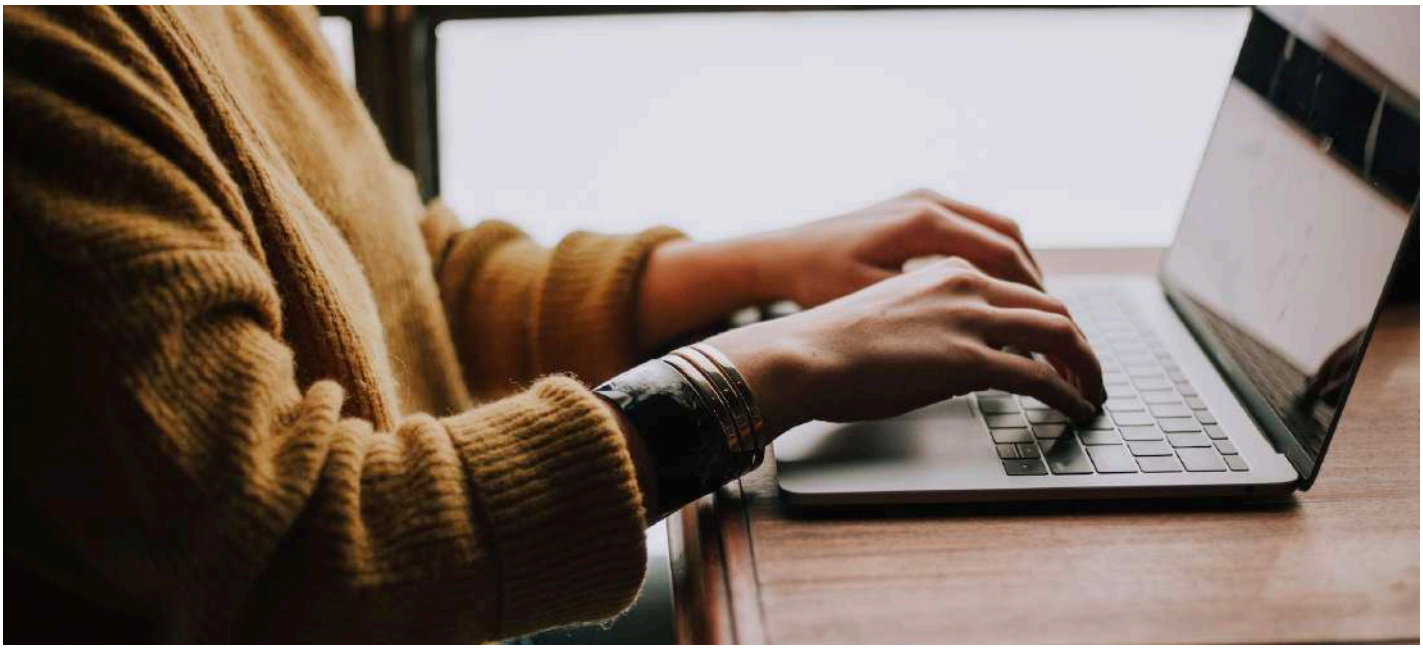
ROZPATRYWANIE WNIOSKU PRACOWNIKA O PRACĘ ZDALNĄ W ZWIĄZKU Z NIEPEŁNOSPRAWNOŚCIĄ OSOBY TRZECIEJ

Pracodawca, rozpatrując wniosek pracownika o całkowitą pracę zdalną w związku z niepełnosprawnością osoby trzeciej, powinien ograniczyć pozyskiwanie informacji o niepełnosprawności tej osoby. Nieuzasadnione wydaje się żądanie przekazania orzeczenia o niepełnosprawności osoby, nad którą pracownik sprawuje opiekę. Wystarczające powinno być złożenie przez pracownika stosownego oświadczenia, a po jego ewentualnej weryfikacji sporządzenie stosownej adnotacji i dołączenie jej do akt osobowych pracownika.

Przepisy ustawy z 26 czerwca 1974 r. – Kodeks pracy (art. 22^1 § 3 pkt 3) uprawniają pracodawcę do żądania od pracownika podania danych osobowych obejmujących m.in. dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy. Jednym z takich uprawnień jest prawo do świadczenia pracy na warunkach pracy zdalnej. Jednak sposób udokumentowania okoliczności z wniosku pracownika o pracę zdalną, o której mowa w art. 67^{19} § 6 Kodeksu pracy, tj. m.in. sprawującego opiekę nad innym członkiem najbliższej rodziny lub inną osobą pozostającą we wspólnym gospodarstwie domowym, posiadającą orzeczenie o niepełnosprawności albo orzeczenie o znacznym stopniu niepełnosprawności nie został wskazany wprost w przepisach obowiązującego prawa. Niemniej zgodnie z art. 22^1 § 5 Kodeksu pracy udostępnienie pracodawcy danych osobowych następuje w formie oświadczenia osoby, której dane dotyczą, a pracodawca może żądać udokumentowania danych osobowych osób, o których mowa w art. 22^1 § 3 Kodeksu pracy, w zakresie niezbędnym do ich potwierdzenia. Przy czym podkreślenia wymaga, że do realizacji tego przepisu niezbędne jest przestrzeganie zasady minimalizacji danych, o której mowa w art. 5 ust. 1 lit. c RODO. Stanowi ona, że dane osobowe muszą być: adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.
Dla administratora (w tym przypadku pracodawcy) oznacza to obowiązek poszukiwania takich rozwiązań, które z jednej strony pozwolą na prawidłową weryfikację złożonych oświadczeń, zaś z drugiej strony na pozyskiwanie, a następnie przechowywanie danych niezbędnych do realizacji zakładanego celu. Biorąc pod uwagę szczególny charakter uprawnienia pracownika składającego wniosek o pracę zdalną w związku z niepełnosprawnością osoby trzeciej pozostającej we wspólnym gospodarstwie domowym, zasadne byłoby odpowiednie udokumentowanie przesłanki stanowiącej podstawę wniosku. Uprawnienie takie pracodawca może wywodzić z art. 300 Kodeksu pracy. Przesądza on, że w sprawach nieunormowanych przepisami prawa pracy do stosunku pracy stosuje się odpowiednio przepisy Kodeksu cywilnego, jeżeli nie są one sprzeczne z zasadami prawa pracy. Z kolei art. 6 Kodeksu cywilnego stanowi, że ciężar udowodnienia faktu spoczywa na osobie, która z faktu tego wywodzi skutki prawne.

2 UODO SYGNALIZUJE

Jednak analizując kwestię rozpatrywania wniosku pracownika o pracę zdalną w związku z niepełnosprawnością osoby trzeciej nie można pominąć zasady ograniczenia przechowywania danych, o której mowa w art. 5 ust. 1 lit. e RODO. Stosownie do niej dane osobowe muszą być: przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą.



Zatem rozpatrując wniosek pracownika o pracę zdalną, o której mowa w art. 67^{19} § 6 Kodeksu pracy, należałoby ograniczyć powzięcie informacji o niepełnosprawności osoby trzeciej do sporządzenia stosownej adnotacji i jej dołączenia do akt osobowych pracownika zgodnie z umocowaniem zawartym w § 3 ust. 2 lit. w rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej z 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej.
Jednocześnie, gdy pracodawca spełni wskazane wyżej warunki, przyjąć należy, że dane osobowe dotyczące osoby trzeciej objęte orzeczeniem o niepełnosprawności przedłożonym przez pracownika przetwarza on na podstawie art. 6 ust. 1 lit. c oraz art. 9 ust. 2 lit. b RODO.

STATUS KOMISJI KONKURSOWEJ NA DYREKTORA SZKOŁY

Administratorem danych osobowych kandydatów na stanowisko dyrektora szkoły lub placówki jest organ prowadzący szkołę lub placówkę, który na podstawie art. 63 ust. 14 Prawa oświatowego powołuje komisję konkursową.

W ostatnim okresie jeden z IOD zwrócił się do UODO z prośbą o rozstrzygnięcie wątpliwości dotyczących statusu komisji konkursowej powoływanej przez organ prowadzący do przeprowadzenia konkursu na stanowisko dyrektora szkoły podstawowej. Jak wskazał, w myśl art. 63 ust. 14 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe, w celu przeprowadzenia konkursu organ prowadzący szkołę lub placówkę powołuje komisję konkursową w składzie:

- po trzech przedstawicieli organu prowadzącego szkołę lub placówkę i organu sprawującego nadzór pedagogiczny,
- po dwóch przedstawicieli rady pedagogicznej i rady rodziców,
- po jednym przedstawicielu organizacji związkowych reprezentatywnych w rozumieniu ustawy o Radzie Dialogu Społecznego, wyłonionym spośród członków ich jednostek organizacyjnych albo jednostek organizacyjnych organizacji związkowych wchodzących w skład reprezentatywnych organizacji związkowych, zrzeszających nauczycieli, obejmujących swoim zakresem działania szkołę lub placówkę, w której konkurs się odbywa.

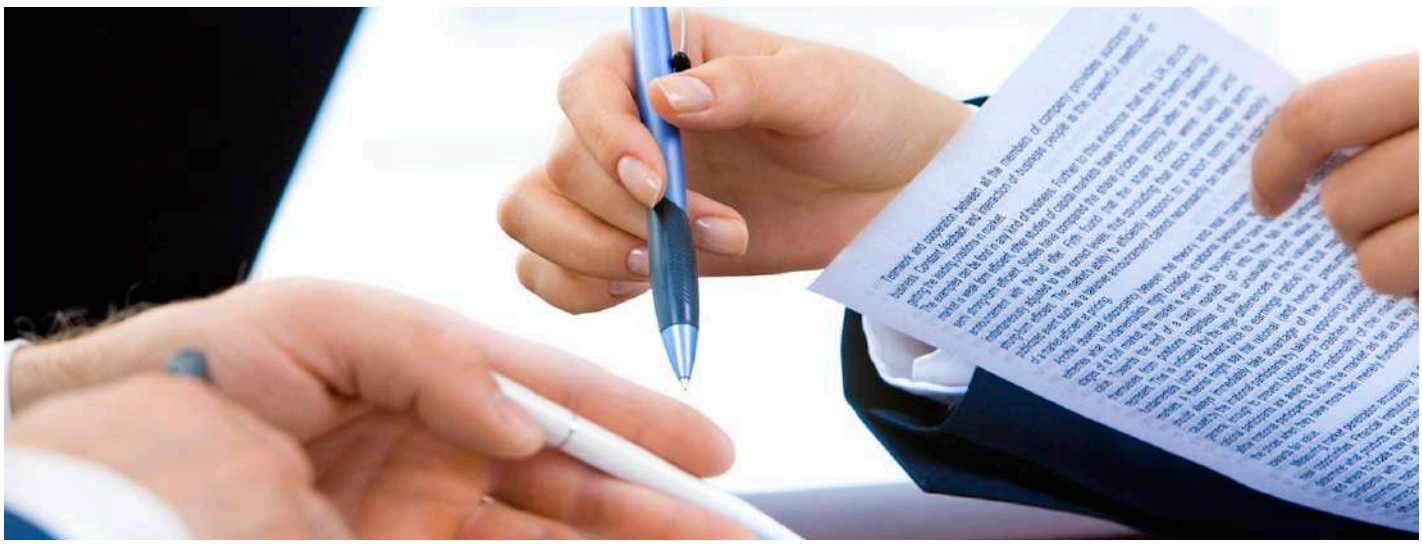
Z kolei zasady pracy komisji definiuje rozporządzenie Ministra Edukacji Narodowej z 11 sierpnia 2017 r. w sprawie regulaminu konkursu na stanowisko dyrektora publicznego przedszkola, publicznej szkoły podstawowej, publicznej szkoły ponadpodstawowej lub publicznej placówki oraz trybu pracy komisji konkursowej. IOD, biorąc te regulacje pod uwagę, prosił o wskazanie podmiotu będącego administratorem danych osobowych kandydatów na stanowisko dyrektora i wyjaśnienie kwestii nadawania członkom komisji konkursowej upoważnień do przetwarzania danych osobowych kandydatów ubiegających się w konkursie o stanowisko dyrektora szkoły. W odpowiedzi Urząd wskazał, że to organ prowadzący szkołę lub placówkę, który na podstawie art. 63 ust. 14 Prawa oświatowego powołuje komisję konkursową, jest administratorem danych osobowych kandydatów na stanowisko dyrektora szkoły lub placówki. Wobec tego to również organ prowadzący jest zobowiązany do zastosowania środków zapewniających bezpieczeństwo przetwarzania danych osobowych. Jeśli organ ten przyjął, że nadawanie upoważnień jest jednym ze stosowanych u niego środków organizacyjnych mających na celu zapewnienie odpowiedniej ochrony danych i kontroli nad procesem przetwarzania danych, wówczas środek taki powinien dotyczyć nie tylko osób na stałe zatrudnionych u administratora, ale także osób, którym administrator zlecił określone prace i które z tego powodu mają mieć dostęp do danych osobowych – w tym przypadku członkom komisji konkursowej. Tak też wskazywaliśmy w odpowiedzi na pytanie **„Czy administrator powinien udzielać upoważnień do przetwarzania danych?”.**

3 WYBRANE DECYZJE UODO

ZAKOŃCZENIE UMOWY I BRAK ZGODY WYKLUCZA KONTYNUACJĘ KORESPONDENCJI

Upomnienie za wysyłanie wiadomości e-mail pomimo braku wyrażonej na nie zgody po ustaniu stosunku prawnego. Taką decyzję podjął organ nadzorczy po rozpatrzeniu skargi jaka wpłynęła na nieprawidłowości w procesie przetwarzania danych osobowych, które polegały na nieuwzględnieniu żądania usunięcia danych osobowych skarżącego.

Administrator pozyskał dane osobowe skarżącego w związku z zawarciem umów o świadczenie usług telekomunikacyjnych. Jednak gdy skarżący zrezygnował z tych usług i wniósł o usunięcie danych osobowych, w odpowiedzi administrator poinformował go, że zgodnie z prawem, spółka musi przechowywać jego dane osobowe oraz dane o wykonanych usługach telekomunikacyjnych przez 12 miesięcy od ostatniego połączenia bądź próby połączenia. Abonent został również poinformowany, że po upływie tego terminu, jego dane osobowe zostaną usunięte bez konieczności ponawiania zgłoszenia. Pomimo zakończenia wykonywania umowy, spółka wysłała wiadomość e-mail do skarżącego. Korespondencja ta zawierała informację o zmianach w cennikach usług telekomunikacyjnych. Treść wiadomości wskazywała na to, że skarżący wciąż korzysta z usług spółki. Podczas postępowania organ nadzorczy uzyskał od administratora wyjaśnienia, że ten nadal przetwarza dane osobowe skarżącego, aby wypełnić obowiązki wynikające z przepisów Ordynacji podatkowej, w celach archiwizacji danych i dokumentów, udzielania odpowiedzi na pisma, wnioski i reklamacje oraz ustalania, obrony i dochodzenia roszczeń.



Ponadto administrator wykazywał, że posiadał podstawę prawną wysłania informacji o zmianach cennika, przedkładając kopie dokumentacji związanych z zawartymi ze skarżącym umowami. Organ nadzorczy uznał jednak, że administrator nie wykazał dysponowania zgodą na przetwarzanie danych osobowych, za co udzielił spółce upomnienia.

3 WYBRANE DECYZJE UODO

Przesłanki legalizujące przetwarzanie

Przepisem uprawniającym administratorów danych do przetwarzania zwykłych danych osób fizycznych jest art. 6 ust. 1 RODO. Dopuszcza on przetwarzanie danych tylko gdy spełniona jest jedna z przesłanek wskazanych w tym przepisie. Katalog przesłanek wymienionych w art. 6 ust. 1 RODO jest zamknięty, a każda z nich ma charakter autonomiczny i niezależny. Oznacza to, że przesłanki te, co do zasady, są równoprawne, a wobec tego spełnienie co najmniej jednej z nich stanowi o zgodnym z prawem przetwarzaniu danych osobowych. Niezależnie od zgody osoby, której dane dotyczą (art. 6 ust. 1 lit. a RODO), przetwarzanie danych osobowych jest dopuszczalne m.in.: wtedy, gdy jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (art. 6 ust. 1 lit. b RODO), gdy jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. lit. c RODO) jak również gdy jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem (art. 6 ust. 1 lit. f RODO).

Co dla administratora jest niezbędne do realizacji obowiązku prawnego?

W omawianej sprawie administrator do czasu zakończenia wykonywania umów, przetwarzał dane osobowe skarżącego, ponieważ było to niezbędne do ich realizacji i wykonania (art. 6 ust. 1 lit. b RODO). Po tym jak abonent zrezygnował z usług telekomunikacyjnych i wniósł o całkowite usunięcie jego danych osobowych, administrator przetwarzał jego dane osobowe z uwagi na obowiązek przechowywania dokumentów wytworzonych w związku z umowami wypowiedzianymi przez skarżącego na podstawie przepisów Ordynacji podatkowej. Takie przetwarzanie danych stanowi realizację przesłanki określonej w art. 6 ust. 1 lit. c RODO, czyli jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. Tym samym, biorąc pod uwagę przepisy szczegółowe, w tym przypadku nie było możliwe uwzględnienie żądania skarżącego w zakresie usunięcia jego danych osobowych przez administratora i dlatego UODO odmówił uwzględnienia wniosku skarżącego w tym zakresie.

Co jest niezbędne dla realizacji prawnie uzasadnionych interesów administratora?

Podczas postępowania administrator wskazał także, że przetwarza dane osobowe skarżącego na podstawie przesłanki z art. 6 ust. 1 lit. f RODO. Należy podkreślić, że prawidłowość przetwarzania danych osobowych w oparciu o ten przepis uzależniona jest od wykazania, że przetwarzanie jest niezbędne dla realizacji prawnie uzasadnionych interesów administratora.

Ponadto interes ten nie powinien mieć nadrzędnego charakteru wobec interesu lub podstawowych praw i wolności osoby, której dane dotyczą.

Zgodnie z motywem 47 RODO podstawą prawną przetwarzania mogą być prawnie uzasadnione interesy administratora, w tym administratora, któremu mogą zostać ujawnione dane osobowe, lub strony trzeciej, o ile w świetle rozsądnych oczekiwań osób, których dane dotyczą, opartych na ich powiązaniach z administratorem nadrzędne nie są interesy lub podstawowe prawa i wolności osoby, której dane dotyczą.

Administrator wyjaśnił, że przetwarza dane osobowe skarżącego w celu dochodzenia roszczeń lub obrony przed nimi oraz do celów archiwizacyjnych. W ocenie UODO dochodzenie przez podmiot roszczeń finansowych jest prawnie uzasadnionym interesem i w tym sensie nadrzędnym nad prawami i wolnościami osoby, której dane dotyczą, bowiem dochodzenie roszczeń nie stanowi nieproporcjonalnego ograniczenia tych praw i wolności. Dodatkowo administrator w trakcie postępowania nie wykazał, aby toczyło się jakiekolwiek postępowanie dotyczące dochodzenia roszczeń, wobec czego nie można uznać, aby istniał prawnie uzasadniony interes uprawniający go do przetwarzania danych osobowych skarżącego. Administrator w swoich wyjaśnieniach powoływał się również na przepisy Prawa telekomunikacyjnego, które dotyczą odpowiedzialności za niewykonanie lub nienależyte wykonanie usług telekomunikacyjnych, a konkretnie na przepis, zgodnie z którym roszczenia przedawniają się z upływem 12 miesięcy od końca okresu rozliczeniowego, w którym zakończyła się przerwa w świadczeniu usługi telekomunikacyjnej, albo od dnia, w którym usługa została nienależycie wykonana lub miała być wykonana. Zdaniem UODO w tej sprawie oprócz tego, że nie toczyło się jakiekolwiek postępowanie dotyczące dochodzenia roszczeń, to samo istnienie przepisu dotyczącego terminu przedawnienia roszczeń nie uprawnia do zachowania danych osobowych na wypadek konieczności ewentualnego dochodzenia lub obrony roszczeń, które dopiero mogą zaistnieć w przyszłości. W ocenie UODO przepisy Prawa telekomunikacyjnego obecnie nie stanowią podstawy prawnej do przetwarzania danych osobowych skarżącego.

Prawo do zapomnienia?

Na podstawie art. 17 ust. 1 RODO osoba, której dane dotyczą ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z okoliczności wskazanych w tym przepisie. Administrator prawidłowo poinformował skarżącego, że nie może usunąć jego danych osobowych, na dzień udzielania odpowiedzi, ponieważ cały czas obowiązywały go przepisy Prawa telekomunikacyjnego i 12-miesięczny okres przechowywania danych dotyczących wykonanych usług telekomunikacyjnych od ostatniego połączenia bądź próby połączenia.

4 NARUSZENIA I KONTROLE

WYJĄTKI OD ZASADY ZGŁASZANIA NARUSZEŃ ORGANOWI NADZORCZEMU

RODO wprowadza szczegółowe procedury postępowania w przypadku naruszenia ochrony danych osobowych. Standardowo, zgodnie z art. 33 ust. 1 RODO, w przypadku naruszenia ochrony danych osobowych, administrator niezwłocznie – jednak nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – musi je zgłosić organowi nadzorczemu. Mimo to istnieją pewne sytuacje, w których notyfikacja nie jest konieczna. Przyjrzyjmy się zatem wyjątkom od tej reguły.

Stosownie do brzmienia ww. przepisu, naruszenie, w przypadku którego „jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych" (ang. „is unlikely to result in risk to the rights and freedoms of natural person") nie musi być zgłoszone Prezesowi UODO. W praktyce stosowania przepisów o ochronie danych osobowych można zauważyć, iż kwestia ta uległa różnym interpretacjom, zaś „małe prawdopodobieństwo" wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych zrównywane jest niekiedy z kategorią tzw. „niskiego ryzyka".

Czym jest „małe prawdopodobieństwo"?

Tymczasem w literaturze przedmiotu wskazuje się na konieczność postrzegania ryzyka w kategoriach: brak ryzyka – ryzyko – wysokie ryzyko. „Małe prawdopodobieństwo" zaistnienia skutku w postaci naruszenia praw lub wolności osoby, której dane dotyczą, powinno być natomiast utożsamiane z sytuacją, w której oceniający posiada przesłanki pozwalające na stwierdzenie, że skutek ten nie urzeczywistni się w ogóle – a zatem wtedy, gdy mówimy o „braku ryzyka". Warto zauważyć, że w polskiej wersji RODO użyto sformułowania „mało prawdopodobne", zaś w angielskiej – terminu „unlikely". Wyraz ten ma silniejsze znaczenie niż nasz rodzimy odpowiednik i służy do określenia czegoś, co jest raczej nieprawdopodobne, wątpliwie lub niemal niemożliwe. Polska odmiana wydaje się być mniej stanowcza, co może prowadzić do rozbieżności interpretacyjnych.

Kiedy więc nie trzeba zgłaszać naruszenia?

EROD sygnalizuje w Wytycznych 9/2022 w sprawie zgłaszania naruszeń ochrony danych osobowych zgodnie z RODO (Guidelines 9/2022 on personal data breach notification under GDPR – version 2.0), że przykładem incydentu niepodlegającego obowiązkowi notyfikacyjnemu może być sytuacja, w której objęte naruszeniem dane osobowe są już publicznie dostępne, a ich ujawnienie nie stwarza dodatkowego ryzyka dla osoby, której dane te dotyczą. Innym przedstawionym przykładem jest naruszenie poufności danych osobowych zaszyfrowanych przy użyciu odpowiedniego algorytmu. W takim przypadku, gdy poufność klucza szyfrującego nie została naruszona – tj. nie został on skompromitowany w wyniku jakiegokolwiek incydentu bezpieczeństwa i został wygenerowany w taki sposób, że nie może zostać złamany przez osobę nieuprawnioną za pomocą dostępnych środków

technicznych – dane pozostają w praktyce niemożliwe do odczytania. W związku z tym, jeżeli administrator uczynił dane osobowe zasadniczo niezrozumiałymi dla osób nieupoważnionych oraz zapewnił jednocześnie istnienie niezawodnych kopii zapasowych tych danych (neutralizując potencjalne skutki naruszenia ich integralności i dostępności), naruszenie może nie wymagać zgłoszenia organowi nadzorczemu, ponieważ jest mało prawdopodobne, aby stanowiło ono zagrożenie dla praw lub wolności osób fizycznych.

Co należy wziąć pod uwagę?

Pomimo to należy pamiętać, że analiza ryzyka jest procesem dynamicznym. Zmieniające się okoliczności mogą wpłynąć na ocenę incydentu, a jeżeli klucz szyfrujący zostanie skompromitowany lub z biegiem czasu wykazana zostanie podatność w oprogramowaniu służącym do szyfrowania, zgłoszenie nadal może być wymagane. Wszystko to zależy od bieżącej oceny prawdopodobieństwa naruszenia praw lub wolności osób, których dane dotyczą. W związku z tym EROD zaznacza, że przy wyborze oprogramowania szyfrującego administratorzy powinni dokładnie zbadać jakość oraz przemyśleć właściwą implementację dostępnych rozwiązań, a także ocenić ich adekwatność wobec zidentyfikowanych zagrożeń. W tym kontekście niezwykle istotne jest również regularne testowanie, mierzenie i ocenianie wdrożonych środków – metody obecnie uznane za odpowiednie przez ekspertów w dziedzinie bezpieczeństwa w niedługim czasie mogą stać się przestarzałe, nie gwarantując już proporcjonalnego poziomu ochrony danych. Podkreślenia wymaga też, iż utrata bezpiecznie zaszyfrowanych danych osobowych nadal może stanowić naruszenie podlegające obowiązkowi zgłoszenia w zależności od tego, czy – i w jakim czasie – administrator będzie w stanie przywrócić ich dostępność.

Rola administratora danych

Podsumowując, choć RODO określa ścisłe zasady postępowania w przypadku naruszeń ochrony danych osobowych, istnieją pewne sytuacje, w których zgłoszenie naruszenia organowi nadzorczemu może nie być wymagane. Kluczową rolę w tej kwestii pełni jednak administrator danych, który poprzez ciągłą analizę i monitorowanie ryzyka musi samodzielnie decydować o konieczności notyfikacji naruszeń. Odpowiednio przeprowadzony proces oceny ryzyka może przynieść korzyści nie tylko w kontekście zgodności z prawem, ale także w budowaniu zaufania wśród osób, których dane są przetwarzane, cementując reputację administratora jako odpowiedzialnego i wiarygodnego partnera.

4 NARUSZENIA I KONTROLE

PRZEWODNIK PO PRAWACH OSÓB W SIS

Komitet Skoordynowanego Nadzoru opublikował 13 kwietnia 2023 r. na swojej stronie przewodnik dotyczący korzystania z praw osób, których dane dotyczą: prawo dostępu, sprostowania i usunięcia danych w Systemie Informacyjnym Schengen (SIS).

Skoordynowany Komitet Nadzoru (CSC) to grupa krajowych organów nadzorczych i Europejskiego Inspektora Ochrony Danych (EIOD), która zapewnia skoordynowany nadzór nad wielkoskalowymi systemami informatycznymi oraz nad organami, urzędami i agencjami UE.

Czym jest SIS?

System Informacyjny Schengen zawiera dwie szerokie kategorie informacji: wpisy dotyczące obywateli państw spoza strefy Schengen i wpisy dotyczące przedmiotów, które zostały wprowadzone do SIS do celów powrotu nielegalnie przebywających obywateli państw trzecich [1], odpraw granicznych [2] oraz współpracy policyjnej i współpracy wymiarów sprawiedliwości [3]. W odniesieniu do wpisów dotyczących osób, SIS obejmuje następujące kategorie osób, których dane dotyczą:

- obywatele państw trzecich podlegający odmowie wjazdu lub pobytu w strefie Schengen lub podlegający procedurom powrotu,
- osoby poszukiwane w celu aresztowania, wydania lub ekstradycji (w przypadku państw stowarzyszonych),
- osoby zaginione (w tym osoby narażone na niebezpieczeństwo, którym należy uniemożliwić podróżowanie, np. dzieci zagrożone uprowadzeniem przez rodzica, w przypadku których istnieje ryzyko, że staną się ofiarami handlu ludźmi lub zostaną zwerbowane jako zagraniczni, terrorystyczni bojownicy),
- osoby poszukiwane, których obecność jest wymagana do celów postępowania prowadzonego przez organy wymiaru sprawiedliwości,
- osoby objęte kontrolą niejawną, rozpytaniami kontrolnymi lub kontrolą szczególną,
- poszukiwane nieznane osoby powiązane z przestępstwem (np. osoby, których odciski palców znaleziono na broni użytej w przestępstwie),
- informacje o obywatelach państw trzecich będących w zainteresowaniu Unii Europejskiej (tzw. „wpisy informacyjne").

4 NARUSZENIA I KONTROLE

Kategorie danych w SIS

Jeżeli wpis dotyczy osoby (z wyjątkiem nieznanej osoby poszukiwanej), informacje muszą zawsze zawierać:

- nazwisko,
- datę urodzenia,
- powód dokonania wpisu,
- płeć,
- odesłanie do decyzji będącej podstawą wpisu,
- podstawę decyzji o odmowie wjazdu i pobytu (w stosownych przypadkach),
- działania, które należy podjąć,
- ostatnią datę okresu dobrowolnego wyjazdu, w stosownych przypadkach,
- informację, czy powrotowi towarzyszy zakaz wjazdu.

Dodatkowo, wpis może również zawierać informacje takie jak: wszelkie szczególne, obiektywne cechy fizyczne niepodlegające zmianom; miejsce urodzenia; fotografie; odciski palców; obywatelstwo (obywatelstwa); informacje, czy dana osoba jest uzbrojona, agresywna lub czy zbiegła; organ dokonujący wpisu; odsyłacze do innych wpisów dokonanych w SIS zgodnie z art. 48 rozporządzenia (UE) 2018/1861 lub art. 63 rozporządzenia (UE) 2018/1862.
Jeżeli wpis dotyczy nieznanych osób poszukiwanych, przetwarzane mogą być wyłącznie dane daktyloskopijne, tj. kompletne lub niekompletne zestawy odcisków linii papilarnych palców lub dłoni, które z powodu ich niepowtarzalnego charakteru i układu cech szczególnych umożliwiają przeprowadzenie dokładnych i dających jednoznaczne wyniki porównań odnośnie do tożsamości danej osoby.

Jakie prawa przysługują osobom, których dane są przetwarzane w SIS

Dokonywanie przez uprawnione organy wpisów do SIS dotyczących osób i przedmiotów może następować bez wiedzy i zgody osób, których dane dotyczą. Dlatego obywatele państw trzecich mogą korzystać z praw związanych z ich danymi osobowymi przetwarzanymi w SIS, przewidzianych w art. 15, 16 i 17 RODO [4] oraz w art. 14 i 16 ust. 1 i 2 dyrektywy (UE) 2016/680 [5], oraz zgodnie z rozporządzeniami w sprawie SIS [6]. Ponadto osoby, których dane dotyczą, są uprawnione do korzystania ze środków ochrony prawnej w celu wyegzekwowania takich praw [7].
W związku z tym osobom, których dane dotyczą, przysługują następujące prawa:

- prawo dostępu do dotyczących ich danych przetwarzanych w SIS,
- prawo do sprostowania nieprawidłowych danych,
- prawo do usunięcia danych, jeśli były one przechowywane niezgodnie z prawem,
- prawo wniesienia do sądu lub właściwego organu żądania o dostęp do informacji,

ich sprostowania, usunięcia lub ich uzyskanie lub o zapłatę odszkodowania w związku z wpisami ich dotyczącymi.

Szczegółowe informacje na temat realizowania praw osób, których dane są przetwarzane w SIS, znajdują się w **przewodniku** Komitetu Skoordynowanego Nadzoru oraz na **stronie internetowej** UODO.

Przypisy

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1860 z dnia 28 listopada 2018 r. w sprawie użytkowania Systemu Informacyjnego Schengen do celów powrotu nielegalnie przebywających obywateli państw trzecich (Dz. Urz. UE. L 312 z 07.12.2018 r., str. 1)

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1861 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, zmiany konwencji wykonawczej do układu z Schengen oraz zmiany i uchylenia rozporządzenia (WE) nr 1987/2006 (Dz. Urz. UE. L 312 z 07.12.2018 r., str. 14)

[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1862 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmiany i uchylenia decyzji Rady 2007/533/WSiSW oraz uchylenia rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1986/2006 i decyzji Komisji 2010/261/UE (Dz. Urz. UE. L 312 z 07.12.2018 r., str. 56)

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE. L 119 z 4.05.2016 r., str. 1, z późn. zm.)

[5] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE. L 119 z 4.05.2016 r., str. 89, z późn. zm.)

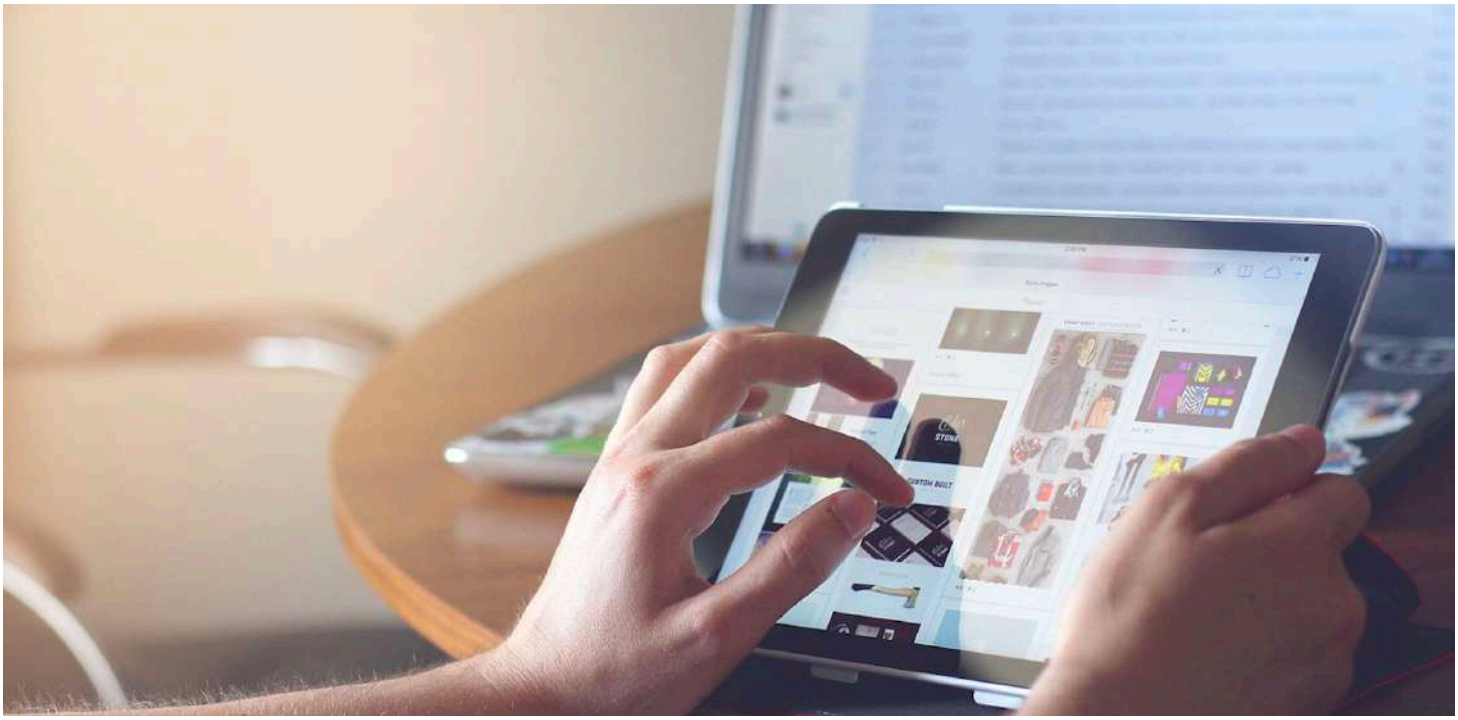
[6] Zob. art. 53 rozporządzenia (UE) 2018/1861 i art. 67 rozporządzenia (UE) 2018/1862.

[7] Zob. art. 54 rozporządzenia (UE) 2018/1861 i art. 68 rozporządzenia (UE) 2018/1862.

5 NOWE TECHNOLOGIE

INTERNET RZECZY A BEZPIECZEŃSTWO DANYCH OSOBOWYCH UŻYTKOWNIKÓW

Szybki rozwój Internetu rzeczy (IoT), pomimo możliwych korzyści, budzi obawy dotyczące ochrony danych osobowych i prywatności. Czym właściwie jest Internet Rzeczy i w jaki sposób wpływa na bezpieczeństwo danych osobowych użytkowników?



W czerwcowym numerze „Biuletynu UODO" pisaliśmy o inteligentnych zabawkach bazujących na Internecie Rzeczy. To tylko jeden z wielu przykładów tej technologii, bo możliwości zastosowania IoT są bardzo szerokie: od tzw. urządzeń ubieralnych (np. smartwatche, które mierzą aktywność, liczbę wykonanych kroków, czy tętno), poprzez sektor medyczny (np. kamizelka do badania EKG), aż po usprawnienie transportu, logistyki i wiele innych. Zastosowanie urządzeń technologii IoT w tych wszystkich obszarach bez wątpienia podnosi komfort życia użytkowników. Niestety, jest to także ogromna baza wiedzy o ich nawykach, a co za tym idzie, może nieść za sobą również potencjalne zagrożenia. Wśród najczęściej wymienianych znajdują się problemy z prywatnością danych, błędy w oprogramowaniu, czy niewystarczający poziom bezpieczeństwa oprogramowania, co z kolei może prowadzić do utraty przetwarzanych w IoT danych (w tym danych wrażliwych), ich kradzieży, czy też próby ingerencji w algorytmy odpowiedzialne za ich przetwarzanie.
IoT to koncepcja umożliwiająca interoperacyjność różnorodnych teleinformatycznych systemów, za pośrednictwem których mogą być gromadzone, przetwarzane i wymieniane dane.
Jednym z najważniejszych aspektów w obszarze IoT jest prywatność, która wymaga skrupulatnie przemyślanych rozwiązań chroniących dane zarówno biznesowe, jak i prywatne użytkowników.

5 NOWE TECHNOLOGIE

Internet Rzeczy niewątpliwie jest jednym z najbardziej obiecujących kierunków rozwoju i może przynieść wiele cennych korzyści. Należy jednak zwrócić uwagę, że wraz z rozwojem tej technologii, pojawiają się nowe rodzaje zagrożeń, dlatego istotnym jest, aby proponowane rozwiązania były zgodne z wymogami prawnymi dotyczącymi prywatności danych. Ponadto kwestie związane z prywatnością muszą być uwzględnione już na etapie projektowania, zgodnie z zasadą privacy by design, która promuje przestrzeganie prywatności i ochrony danych na wszystkich etapach rozwoju technologicznego. Z kolei użytkownicy urządzeń IoT muszą mieć świadomość na temat możliwych zagrożeń, ale również przysługujących im praw, gdyż niewystarczająca wiedza na ten temat może prowadzić do wielu nadużyć ze strony producentów, a co za tym idzie braku kontroli nad przetwarzaniem przekazanych informacji, które często stanowią dane osobowe.

Minimalizacja ryzyka związanego z bezpieczeństwem danych w urządzeniach IoT w 7 krokach:

1. **Wybierz zaufane urządzenia!**
   Wybieraj dostawców urządzeń IoT renomowanych producentów, dbających o bezpieczeństwo i regularnie udostępniających aktualizacje oprogramowania. Przed zakupem sprawdź pod kątem bezpieczeństwa opinie i rankingi producentów i urządzeń.
2. **Zapoznaj się z polityką prywatności!**
   Przyszły administrator systemu IoT powinien spełnić obowiązek informacyjny, dostarczając wszystkich niezbędnych informacji na temat zasad przetwarzania i ochrony danych użytkowników urządzeń IoT.
3. **Aktualizuj oprogramowanie!**
   Regularnie aktualizuj oprogramowanie urządzeń IoT, aby korzystać z najnowszych poprawek zabezpieczeń. Monitoruj i instaluj dostępne aktualizacje, poprawiające bezpieczeństwo urządzeń, tak szybko jak to możliwe.
4. **Stosuj silne hasła i uwierzytelnianie!**
   Tam gdzie to możliwe, stosuj uwierzytelnianie dwuskładnikowe lub inne metody uwierzytelniania, zwiększające poziom bezpieczeństwa.
5. **Zabezpiecz sieć i unikaj korzystania z publicznych połączeń Wi-Fi do zarządzania urządzeniami IoT!**
   Nie loguj się do urządzeń IoT podczas korzystania z otwartych sieci, ponieważ może to grozić udostępnieniem Twoich danych cyberprzestępcom.
6. **Ogranicz zbieranie danych!**
   Upewnij się, że wszelkie dane, które będą zbierane są niezbędne, a ich przekazywanie jest konieczne do sprawnego funkcjonowania tego urządzenia.
7. **Miej świadomość!**
   Zarówno praw jakie przysługują Ci w związku z korzystaniem z inteligentnych urządzeń (m.in. dostęp do swoich danych, sprostowania danych, usunięcia danych, ograniczenia przetwarzania danych, przenoszenia danych i wniesienia sprzeciwu), jak i na temat potencjalnych zagrożeń.

6 SPRAWY MIĘDZYNARODOWE

ANU TALUS PRZEWODNICZY EUROPEJSKIEJ RADZIE OCHRONY DANYCH

Europejska Rada Ochrony Danych wybrała w maju 2023 roku Anu Talus na stanowisko przewodniczącej. Finka zastąpiła dotychczasową przewodniczącą Andreę Jelinek.

Anu Talus jest szefową Fińskiego Urzędu Ochrony Danych, którą to funkcję będzie teraz łączyć z rolą przewodniczącej Europejskiej Rady Ochrony Danych.

– Jestem zaszczycona i wdzięczna za wybór na stanowisko Przewodniczącej Europejskiej Rady Ochrony Danych i postrzegam to jako wyraz uznania ze strony moich kolegów szefów organów ochrony danych. Jako ściśle zintegrowana sieć organów ochrony danych, Europejska Rada Ochrony Danych ma ważne zadanie zapewnienia 450 milionom Europejczyków takiego samego stopnia ochrony danych, niezależnie od ich miejsca zamieszkania – powiedziała Anu Talus.

– Część nowo przyjętego prawodawstwa cyfrowego UE pokrywa się z RODO. W przyszłości kluczowe znaczenie ma zapewnienie spójności ram prawnych związanych z ochroną danych, zabezpieczenie kompetencji Europejskiej Rady Ochrony Danych i uniknięcie fragmentacji. Szare strefy nie są korzystne dla nikogo, ani dla osób, których dane osobowe chronimy, ani dla podmiotów gospodarczych, które potrzebują pewności prawa – dodała nowa przewodnicząca EROD.

Zgodnie z art. 73 RODO, EROD wybiera jednego przewodniczącego i dwóch wiceprzewodniczących spośród swoich członków zwykłą większością głosów w głosowaniu tajnym. Ich kadencja trwa pięć lat, z możliwością jednokrotnego przedłużenia. Przewodniczący EROD nadzoruje wszystkie zadania Rady i zapewnia ich terminową realizację. Reprezentuje on EROD.

Europejska Rada Ochrony Danych wybrała również Irene Loizidou Nikolaidou (z organu ochrony danych Cypru) na stanowisko nowej wiceprzewodniczącej, która zastąpi ustępującego wiceprzewodniczącego Ventsislava Karadjova.

Wiceprzewodniczący Europejskiej Rady Ochrony Danych Aleid Wolfsen (z Holandii) został wybrany 15 maja 2019 r.; jego kadencja zakończy się 15 maja 2024 r.

Europejska Rada Ochrony Danych (EROD) jest niezależnym organem europejskim, który przyczynia się do spójnego stosowania przepisów o ochronie danych w całej Unii Europejskiej i promuje współpracę między organami ochrony danych w UE. Europejska Rada Ochrony Danych została ustanowiona na mocy ogólnego rozporządzenia o ochronie danych (RODO).

Źródło: **komunikat EROD z 25 maja 2023 r. na temat wyboru nowego przewodniczącego**

6 SPRAWY MIĘDZYNARODOWE

ZA NAMI 44. POSIEDZENIE PLENARNE T-PD

W Strasburgu w dniach 14-16 czerwca 2023 r. odbyło się 44. posiedzenie plenarne Komitetu Konsultacyjnego Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych (Komitetu T-PD). Członkiem Komitetu T-PD z ramienia Rzeczypospolitej Polskiej jest Urząd Ochrony Danych Osobowych, którego przedstawiciel wziął czynny udział w posiedzeniu.

Wśród najważniejszych punktów obrad posiedzenia wskazać należy przyjęcie dwóch dokumentów: Wytycznych w sprawie ochrony danych przy przetwarzaniu danych osobowych do celów przeciwdziałania praniu pieniędzy/finansowaniu terroryzmu i Wzorcowych klauzul umownych dotyczących przekazywania danych osobowych.
Ponadto uczestnicy posiedzenia omawiali m.in. pierwszy projekt wytycznych w sprawie ochrony danych, w tym podczas korzystania z danych biometrycznych, w ramach głosowania i wyborów.

Raport z posiedzenia dostępny jest na stronie Rady Europy

6 SPRAWY MIĘDZYNARODOWE

FRANCJA: JASNOWIDZENIE ONLINE KONTRA RODO

Francuski organ ochrony danych (CNIL) nałożył na KG COM karę w wysokości 150 000 euro, ponieważ spółka nie wywiązała się ze swoich obowiązków wynikających z RODO i francuskiej ustawy o ochronie danych. W szczególności firma gromadziła nadmierną ilość danych, a także dane wrażliwe bez uprzedniej i wyraźnej zgody oraz nie zapewniła w wystarczającym stopniu bezpieczeństwa danych.

KG COM prowadzi kilka stron internetowych oferujących swoim klientom odczyty jasnowidzenia przez czat lub telefon. Po opublikowaniu w 2020 r. artykułu prasowego ujawniającego naruszenie ochrony danych osobowych z udziałem spółki, CNIL przeprowadził trzy postępowania w sprawie KG COM. W wyniku postępowań CNIL stwierdził kilka naruszeń, w szczególności dotyczących systematycznego nagrywania rozmów telefonicznych, gromadzenia danych medycznych i informacji dotyczących orientacji seksualnej, przechowywania danych bankowych bez zgody osób fizycznych, a także naruszenie obowiązku zgłoszenia naruszenia ochrony danych oraz zasad dotyczących plików cookie. W konsekwencji nałożono dwie administracyjne kary pieniężne: – karę w wysokości 120 000 euro za naruszenie RODO. Kara ta została nałożona we współpracy z kilkoma europejskimi organami ochrony danych (z Belgii, Luksemburga, Włoch, Hiszpanii, Portugalii, Bułgarii, Berlina i Irlandii) w ramach mechanizmu kompleksowej współpracy, ponieważ KG COM ma klientów i potencjalnych klientów w kilku państwach członkowskich Unii Europejskiej; – karę w wysokości 30 000 euro za nieprzestrzeganie przepisów dotyczących korzystania z plików cookie (art. 82 francuskiej ustawy o ochronie danych).

Główne naruszenia objęte sankcjami

Spółka systematycznie nagrywała wszystkie rozmowy telefoniczne między operatorami telefonicznymi a potencjalnymi klientami, a także między wróżbitami a klientami, w celu sprawdzenia jakości usług, udowodnienia zawarcia umowy i reagowania na potencjalne nakazy sądowe. Chociaż spółka zaprzestała obecnie telefonicznych odczytów jasnowidzenia, a tym samym nagrywania rozmów telefonicznych, nie przedstawiła żadnego uzasadnienia dla wcześniejszej potrzeby systematycznego nagrywania wszystkich rozmów w tych celach.

Spółka przechowywała dane konta bankowego swoich klientów dłużej, niż jest to absolutnie konieczne do sfinalizowania transakcji, w celach zwalczania nadużyć finansowych i ułatwiania klientom kolejnych zakupów nowych sesji jasnowidzenia. Jeśli podstawą prawną przechowywania danych konta bankowego do celów zwalczania nadużyć finansowych jest uzasadniony interes, podstawa ta nie ma zastosowania do przechowywania danych do kolejnych zakupów, na które firma powinna uzyskać zgodę osób fizycznych. Podczas odczytów klienci mogli podawać informacje o swoim stanie zdrowia i orientacji seksualnej, które były odnotowywane w rejestrach przechowywanych przez jasnowidzów.

Spółka powinna była uzyskać uprzednią wyraźną zgodę swoich klientów na przetwarzanie ich danych wrażliwych. Zwykła chęć skorzystania z usług wróżbiarskich i spontaniczne ujawnienie wrażliwych informacji nie stanowią wyraźnej zgody. Spółka powinna była również przekazać osobom, których dane dotyczą, szczegółowe informacje na temat gromadzenia ich danych wrażliwych.
Spółka wdrożyła niewystarczająco silne hasła do kont użytkowników i nie zabezpieczyła dostępu do strony internetowej www.voyance-en-direct.tv za pomocą protokołu http zamiast protokołu https, co naraziło dane na ryzyko ataków hakerskich lub wycieków. Korzystała również z mechanizmu szyfrowania danych bankowych, który miał luki w zabezpieczeniach.
We wrześniu 2020 roku spółka została poinformowana przez dziennikarza, który dostarczył jej próbkę bazy danych, że doszło do naruszenia ochrony danych. Spółka nie zgłosiła jednak CNIL naruszenia ochrony danych. Uznała, że nie mogła zaobserwować naruszenia ochrony danych ze względu na zamknięcie serwera i brak przechowywania logów na serwerze przez podmiot przetwarzający. Spółka mogła jednak zidentyfikować naruszenie ochrony danych, porównując przykładowe dane dostarczone przez dziennikarza ze swoją bazą danych. Spółka, ponieważ jest administratorem danych, miała obowiązek zgłosić naruszenie ochrony danych, nawet jeśli naruszenie to było spowodowane błędem, który można przypisać podmiotowi przetwarzającemu.
CNIL zauważył brak baneru informującego o plikach cookie i umieszczenie trzech plików cookie na terminalu użytkownika bez jego zgody i po wejściu na stronę internetową. Następnie spółka ustawiła baner informacyjny, który jednak nie pozwalał użytkownikom na odmowę umieszczenia plików cookie tak łatwo, jak na ich akceptację.

Źródło: **decyzja organu nadzorczego**

7 EDUKACJA

DANE OSOBOWE – CZY WIEMY, JAK JE CHRONIĆ? OMÓWIENIE WYNIKÓW RAPORTU

Raport „Dane osobowe – czy wiemy jak je chronić?" przedstawia wnioski z trzeciej już edycji badania pt. „Wiedza na temat bezpieczeństwa ochrony danych osobowych w Polsce" przeprowadzonego pod patronatem Urzędu Ochrony Danych Osobowych i Instytutu Prawa Ochrony Danych Osobowych przez Krajowy Rejestr Długów oraz serwis ChronPESEL.pl. Dla omówienia jego wyników UODO zorganizował webinarium, które odbyło się 29 czerwca 2023 r.

Badanie, podobnie jak przy poprzednich edycjach, zostało przeprowadzone w maju 2023 roku metodą CAWI na reprezentatywnej grupie 1007 respondentów przez IMAS International.

Numer PESEL na pierwszym miejscu

Zastępca Prezesa UODO Jakub Groszkowski po powitaniu prelegentów i uczestników webinarium, podkreślił jak ważne są działania edukacyjne Urzędu, w tym współpraca w ramach przygotowanego badania. Następnie odniósł się do postawionego po raz pierwszy w tegorocznej edycji pytania: Co zdaniem respondentów wchodzi w skład danych osobowych? W swoich odpowiedziach badani najczęściej wskazywali numer PESEL (92%). W dalszej kolejności imię i nazwisko (89,5%) oraz adres zamieszkania (84%). Co może nieco zaskakiwać, dopiero na czwartym miejscu znalazł się numer dowodu tożsamości (78%), chociaż dla respondentów w wieku 55–64 lata wskaźnik ten był znacząco wyższy (88%). Zdecydowanie mniej ankietowanych uznało za dane osobowe numer telefonu (49%), co istotne i w tym wypadku dla jednej z grup wiekowych wskaźnik ten był wyraźnie wyższy – 65% dla osób w wieku 18–24 lata. Wizerunek (np. utrwalony na fotografii) został wskazany przez 45%, a odciski palców przez 39% ankietowanych. Co ciekawe, za dane osobową zaledwie 29% badanych uznało informacje o stanie zdrowia. Jako ostatnie badani wskazali adres IP (23%), dane o lokalizacji np. w telefonie komórkowym (22%) i w końcu numer resjestracyjny samochodu (16%).
Przechodząc do interpretacji przedstawionych powyżej wyników, Jakub Groszkowski, Zastępca Prezesa UODO, zaznaczył, że tak wysoki procent wskazań numeru PESEL świadczy o tym, jak bardzo

ważna i unikatowa jest dla obywateli ta informacja. Podkreślił również, że od początku istnienia Urzędu była ona traktowana przez organ nadzorczy w sposób szczególny i cieszy, że to podejście znajduje tak pozytywne odzwierciedlenie w odpowiedziach respondentów.
Z kolei Andrzej Kulik, dyrektor Departamentu Analiz Rynkowych i Komunikacji w KRD, zwrócił uwagę, że dominuje raczej „wąskie podejście" i do danych osobowych respondenci w większości zaliczają te dane, które umożliwiają ich bezpośrednią identyfikację, np. nr PESEL i numer dowodu osobistego, imię i nazwisko, adres zamieszkania. Natomiast dopiero co drugi ankietowany (z ważnym wyjątkiem najmłodszej grupy respondentów w wieku 18–24 lata, gdzie wskaźnik ten wyniósł 65%), zaklasyfikował numer telefonu do kategorii danych osobowych. Przedstawione wyniki sprzyjają przyjęciu ogólnej konstatacji, że dla ponad połowy badanych, dane osobowe umożliwiające pośrednią identyfikację, są znacznie mniej intuicyjne niż te, które uplasowały się na pierwszych pozycjach.

Diabeł tkwi w szczegółach

Interpretując wyniki badania, Andrzej Kulik, ekspert KRD, zwrócił również uwagę, że wzorem roku poprzedniego, prawie 90% respondentów deklaruje, iż wie jak chronić swoje dane osobowe.
W oderwaniu od pozostałej części badania taki rezulat mógłby napawać optymizmem, jak jednak podkreślił ekspert „diabeł tkwi w szczegółach". Nadal bowiem zdecydowaną pewnością może się pochwalić zaledwie 15% ankietowanych i podobnie jak w latach poprzednich większą pewnością odznaczają się młodsi respondenci w przedziale wiekowym 18–34 lata. W przypadku osób starszych powyżej 55 roku życia wskaźnik ten wynosi zaledwie 10%, co jego zdaniem potwierdza, iż zaobserwowana w poprzednich latach różnica pokoleniowa nadal się utrzymuje. Również wzorem poprzednich edycji badania, największe zagrożenie dla bezpieczeństwa swoich danych osobowych ankietowani upatrywali w działalności przestępców wyłudzających dane (42%). Na drugim miejscu znalazły się wycieki danych (z firm prywatnych i instytucji państwowych). Jednak w tegorocznej edycji, liczba wskazań zwiększyła się tutaj o kilka punktów procentowych (38%) – w latach 2022 i 2021 było to odpowiednio – 33,5 i 34,5%. Również 86% Polaków deklaruje, że potrafi rozpoznać fałszywy e-mail, SMS lub telefon, w którym przestępcy podszywają się pod znaną firmę lub instytucję. Ale absolutną pewność ma tylko co piąty ankietowany. Zbliżone do wyników z lat poprzednich były również wskazania odnośnie działań, jakie należy podjąć w wypadku wyłudzenia lub kradzieży danych osobowych. Wzorem roku ubiegłego niewiele ponad połowa badanych (55,5%) zadeklarowało, że wie jak się zachować w wypadku zaistnienia takiego incydentu. Jako organ, do którego należy się zgłosić w pierwszej kolejności, badani wskazywali policję (85%). Wciąż jednak wielu ankietowanych zaznaczało UODO, jako instytucję, do której należy zgłaszać sprawy wyłudzenia danych czy kradzieży tożsamości (51,5%).

7 EDUKACJA

Sufity statystyczne cieszą, ale nadal nie wszyscy instalują antywirusy

Włączając się w interpretację wyników, Wiesław Paluszyński, prezes Polskiego Towarzystwa Informatycznego oraz przewodniczący Sektorowej Rady do spraw Kompetencji Telekomunikacja i Cyberbezpieczeństwo, zwrócił uwagę na istnienie zjawiska tzw. sufitu statystycznego, a więc osiągnięcia pewnego bardzo wysokiego wyniku, którego przekroczenie jest już niemożliwe przy uwzględnieniu pewnych metod badawczych. Odnosiło się to do tych odpowiedzi badanych, które oscylowały wokół wyniku 90%. W sekcji „Lista grzechów – niebezpieczne zachowania" raportu „Dane osobowe. Czy wiemy, jak je chronić?" cieszy bowiem, że aż 92% badanych zadeklarowało, że nie klika w linki otrzymane w e-mailu lub SMS-ie oraz nie otwiera e-maili niewiadomego pochodzenia. Poza tym, aż 94% badanych nie podaje numeru PESEL, jeżeli nie jest to absolutnie konieczne. Niepokoić może z kolei, iż nadal część respondentów w ogóle nie ma zainstalowanych programów antywirusowych (15% na laptopie/komputerze, 26% w telefonie/na smartfonie), 26% stosuje te same hasła do różnych kont logowania i tylko 36% weryfikuje regulaminy i polityki prywatności.

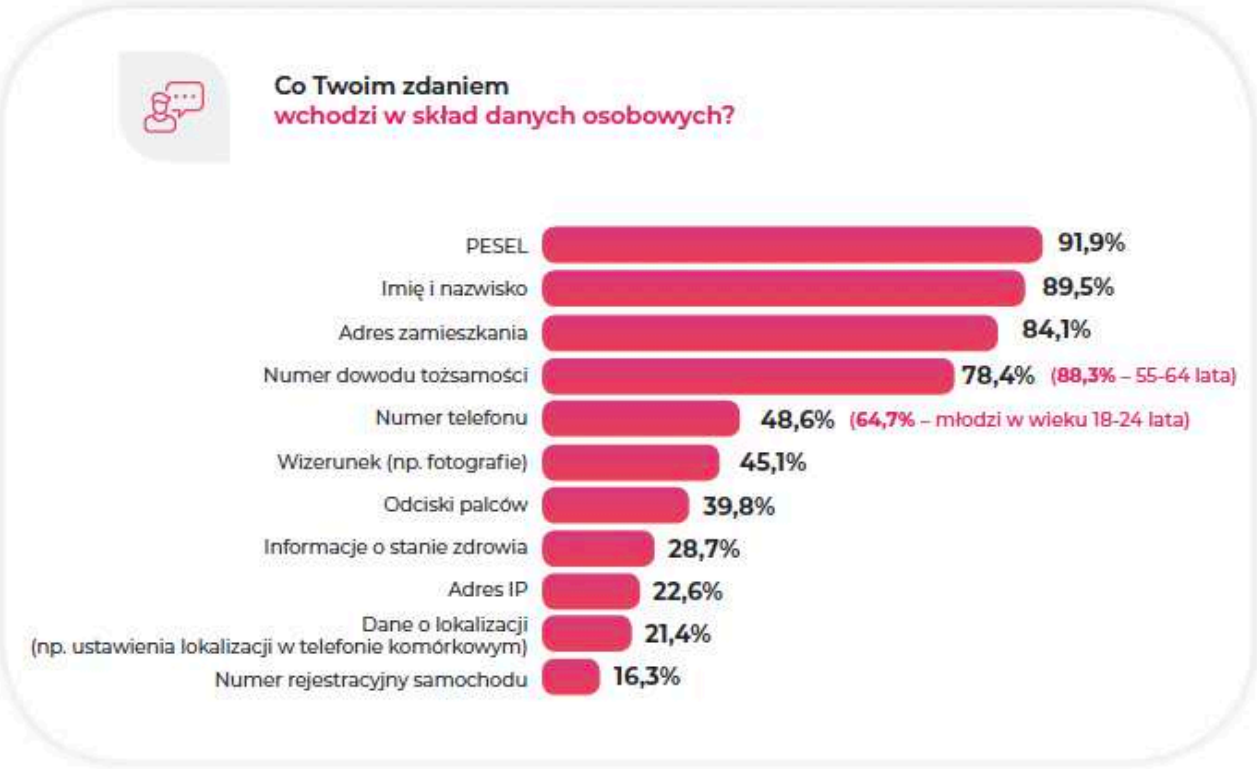
Jacek Młotkiewicz, Dyrektor Departamentu Kontroli i Naruszeń, podkreślił, jak ważne dla uniknięcia wycieku danych, jest posiadanie odpowiednich zabezpieczeń technicznych, np. w postaci najnowszych aktualizacji porgramów antywirusowych pochodzących od producenta. Na tym tle szczególnie niepokojące było spostrzeżenie, iż część respondentów w ogóle nie korzysta, z wydawałoby się, tak podstawowych zabezpieczeń. Szczególnie niepokojące wydaje się to w zestawieniu z częścią badania, w której co prawda 60% ankietowanych wskazało, że zna skutki ewentualnego naruszenia ochrony danych osobowych, co oznacza jednak, że dla pozostałych 40% respondentów wciąż nie są znane ewentualne konsekwencje takiego wycieku. Na pierwszym miejscu, wzorem poprzednich edycji badania, jako ewentualne następstwo takiego wycieku została zaznaczona możliwość zaciągnięcia zobowiązań finansowych (89%) oraz kradzież tożsamości (77%). Nadal prawie ¾ Polaków nie wie, kto powinien zająć się neutralizacją skutków wycieku danych. Na pierwszym miejscu zostały wskazane policja i prokuratura (65,9%). Najmniejsza liczba wskazań odnosiła się natomiast do osoby, której dane wyciekły (37,5%).

7 EDUKACJA

Działania edukacyjne wciąż potrzebne

Tegoroczną edycję badania można spuentować, że pomimo istnienia tzw. sufitów statystycznych i wyników, które napawają zdecydowanym optymizmem, wciąż potrzebne są działania edukacyjne, zwłaszcza w tych obszarach, gdzie deklarowana wiedza nie pokrywa się z rzeczywistymi działaniami oraz tam, gdzie pewne grupy wiekowe wciąż nie mogą nadążyć za najmłodszymi respondentami. Ekspert serwisu ChronPESEL.pl Bartłomiej Drozd po raz kolejny podkreślił, iż również na indywidulanych użytkownikach spoczywa odpowiedzialność za bezpieczeństwo ich danych osobowych. Biorąc pod uwagę wyniki odzwierciedlające rozumienie przez badanych pojęcia „danych osobowych" wydaje się również wskazane podejmowanie działań edukacyjnych w przybliżaniu podstawowych pojęć definicyjnych RODO. Jakub Groszkowski, Zastępca Prezesa UODO jako miejsce, które mogłoby służyć pełnieniu tak różnorodnej roli edukacyjnej, wskazał niedawno powstały Instytut Prawa Ochrony Danych Osobowych, który również po raz pierwszy w tym roku objął patronat nad badaniem i prezentacją jego wyników.

Raport pt. „Dane osobowe – czy wiemy, jak je chronić? jest dostępny na stronie **www.uodo.gov.pl** w dziale „Aktualności".
Zapraszamy do lektury!



8 WSPÓŁPRACA Z UODO

Instytut Prawa Ochrony Danych Osobowych, który powstał z inicjatywy UODO zawarł 29 czerwca 2023 r. porozumienie ze Stowarzyszeniem Prawa Nowych Technologii.
Poniżej prezentujemy opracowania przedstawicieli SPNT

NOWA PODSTAWA TRANSFERÓW DANYCH OSOBOWYCH POMIĘDZY UE I USA - RAMY OCHRONY DANYCH. DO KOGO ZNAJDZIE ZASTOSOWANIE I JAK Z NIEJ SKORZYSTAĆ?

10 lipca 2023 roku Komisja Europejska przyjęła, trzecią już z kolei, decyzję, tym razem o nazwie Ramy ochrony danych (ang. EU-U.S. Data Privacy Framework), stwierdzającą adekwatny poziom ochrony danych osobowych w Stanach Zjednoczonych porównywalny z poziomem Unii Europejskiej – w miejsce poprzednich podstaw UE Safe Harbor i Privacy Shield uchylonych wyrokami Trybunału Sprawiedliwości Unii Europejskiej.

Podobnie jak w przypadku swoich poprzedników, Ramy ochrony danych umożliwiają certyfikowanym firmom amerykańskim, które zobowiązują się przestrzegać Zasad Ram ochrony danych (zawartych w załączniku I do Decyzji Komisji), otrzymywanie danych osobowych z Unii Europejskiej bez konieczności polegania na zatwierdzonych przez UE mechanizmach przekazywania danych, takich jak standardowe klauzule umowne (SCC) lub wiążące reguły korporacyjne (BCR). Dla prawie 3000 firm amerykańskich, które utrzymały swoje certyfikaty Tarczy prywatności od czasu decyzji Schrems II, nowa decyzja o adekwatności powinna pozwolić im na stosunkowo szybkie skorzystanie z nowej podstawy transferu. Firmy nieposiadające obecnie certyfikatu będą musiały rozpocząć proces certyfikacji w programie od zera. W najbliższym czasie spodziewamy się także przyjęcia analogicznej decyzji przez Wielką Brytanię, a następnie prawdopodobnie także przez Szwajcarię. Kierowana przez Maxa Schremsa organizacja NOYB („None of Your Business") już zapowiedziała podjęcie kroków w celu unieważnienia najnowszej decyzji Komisji Europejskiej. Przypomnijmy, że dwa wcześniejsze mechanizmy – Safe Harbor oraz Privacy Shield – zostały unieważnione przez Trybunał Sprawiedliwości Unii Europejskiej wyrokami w tak zwanych sprawach Schrems I oraz Schrems II – nazwanymi tak od nazwiska wspomnianego wyżej austriackiego aktywisty, którego wieloletni spór z Facebookiem, a obecnie z Meta, zaowocował skierowaniem do TSUE pytań prejudycjalnych.

Kto może skorzystać z nowej podstawy transferów

Przede wszystkim należy pamiętać, że Ramy ochrony danych nie mają zastosowania do wszystkich podmiotów w Stanach. Podobnie jak w przypadku wcześniejszej Tarczy prywatności, nowy mechanizm ograniczony będzie do transferów danych do amerykańskich firm nadzorowanych przez amerykańską Federalną Komisję Handlu (FTC) lub Departament Transportu (DOT). FTC ma szerokie uprawnienia wobec firm zaangażowanych w handel, nie ma jednak nadzoru m.in. nad organizacjami

non-profit, większością instytucji depozytowych (banki, federalne organizacje kredytowe oraz instytucje oszczędnościowo-pożyczkowe) i przewoźnikami. Nie obejmie więc przypadków, w których odbiorcą danych będą przykładowo amerykańskie instytucje finansowe jak banki bądź operatorzy telekomunikacyjni, nie podlegający FTC i DOT. oraz instytucje oszczędnościowo-pożyczkowe) i przewoźnikami. Nie obejmie więc przypadków, w których odbiorcą danych będą przykładowo amerykańskie instytucje finansowe jak banki bądź operatorzy telekomunikacyjni, nie podlegający FTC i DOT. Amerykańskie organizacje, które mają wątpliwości co do tego czy podlegają jurysdykcji FTC lub DOT mogą skontaktować się ze specjalnym zespołem działającym w ramach Departamentu Handlu. Podmioty z siedzibą w Stanach Zjednoczonych, które wcześniej samodzielnie certyfikowały swoje zobowiązanie do przestrzegania zasad Tarczy prywatności UE-USA, muszą przestrzegać teraz nowych zasad określonych Ramami ochrony danych, w tym dostosowując swoje polityki prywatności do nowych wymagań do 10 października 2023 r. Organizacje te nie muszą składać oddzielnego, wstępnego oświadczenia o samocertyfikacji, aby uczestniczyć w nowym programie i mogą natychmiast zacząć polegać na decyzji dotyczącej adekwatności, aby swobodnie otrzymywać dane osobowe z Unii Europejskiej. Z perspektywy europejskiej organizacji eksportującej dane osobowe do USA kluczowe będzie zatem uzyskanie od kontrahentów zza oceanu informacji o tym czy podlegają nowemu mechanizmowi oraz uwzględnienie odpowiednich gwarancji w umowach. W przypadku transferów, w stosunku do których nie będzie możliwe poleganie na tym mechanizmie, europejskie firmy eksportujące dane osobowe za ocean będą musiały w dalszym ciągu stosować standardowe klauzule umowne lub wiążące reguły korporacyjne, a także – w zależności od poziomu ryzyka danego transferu – ewentualne dodatkowe zabezpieczenia techniczne oraz organizacyjne.

Co wprowadza nowy mechanizm?

Mechanizm Ramy ochrony danych UE-USA wprowadza szereg nowych wiążących zabezpieczeń takich jak ograniczenie dostępu amerykańskich służb wywiadowczych do danych dotyczących Europejczyków do tego, co jest niezbędne i proporcjonalne, oraz ustanowienie sądu zajmującego się kwestiami ochrony danych (*Data Protection Review Court*), do którego osoby fizyczne z UE będą mogły się odwołać. W przypadku, gdy sąd ten stwierdzi, że dane zostały zgromadzone z naruszeniem obowiązujących zabezpieczeń, będzie mógł nakazać usunięcie takich danych. Wprowadzone zostanie także kilka mechanizmów dochodzenia roszczeń w przypadku niewłaściwego przetwarzania danych osobowych przez amerykańskie firmy. Funkcjonowanie Ram ochrony danych będzie podlegać okresowym przeglądom, które będą przeprowadzane przez Komisję Europejską wraz z przedstawicielami europejskich organów ochrony danych i właściwych organów USA. Pierwszy przegląd odbędzie się w ciągu roku od wejścia w życie decyzji stwierdzającej odpowiedni stopień ochrony, w celu sprawdzenia, czy wszystkie istotne elementy zostały w pełni wdrożone do ram prawnych USA i skutecznie funkcjonują w praktyce.

8 WSPÓŁPRACA Z UODO

Co dalej?

Unia Europejska pozostaje wiodącym globalnym graczem w kwestii kształtowania podejścia do ochrony danych. Świadczy o tym przewodnia rola w regulacji transferów danych z państw europejskich do Stanów Zjednoczonych, ale także najnowsze zmiany prawa ochrony danych w Szwajcarii zbliżające je w większym stopniu do zasad znanych z RODO. Z drugiej strony istotnym graczem może stać się także Wielka Brytania, która od czasu opuszczenia UE pracuje nad reformą swoich regulacji obecnie będących kopią RODO. Zapowiadane zmiany mają iść w kierunku stworzenia środowiska bardziej przyjaznego dla biznesu. W kwestii podstawowych zasad nie spodziewamy się jednak rewolucji, ponieważ mogłaby ona zagrozić pewności transferów danych z UE do Wielkiej Brytanii. Niewątpliwie jednak organizacje działające globalnie powinny bacznie śledzić coraz gęstszą siatkę regulacji, która już dawno przestała obejmować jedynie Europę.

Autor: r. rp. Ewa Kurowska-Tober, Partner w kancelarii dla Piper Giziński Kycia Sp. K., Członek Stowarzyszenia Prawa Nowych Technologii

TWOJE DANE TWOJA SPRAWA

Rozpoczynamy XIV edycję ogólnopolskiego programu edukacyjnego **"Twoje dane - Twoja sprawa"**
Rekreacja startuje 1 września 2023 r.
Zapraszamy szkoły i placówki doskonalenia nauczycieli

8 WSPÓŁPRACA Z UODO

CHATBOTY SI A ZGODNOŚĆ Z PRZEPISAMI RODO

W ostatnim czasie ogromną popularność zdobyły różne programy (usługi) sztucznej inteligencji, które tworzą treści w języku ludzkim w odpowiedzi na zapytania użytkowników (chatbot SI). Oparte są one na modelach tzw. generatywnej sztucznej inteligencji (generative AI). Zaliczyć do nich należy np. ChatGPT, Bing Chat, czy Bard(Google).

Wyróżnić można trzy podstawowe źródła danych wykorzystywanych przez chatboty SI:

1) informacje ogólnodostępne w Internecie,
2) informacje przekazywane przez użytkowników oraz
3) informacje licencjonowane od podmiotów trzecich.

Nie budzi wątpliwości, że wiele z powyższych informacji ma charakter danych osobowych w rozumieniu art.4 pkt 1 RODO. Przykładowo charakter taki mogą mieć ogólnodostępne w Internecie informacje o użytkowniku, informacje zawarte w jego zapytaniach do chatbota, czy też informacje o sposobie korzystania przez niego z tej usługi.

Stanowiska regulatorów państw UE

Zgodność chatbotów SI z wymogami RODO była przedmiotem decyzji włoskiego organu ds. ochrony danych z 31 marca 2023 r., zakazującego przetwarzania przez OpenAI, operatora ChatGPT, danych osobowych użytkowników znajdujących się na terytorium Włoch. Decyzja ta, po dokonaniu odpowiednich modyfikacji przez OpenAI, została następnie uchylona w kwietniu 2023 roku.
W sprawie korzystania z usług chatbotów SI wypowiedziały się również organy ds. ochrony danych osobowych we Francji, Hiszpanii, Holandii, Irlandii oraz w Niemczech.
Na podstawie ww. decyzji oraz opinii regulatorów można wskazać na największe, z punktu widzenia RODO, ryzyka prawne dotyczące przetwarzania danych osobowych w związku z tworzeniem i korzystaniem z chatbotów SI.
W konsekwencji, organy ds. ochrony danych osobowych stwierdziły, że przetwarzanie danych osobowych, zarówno na etapie trenowania, jak i wykorzystywania modeli sztucznej inteligencji, w oparciu o które działają chatboty, może naruszać przepisy art. 5–8, 13, 25 i 32 RODO.

8 WSPÓŁPRACA Z UODO

6 ryzyk dotyczących przetwarzania danych osobowych gdy tworzymy lub korzystamy z SI

1. Brak przejrzystości przetwarzania danych osobowych przez chatboty, w tym nie przekazywanie użytkownikom odpowiednich informacji dotyczących przetwarzania zarówno na etapie „trenowania", jak i korzystania z modeli sztucznej inteligencji na których są one oparte.
2. Brak określenia podstaw prawnych przetwarzania danych osobowych przez operatorów chatbotów.
3. Brak weryfikacji wieku użytkowników, w wyniku czego użytkownicy poniżej 13. roku życia mogą uzyskiwać od chatbotów odpowiedzi nieodpowiednie do ich stopnia rozwoju i samoświadomości.
4. Brak poprawności danych osobowych przetwarzanych i dostarczanych przez chatboty.
5. Nieodpowiedni poziom realizacji praw podmiotów danych, których dane osobowe są przetwarzane przez chatboty.
6. Niewprowadzenie adekwatnych środków bezpieczeństwa, co skutkuje możliwością wykorzystywania generatywnych modeli sztucznej inteligencji do wyodrębnienia danych osobowych lub obejścia zabezpieczeń prywatności za pomocą odpowiednio przygotowanych podpowiedzi.

Środki zgodności z RODO wprowadzone przez operatorów chatbotów SI

W związku z powyższymi zarzutami, formułowanymi przez regulatorów, operatorzy chatbotów SI podjęli następujące środki mające zapewnić zgodność przetwarzania danych osobowych z RODO:

- jako podstawę przetwarzania danych osobowych określono prawnie uzasadnionych interes administratora (art.6 ust.1 pkt f) RODO), argumentując – w ramach wykonywanego testu równowagi – że dane wykorzystywane na etapie „trenowania" modeli sztucznej inteligencji przeważnie pochodzą ze źródeł ogólnodostępnych i nie są później przechowywane przez chatboty,
- w politykach prywatności i innej dokumentacji szczegółowo opisano proces „szkolenia i rozwoju" sztucznej inteligencji, w tym jakie kategorie danych osobowych i w jakich celach są przetwarzane na te cele, a także informując użytkowników, że z uwagi na sposób działania tzw. dużych modeli językowych, podawane odpowiedzi mogą być nieraz nieprawdziwe lub niekompletne,
- wprowadzenie mechanizmów filtrujących, które mają na celu zapobieżenie przetwarzaniu danych wrażliwych,
- wprowadzenie mechanizmów (np. „wyskakujących okienek"), w wyniku których użytkownicy muszą potwierdzić, że mają co najmniej 13 lat i samodzielnie lub za zgodą opiekuna wyrażają zgodę na przetwarzanie ich danych osobowych,

- umożliwienie realizacji praw podmiotów danych, w tym żądania – za pomocą formularzy online – aby ich dane nie były wykorzystywane do szkolenia sztucznej inteligencji,
- wykonanie oceny skutków przetwarzania danych dla ochrony danych osobowych użytkowników.

Inicjatywa EROD

Środki zastosowane przez operatorów chatbotów SI, w tym ChatGPT i (Google) Bard są krokiem w dobrym kierunku, jednak nie rozwiewają wszystkich wątpliwości dotyczących zgodności ich funkcjonowania z RODO. Z tych przyczyn, Europejska Rada Ochrony Danych Osobowych 13 kwietnia 2023 r. powołała specjalną grupę (*task force*), której zadaniem jest wydanie dalszych wytycznych w tym zakresie.

Autor: adw. Xawery Konarski, Traple Konarski Podrecki i Wspólnicy sp.j., Prezes Stowarzyszenia Prawa Nowych Technologii

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl