URZĄD OCHRONY DANYCH OSOBOWYCH

# BIULETYN UODO

Nr 4/06/23

# SPIS TREŚCI

**Drodzy Czytelnicy!**

Działalność edukacyjna to jedno z zadań Prezesa Urzędu Ochrony Danych Osobowych. Od lat widzimy, że potrzebne jest nieustanne podnoszenie wiedzy z zakresu ochrony danych osobowych nie tylko osób fizycznych, ale także specjalistów w tej dziedzinie.
Dlatego UODO zainaugurował właśnie kolejny projekt edukacyjny, tym razem skierowany do osób kończących studia lub wchodzących na rynek pracy pn. „Letnia Akademia Liderów RODO", które chcą wzbogacić swoje kompetencje o wiedzę z zakresu ochrony danych osobowych i prawa do prywatności. Ta inicjatywa powstała z myślą o kształceniu przyszłych liderów ochrony danych osobowych, czyli o studentach i absolwentach takich kierunków, jak: prawo, administracja, stosunki międzynarodowe czy informatyka. Uczestnicy Akademii będą mogli podczas wykładów i zajęć praktycznych trwających od lipca do września br. zdobyć umiejętności zawodowe, czerpiąc z wiedzy i doświadczenia ekspertów UODO oraz zewnętrznych aktualnych liderów ochrony danych osobowych.
Ogłoszenie możliwości uczestnictwa w „Letniej Akademii Liderów RODO" wywołało tak duże zainteresowanie inicjatywą, że już po pierwszym dniu rejestracji, nabór uczestników został zakończony. Ogromnie cieszy nas, że młodzi ludzie chcą rozwijać się w tej dziedzinie i zauważają, że ochrona danych osobowych nabiera coraz większego znaczenia. W dobie nadchodzących zmian regulacyjnych i wykorzystywania nowych technologii w różnych obszarach działalności, młodzi ludzie dostrzegają bowiem wzrost znaczenia dostępu do informacji, a co za tym idzie wartość ochrony danych osobowych. To dowód na rosnącą pozycję ochrony danych osobowych jako dziedziny wpływającej na funkcjonowanie wielu branż.
„Letnia Akademia Liderów RODO" to nie pierwsza i nie ostatnia inicjatywa edukacyjna Urzędu Ochrony Danych Osobowych. Organ nadzorczy nadal będzie prowadził aktywną działalność edukacyjną na wielu płaszczyznach. Tylko w obecnym roku, a mamy dopiero jego połowę, udało się zorganizować szkolenia dla administracji rządowej, inspektorów ochrony danych pełniących swoje funkcje w samorządach zawodowych, ale również dla administracji samorządowej czy seniorów z Uniwersytetu Trzeciego Wieku.
Nie zwalniamy tempa, przed nami jeszcze wiele inicjatyw edukacyjnych, do których udziału Państwa zapraszamy.

***Jakub Groszkowski***
Zastępca Prezesa UODO

**Drodzy Czytelnicy!**

Jak wynika ze wspólnego badania serwisu ChronPESEL.pl i Krajowego Rejestru Długów pod patronatem Urzędu Ochrony Danych Osobowych i Instytutu Prawa Ochrony Danych Osobowych prawie 92 proc. ankietowanych wskazuje jako dane osobowe w pierwszej kolejności numer PESEL, a dopiero potem imię i nazwisko czy adres zamieszkania. Co ciekawe, jedynie 45,1 proc. uczestników badania uważa wizerunek za dane osobowe, zaś uznanie odcisków palców za dane osobowe wskazało 40 proc. badanych. To świadczy o tym, że nadal w sposób bardzo podstawowy rozumiemy, czym są dane osobowe. Pełne wyniki badania przeprowadzonego w maju br. przedstawimy niebawem na stronie Urzędu. Już teraz zapraszam także na webinarium połączone z debatą ekspertów, na którym szczegółowo zajmiemy się najnowszymi badaniami. Wracając do czerwcowego wydania „Biuletynu UODO" prezentujemy w nim kolejną porcję użytecznych informacji poświęconych ochronie danych osobowych. W kontekście nowych technologii, z których tak chętnie przecież korzystamy, warto przeczytać materiał o inteligentnych zabawkach. Uświadamia on, jak wiele informacji o użytkownikach – naszych dzieciach – mogą pozyskiwać te urządzenia. Niestety, niejednokrotnie mogą one stanowić zagrożenie dla ich prywatności. UODO niezmiennie podkreśla, że administrator powinien przetwarzać dane osobowe na podstawie przepisów prawa, jednocześnie zapewniając danym osobowym bezpieczeństwo poprzez odpowiednie zastosowanie środków technicznych i organizacyjnych. Dlatego w czerwcowym wydaniu chcemy nawiązać do tego zagadnienia, dając Państwu odpowiedź na pytanie: jak pseudonimizować dane w dokumentach publikowanych w BIP. Odpowiedzi szukajcie w opracowaniu opisującym jedną z decyzji UODO, która zakończyła się upomnieniem administratora. Inną istotną publikacją jest analiza wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie, który oddalił skargę administratora na decyzję UODO. Co ważne, sąd podkreślił, że głównym celem RODO jest ochrona podstawowych praw i wolności osób fizycznych, a w przypadku jakichkolwiek wątpliwości związanych z przetwarzaniem danych osobowych, powinniśmy tę wartość stawiać na pierwszym miejscu. Myślę, że to ważne orzeczenie, które wyznacza kierunek działania tak organu nadzorczego, jak i administratorów, inspektorów ochrony danych. Ma on wpływ także na osoby, których dane dotyczą.
Zapraszam do lektury!

***Adam Sanocki***
Dyrektor Departamentu
Komunikacji Społecznej,
Rzecznik Prasowy UODO

# 1 ROZMOWA Z EKSPERTEM

## WSPÓŁPRACA KLUCZEM DO ZAPEWNIENIA JEDNOLITOŚCI STOSOWANIA PRZEPISÓW

**Maria Owczarek, Zastępca Dyrektora Departamentu Współpracy Międzynarodowej i Edukacji w rozmowie z Eweliną Janczylik-Foryś mówi o współpracy organów nadzorczych i dalszej harmonizacji stosowania przepisów RODO.**

**Za nami 5 lat stosowania ogólnego rozporządzenia o ochronie danych (RODO). Przy okazji tej rocznicy w ostatnim czasie dokonano wielu podsumowań, analizowano przepisy RODO. Jak z punktu widzenia współpracy międzynarodowej jest odbierany ten akt prawny?**

Uważam, że jednym z największych sukcesów RODO jest wzmocnienie pozycji europejskich organów nadzorczych i współpraca między nimi dzięki narzędziom, które zagwarantowało RODO i za sprawą ustanowienia Europejskiej Rady Ochrony Danych (EROD).

Na początku obowiązywania ogólnego rozporządzenia o ochronie danych EROD postawiła duży nacisk na przyjmowanie wytycznych, aby wytłumaczyć najważniejsze założenia RODO oraz zapewnić jasną interpretację pojęć stosowanych w tym rozporządzeniu. EROD kontynuuje prace nad wytycznymi, jednak w tym momencie skupia większą uwagę na monitorowaniu egzekwowania prawa i na narzędziach rozliczalności, takich jak wiążące reguły korporacyjne, kodeksy postępowania czy certyfikacja. Organy przyjmują także coraz więcej decyzji krajowych, co przekłada się na wzrost decyzji przyjmowanych przez EROD. To dowód na wzrost egzekwowania prawa, co stało się jednym z ostatnich kluczowych działań Rady. Większa liczba przyjmowanych decyzji przez EROD to także efekt ukształtowania nowych wewnętrznych procedur w Radzie, które służą osiągnięciu porozumienia przez organy nadzorcze i wypracowaniu wspólnego stanowiska.

**Wdrażając przepisy RODO, zwracano również uwagę na ważną rolę mechanizmu kompleksowej współpracy.**

Niewątpliwie efektywne prowadzenie postępowań w ramach mechanizmu kompleksowej współpracy przez organy nadzorcze jest jednym z kluczowych punktów reformy ochrony danych osobowych. EROD stworzyła procedury w systemie wymiany informacji na rynku wewnętrznym (system IMI), aby umożliwić organom nadzorczym określenie ich odpowiednich ról i efektywne korzystanie z mechanizmów współpracy i spójności na mocy RODO, a także skuteczną, szybką i bezpieczną wymianę informacji. Dane statystyczne potwierdzają, że organy nadzorcze skutecznie współpracują ze sobą i wymieniają się wzajemnie informacjami. Jak wynika z rocznego sprawozdania EROD za rok 2022, tylko w okresie od 1 stycznia do 31 grudnia ub.r., przeprowadzono 714 postępowań w ramach mechanizmu kompleksowej współpracy, w wyniku których wydano 330 ostatecznych decyzji.

**Wymienione przez panią aktywności świadczą o dużym sukcesie dotychczasowego stosowania RODO i o coraz skuteczniejszej współpracy organów nadzorczych w ramach EROD.**
**A jakie widzi pani wyzwania na kolejne lata?**

Obszary, w ramach których organy nadzorcze mierzą się z wyzwaniami na co dzień i będą się mierzyć w najbliższych latach, to m.in. skuteczna współpraca organów nadzorczych w zakresie egzekwowania prawa oraz wyzwania związane z nową architekturą prawną jednolitego rynku cyfrowego.
Ostatnie doświadczenia z pracy organów nadzorczych w ramach RODO pokazały, że efektywne egzekwowanie przepisów jest kluczowe dla zapewnienia spójnej interpretacji RODO. Na potrzebę wzmocnienia działań w zakresie egzekwowania prawa wskazały również Komisja Europejska i Parlament Europejski w ocenie RODO po dwóch latach jego stosowania.
Aby zapewnić skuteczność narzędzi przewidzianych w RODO, Europejska Rada Ochrony Danych w kwietniu 2022 roku zorganizowała w Wiedniu spotkanie wysokiego szczebla w sprawie egzekwowania przepisów. W wyniku tego spotkania EROD przyjęła oświadczenie w sprawie współpracy w zakresie egzekwowania prawa, w którym organy ochrony danych wskazały między innymi na aspekty proceduralne, które można by dalej zharmonizować w prawie UE, aby zmaksymalizować skuteczność mechanizmu współpracy.

**Z tego wynika, że EROD nadal widzi potrzebę dalszej i mocniejszej współpracy między organami nadzorczymi.**

Owszem, współpraca między organami nadzorczymi wymaga stałego zacieśniania. Biorąc pod uwagę postępujący rozwój nowych technologii i globalizację usług, zapewnienie jednolitego podejścia ma ogromne znaczenie.
Co więcej, EROD dostrzegła także potrzebę zapewnienia bardziej efektywnego egzekwowania unijnych przepisów o ochronie danych.
Co w tym przypadku jest niezmiernie istotne to fakt, że to organy nadzorcze same zidentyfikowały te przeszkody, które ich zdaniem nie dają się wyeliminować na poziomie stosowania RODO i wskazały potrzebę wprowadzenia zmian.
EROD przyjęła wykaz działań proceduralnych wymagających dalszej harmonizacji w UE, który został przesłany do Komisji Europejskiej. Ta tzw. „lista życzeń” dotyczy m.in. statusu i praw stron w postępowaniach administracyjnych, terminów proceduralnych, wymogów dopuszczalności lub odrzucania skarg czy też praktycznego wdrożenia procedury współpracy. UODO brał aktywny udział w opracowaniu tego wykazu, dostrzegając przeszkody proceduralne, jako jeden z bardziej aktywnych organów prowadzących postępowania transgraniczne.
Obecnie Komisja pracuje nad dalszym doprecyzowaniem zasad proceduralnych związanych z egzekwowaniem RODO. Jest to duże wyzwanie, ale i duży krok w kierunku wzmocnienia skuteczności współpracy w zakresie egzekwowania prawa między organami ochrony danych.

# 1 ROZMOWA Z EKSPERTEM

**Nie sposób nie podjąć szalenie istotnego tematu w kontekście nowych technologii, czyli pakietu usług cyfrowych i strategii EROD w tym zakresie. Czy ochronę danych osobowych można połączyć z postępem technologicznym?**

Można, i rzeczywiście, w kolejnych latach istotnym wyzwaniem w tym kontekście będzie kwestia zastosowania w praktyce aktów stanowiących część pakietu usług cyfrowych i strategii w zakresie danych osobowych. Te nowe instrumenty prawne przewidują powołanie nowych organów oraz nowych europejskich struktur współpracy między tymi organami. Nie możemy uniknąć postępu technologicznego, ale możemy spowodować, aby szanowano prawa osób, których dane dotyczą. EROD m.in. w swoim oświadczeniu w sprawie pakietu usług cyfrowych i strategii w zakresie danych, wskazuje na wiele obaw i przedstawia zalecenia, jak zbliżyć treść wniosków prawodawczych z pakietu usług cyfrowych i strategii w zakresie danych do obowiązującego prawodawstwa Unii w tej tematyce.

**Czy może pani przedstawić konkretnie, jakie to są obawy EROD?**

Jak wskazuje EROD obawy te można podzielić na trzy kategorie: brak ochrony podstawowych praw i wolności osób fizycznych, fragmentaryczny nadzór i ryzyko wystąpienia niespójności. Przykładowo, wniosek prawodawczy dotyczący aktu w sprawie sztucznej inteligencji w jego pierwotnej wersji umożliwiałby stosowanie systemów sztucznej inteligencji, które klasyfikują osoby fizyczne na podstawie danych biometrycznych (np. rozpoznawanie twarzy) według kryteriów, takich jak pochodzenie etniczne, płeć, orientacja polityczna lub seksualna, czy inne cechy dyskryminacyjne, a także stosowanie systemów sztucznej inteligencji, których skuteczność nie została naukowo potwierdzona lub które sprzeczne są z podstawowymi wartościami UE.

**EROD nawet uznała, że takie systemy powinny być zakazane w UE.**

Tak, i zaapelowała do współprawodawców o wprowadzenie takiego zakazu w akcie dotyczącym sztucznej inteligencji. Dodatkowo, jak wskazała EROD, wykorzystywanie sztucznej inteligencji do wykrywania emocji osoby fizycznej jest niepożądane i powinno być zakazane, z wyjątkiem konkretnych precyzyjnie określonych przypadków zastosowania, takich jak cele zdrowotne lub badawcze, pod warunkiem odpowiednich zabezpieczeń, warunków i ograniczeń. Co ważne, apele EROD i organizacji społecznych o zapewnienie ochrony praw i wolności osób fizycznych w projektowanym akcie przyniosły rezultaty – przyjęte w maju br. przez komisje Parlamentu Europejskiego poprawki do AI Act uwzględniają wskazane przez EROD zastrzeżenia. Nowa wersja aktu zawiera zakazy stosowania inwazyjnych i dyskryminujących zastosowań systemów sztucznej inteligencji, m.in. takich jak: zdalne systemy identyfikacji biometrycznej „w czasie rzeczywistym” w publicznie dostępnych przestrzeniach, systemy kategoryzacji biometrycznej wykorzystujące cechy wrażliwe, systemy rozpoznawania emocji w egzekwowaniu prawa, zarządzaniu granicami, miejscu pracy i instytucjach edukacyjnych, czy też masowe pobieranie danych biometrycznych z mediów społecznościowych lub nagrań z monitoringu w celu tworzenia baz danych rozpoznawania twarzy.

# 1 ROZMOWA Z EKSPERTEM

**To były zastrzeżenia, jak rozumiem, dotyczące ochrony podstawowych praw i wolności. A jaki organ będzie dokonywał oceny, czy te prawa są faktycznie respektowane?**

Pani pytanie odnosi się do obaw EROD związanych z fragmentarycznym nadzorem. Rada wyraziła zaniepokojenie faktem, że we wnioskach nie określono jasno, w jaki sposób ustanowione aktami nowe organy mają współpracować z organami nadzorczymi (i z EROD). W szczególności w niektórych wnioskach nie uregulowano odpowiednio sytuacji potencjalnego nakładania się kompetencji ani sytuacji, w których organy powinny konsultować się ze sobą w kwestiach będących przedmiotem wspólnego zainteresowania.

EROD dostrzegła także potrzebę zapewnienia bardziej efektywnego egzekwowania unijnych przepisów o ochronie danych. Co w tym przypadku jest niezmierne istotne to fakt, że to organy nadzorcze same zidentyfikowały te przeszkody, które ich zdaniem nie dają się wyeliminować na poziomie stosowania RODO i wskazały potrzebę wprowadzenia zmian.

**W ostatnim czasie opinię publiczną obiegła decyzja włoskiego organu dotycząca zakazu przetwarzania danych przez ChatGPT.**

W decyzji z 31 marca 2023 r. włoski organ nadzorczy (Garante) nakazał OpenAI zaprzestanie przetwarzania danych włoskich obywateli, powołując się na toczące się postępowanie dotyczące nieprawidłowości w przetwarzaniu danych osobowych, w tym przetwarzania danych osobowych bez podstawy prawnej wynikającej z RODO.

**Na jakim etapie jest obecnie ta sprawa?**

Włoski organ wydał następnie kolejną decyzję znoszącą tymczasowe ograniczenie, pod warunkiem, że OpenAI wdroży odpowiednie środki, dotyczące przejrzystości, praw osób, których dane dotyczą – w tym użytkowników i osób niebędących użytkownikami – i podstawy prawnej przetwarzania dla szkoleń algorytmicznych opierających się na danych użytkowników. W związku z tym, że ChatGPT jest powszechnie stosowany przez użytkowników w Unii, EROD zadecydowała następnie o utworzeniu grupy zadaniowej w celu wspierania współpracy i wymiany informacji na temat ewentualnych działań w zakresie postępowań, prowadzonych przez organy nadzorcze, w związku z działaniem ChatGPT. Prace tej grupy trwają. Ponadto, przyjęte w maju przez komisje Parlamentu Europejskiego, poprawki do AI Act, uwzględniają także dodatkowe obowiązki dostawców usług w zakresie przejrzystości. Zgodnie z wprowadzonym zmianami, jak wskazuje Parlament w oświadczeniu prasowym z 11 maja 2023 r. dotyczącym wprowadzonych poprawek, modele generatywne, takie jak np. ChatGPT, musiałyby uwzględnić obowiązek ujawniania, że treści zostały wygenerowane przez sztuczną inteligencję, zaprojektować model w sposób uniemożliwiający generowanie nielegalnych treści i publikować podsumowania danych chronionych prawem autorskim wykorzystanych do szkolenia.

Na koniec chciałabym podkreślić, że zagadnienie dotyczące relacji pomiędzy ochroną danych osobowych a sztuczną inteligencją, od dawna jest również przedmiotem zainteresowania Urzędu Ochrony Danych Osobowych. Dla lepszego zrozumienia tej technologii, potencjału jej wykorzystania, korzyści i zagrożeń Urząd podejmował wiele inicjatyw edukacyjnych i naukowych mających ułatwić jej poznanie. Oprócz organizowania wydarzeń kierowanych do ekspertów, temat sztucznej inteligencji był także przedstawiany uczniom w ramach programu edukacyjnego UODO „Twoje dane – Twoja sprawa".

W opinii EROD – z czym należy się zgodzić – w najbliższych latach kluczowe będzie solidne osadzenie RODO w ogólnej architekturze regulacyjnej tworzonej na potrzeby rynku cyfrowego. Konieczne będzie także zapewnienie jasnego podziału kompetencji między organami regulacyjnymi, a także skutecznej ich współpracy.

Jestem przekonana, że w kolejnych latach stosowania RODO będziemy mieli szansę obserwować wzmacnianie współpracy organów nadzorczych, a także coraz bardziej efektywne egzekwowanie RODO – dzięki wysiłkom Europejskiej Rady Ochrony Danych, w tym wytężonej pracy pracowników UODO w tym zakresie.

**Dziękuję za rozmowę.**

## WERYFIKACJA WDROŻENIA PRZEZ PODMIOT PRZETWARZAJĄCY ODPOWIEDNICH ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH

**Administrator, zarówno podejmując decyzję, komu powierzyć przetwarzanie danych osobowych, jak i w czasie trwania umowy powierzenia, ma prawo domagać się, aby podmiot przetwarzający udokumentował wdrożenie odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Trudno uznać, aby samo oświadczenie podmiotu przetwarzającego w tej sprawie było wystarczające dla weryfikacji przez administratora kompetencji procesora i spełniania przez niego wymogów z RODO.**

Ponieważ dane osobowe (stosownie do art. 5 ust. 1 lit. a i lit. f RODO) muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość") oraz w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność"), to bardzo ważne z punktu widzenia administratora jest to, jakiemu podmiotowi powierza przetwarzanie tych danych. Tym bardziej, że art. 5 ust. 2 RODO stanowi, iż to administrator ponosi odpowiedzialność za przetwarzanie danych osobowych zgodnie z tymi zasadami i musi być w stanie wykazać ich przestrzeganie („rozliczalność"). Jednocześnie przepisy RODO stanowią (art. 28), że jeżeli przetwarzanie ma być dokonywane w imieniu administratora, to korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą. Wskazują jednak (art. 28 ust. 3 lit. h), że umowa lub inny instrument prawny, na podstawie którego odbywa się przetwarzanie danych przez podmiot przetwarzający, stanowią w szczególności, że podmiot przetwarzający udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

Z wytycznych EROD 7/2020 dotyczących pojęć administratora i podmiotu przetwarzającego zawartych w RODO wynika ponadto, że w czasie oceny procesora „Elementami, które należy wziąć pod uwagę, mogą być: wiedza fachowa podmiotu przetwarzającego (np. wiedza techniczna w zakresie środków bezpieczeństwa i naruszeń ochrony danych); wiarygodność podmiotu przetwarzającego; zasoby podmiotu przetwarzającego oraz stosowanie przez podmiot przetwarzający zatwierdzonego kodeksu postępowania lub mechanizmu certyfikacji", a także, że „Administrator jest (…) odpowiedzialny za ocenę adekwatności gwarancji udzielonych przez podmiot przetwarzający i powinien być w stanie udowodnić, że poważnie wziął pod uwagę wszystkie elementy przewidziane w RODO.

## 2 UODO SYGNALIZUJE

Ocena administratora, czy gwarancje są wystarczające, jest formą oceny ryzyka, która w znacznym stopniu zależy od rodzaju przetwarzania powierzonego podmiotowi przetwarzającemu i musi być dokonywana indywidualnie dla każdego przypadku, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania, a także zagrożeń dla praw i wolności osób fizycznych".
W tej kwestii EROD rekomenduje zapoznanie się administratora z odpowiednią dokumentacją (np. polityką prywatności, warunkami świadczenia usług, rejestrem czynności przetwarzania, polityką zarządzania dokumentacją, polityką bezpieczeństwa informacji, sprawozdaniami z zewnętrznych audytów ochrony danych, uznanych międzynarodowych certyfikatów, takich jak normy ISO 27000). Brak weryfikacji podmiotu przetwarzającego oraz jego gwarancji dla przetwarzania zgodnie z przepisami o ochronie danych osobowych może wiązać się z konsekwencjami dla osób fizycznych, których dane osobowe zostały powierzone podmiotowi przetwarzającemu, np. w postaci utraty danych osobowych.
Zatem decyzja, komu administrator ma powierzyć przetwarzanie danych osobowych nie może być podejmowana bezpodstawnie. Dopiero po zbadaniu kompetencji i adekwatności wybranego podmiotu przetwarzającego, administrator może przystąpić do zawarcia stosownej umowy powierzenia. Jednocześnie trudno uznać, aby samo oświadczenie podmiotu przetwarzającego o zapewnieniu gwarancji wdrożenia i stosowania odpowiednich środków technicznych i organizacyjnych było dla administratora wystarczające do weryfikacji jego kompetencji i spełniania przez niego wymogów z RODO. Domaganie się przez administratora odpowiedniego udokumentowania określonych oświadczeń jest jednym z jego uprawnień przy dokonywaniu wyboru właściwego podmiotu, któremu zechce powierzyć dane osobowe.
Co istotne, nie należy zapominać, że obowiązki administratora w zakresie zapewnienia powierzenia przetwarzania danych osobowych podmiotowi spełniającemu wymogi wskazane w art. 28 ust. 1 RODO, trwają co najmniej tak długo, jak okres powierzenia.

Jak wskazano w powołanych wytycznych EROD „Obowiązek korzystania wyłącznie z usług podmiotów przetwarzających zapewniających wystarczające gwarancje zawarty w art. 28 ust. 1 RODO jest obowiązkiem ciągłym. Nie kończy się w momencie zawarcia umowy lub innego aktu prawnego przez administratora i podmiot przetwarzający. Administrator powinien raczej w odpowiednich odstępach czasu weryfikować gwarancje podmiotu przetwarzającego, w tym w stosownych przypadkach przez audyty i inspekcje".

**Takie podejście organu nadzorczego potwierdzają wydane przez niego decyzje, w tym decyzja DKN.5131.29.2022**.

## OCHRONA ŻYWOTNYCH INTERESÓW JAKO PRZESŁANKA LEGALIZUJĄCA PRZETWARZANIE DANYCH OSOBOWYCH

**Żywotny interes innej osoby fizycznej powinien zasadniczo być podstawą przetwarzania danych osobowych wyłącznie w przypadkach, gdy ewidentnie przetwarzania tego nie da się oprzeć na innej podstawie prawnej.**
**Ponadto dla zastosowania przepisu art. 6 ust. 1 lit. d RODO jako podstawy legalizującej przetwarzanie danych osobowych konieczne jest nie tylko występowanie żywotnego interesu podmiotu danych lub innej osoby, której dane dotyczą, ale również niezbędność ich przetwarzania dla ochrony tych interesów.**

Warunki, jakie muszą być spełnione, by móc zastosować art. 6 ust. 1 lit. d RODO jako przesłankę legalizującą przetwarzanie danych osobowych organ nadzorczy wskazał, odpowiadając na jedno z otrzymanych niedawno pism.
W odpowiedzi Urząd podkreślił, że dla zajęcia wiążącego stanowiska konieczna jest dokładna znajomość wszystkich okoliczności prawnych i faktycznych sprawy.
Niemniej udzielił pewnych wskazówek, które mogą być pomocne w rozstrzyganiu wątpliwości związanych z możliwością powoływania się na ochronę żywotnych interesów jako podstawę przetwarzania danych osobowych.
UODO zaznaczył, że przesłanka z art. 6 ust. 1 lit. d RODO, pozwalająca na przetwarzanie (w tym udostępnianie) danych osobowych, jeżeli przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, ma zastosowanie wówczas, gdy:
– dochodzi do zagrożenia żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,
– ochrona tych interesów nie jest możliwa w inny sposób, tylko przez przetwarzanie danych osobowych.
Wskazał, że dla możliwości oparcia przetwarzania danych osobowych na tym przepisie niezbędne jest występowanie żywotnych interesów.

Podniósł przy tym, iż w motywie 46 RODO wskazano, że chodzi tu o interesy, które mają znaczenie dla życia podmiotu danych lub innej osoby fizycznej. Również w tym motywie wskazane zostały przykłady tak rozumianych żywotnych interesów. Znalazły się wśród nich: cele humanitarne, monitorowanie epidemii i ich rozprzestrzeniania się, nadzwyczajne sytuacje humanitarne, a w szczególności klęski żywiołowe i katastrofy spowodowane przez człowieka. Ponadto w doktrynie wskazuje się, że do tego katalogu można również zaliczyć przypadki konieczności ratowania życia, zdrowia, a także ochrony majątku (zob. D. Lubasz, W. Chomiczewski [w:] RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. E. Bielak-Jomaa, Warszawa 2018, art. 6).
Jak wskazuje się w literaturze, intencją prawodawcy jest ochrona interesów większej wagi, która uzasadnia czasowy brak respektowania ochrony prywatności człowieka, zwłaszcza w aspekcie jego autonomii informacyjnej (A. Nerka, M. Sakowska-Baryła, w: Ogólne rozporządzenie o ochronie danych osobowych, s. 164). Chodzi tu zatem o sytuacje, gdy w wyniku ważenia interesów administrator uzna, że dobra w postaci ochrony żywotnych interesów osoby fizycznej mają większą wagę niż dobra w postaci prawa do ochrony danych osobowych.
Organ nadzorczy zaznaczył też, że żywotny interes, o którym mowa w powyższym przepisie, musi być interesem osoby, której dane dotyczą lub innej osoby fizycznej. Zastosowanie tego przepisu nie może być zatem uzasadnione interesami np. osoby prawnej. W odniesieniu do przetwarzania danych innych osób fizycznych w motywie 46 preambuły RODO znalazło się jeszcze dodatkowe zastrzeżenie, zgodnie z którym żywotny interes innej osoby fizycznej powinien zasadniczo być podstawą przetwarzania danych osobowych wyłącznie w przypadkach, gdy ewidentnie przetwarzania tego nie da się oprzeć na innej podstawie prawnej.
Jeśli zaś przetwarzanie miałoby dotyczyć danych osobowych szczególnej kategorii, to administrator musiałby również zapewnić spełnienie wymogów art. 9 ust. 2 lit. c. Przepis ten legalizuje przetwarzanie tego typu danych, gdy jest ono niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody. Dla zastosowania przepisu art. 6 ust. 1 lit. d RODO konieczne jest nie tylko występowanie żywotnego interesu podmiotu danych lub innej osoby, której dane dotyczą, ale również niezbędność przetwarzania dla ochrony tych interesów. Rozstrzygnięcie, czy przetwarzanie danych jest niezbędne, powinno być dokonywane przez administratora indywidualnie, w konkretnym przypadku, z uwzględnieniem faktycznych okoliczności przetwarzania danych.
Przy ocenie niezbędnego charakteru przetwarzania danych osobowych dla ochrony żywotnych interesów podmiotu danych należy kierować się wyrażoną w przepisie art. 5 ust. 1 lit. c RODO zasadą minimalizacji danych. A zatem administrator powinien przetwarzać tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne ze względu na cel zbierania danych. Ponadto, jak wskazano w motywie 39 RODO, dane powinny być przetwarzane wyłącznie w takich przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami.

## SPOTKANIE Z INICJATORAMI KODEKSU DLA BRANŻY SPORTOWEJ

**Na prośbę Instytutu Sportu – Państwowego Instytutu Badawczego (IS-PIB) 2 czerwca 2023 r. odbyło się spotkanie przedstawicieli Urzędu Ochrony Danych Osobowych z inicjatorami stworzenia „Kodeksu dla Sportu". Podczas spotkania omówiono najważniejsze kwestie związane z tworzeniem tego projektu.**

IS-PIB będzie wnioskodawcą, a także punktem kontaktowym oraz podmiotem zarządzającym i wspierającym członków kodeksu. Aktualnie 18 polskich związków sportowych wyraziło zainteresowanie i chęć przystąpienia do kodeksu postępowania.


Inicjatorzy mają pomysł i wizję, w jaki sposób przygotować kodeks tak, aby najpełniej wesprzeć nie tylko związki sportowe, ale również innych uczestników szeroko pojętego sportu (m.in. kluby, zawodników, trenerów, sędziów, dzieci, opiekunów) w rozwiązaniu szeregu zidentyfikowanych problemów związanych z przetwarzaniem danych osobowych.

Na spotkaniu poruszono takie kwestie, jak: forma przystąpienia do kodeksu, charakterystyka podmiotów zainteresowanych przystąpieniem do inicjatywy kodeksowej, transfer danych poza kraje Europejskiego Obszaru Gospodarczego, rolę i zadania podmiotu monitorującego oraz zakres konsultacji społecznych.

Jak poinformowali przedstawiciele IS-PIB pomysł opracowania kodeksu poparł Minister Sportu i Turystyki.

Ze strony UODO inicjatorzy kodeksu dla sportu otrzymali zapewnienie wsparcia na każdym etapie tworzenia tego dokumentu.

Więcej informacji nt. inicjatywy opracowania kodeksu postępowania dla sportu, w tym dane do kontaktu, zostały opublikowane na stronie UODO w sekcji **Inicjatywy opracowania kodeksów postępowania.**

# 3 WYBRANE DECYZJE UODO

## UPOMNIENIE ZA UDOSTĘPNIENIE DANYCH OSOBOWYCH W BIP

**Szkoła, udostępniając dokumenty z danymi osobowymi w Biuletynie Informacji Publicznej, powinna poddać je odpowiedniej pseudonimizacji tak, aby nie było możliwe zidentyfikowanie danych osobowych osób, których dokumenty dotyczą.**

Do Urzędu Ochrony Danych Osobowych wpłynęła skarga na nieprawidłowości w procesie przetwarzania danych osobowych skarżącej, w zakresie jej imienia, nazwiska poddanego pseudonimizacji poprzez jego skrócenie oraz na udostępnienie tych danych na stronie internetowej szkoły. Skarga odnosiła się również do danych dotyczących małoletniego dziecka skarżącej, także tych obejmujących jego zdrowie. Dyrektor szkoły na podstawie wniosku o dostęp do informacji publicznej na stronie internetowej szkoły udostępniała wymagane dokumenty, w tym protokoły z kontroli przeprowadzonych w ciągu pięciu ostatnich lat. Udostępniony dokument, będący m.in. przedmiotem postępowania w UODO, został poddany anonimizacji przez dyrektor szkoły. W treści opublikowanego w BIP szkoły protokołu z przeprowadzonej w placówce kontroli, ujawniono: imię skarżącej, początkową część jej nazwiska oraz informację, że jest matką ucznia. Wskazano także imię jej dziecka i podano, do której placówki oświatowej uczęszcza i w której klasie się uczy. Ponadto w treści udostępnionego protokołu zawarta była uwaga o nieharmonijnym rozwoju niektórych funkcji poznawczych ucznia. Po wszczęciu postępowania administracyjnego omawiany protokół kontroli został usunięty z BIP szkoły, a placówka wyjaśniła, że wszelkie błędy w anonimizacji są wynikiem omyłki i braku doświadczenia w tym zakresie.

### Czy to są dane osobowe?

W tej sprawie w pierwszej kolejności należy ocenić, czy dane udostępnione w protokole kontroli w ogóle stanowią dane osobowe w rozumieniu ogólnego rozporządzenia o ochronie danych (RODO). Zgodnie z rozporządzeniem „dane osobowe” oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”). Należy mieć na uwadze, że możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Ponadto nie można zapomnieć, że zgodnie z motywem 26 RODO, zasady ochrony danych powinny mieć zastosowanie do wszelkich informacji o zidentyfikowanych lub możliwych do zidentyfikowania osobach fizycznych. Aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądne sposoby, w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić,

czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania trzeba uwzględnić technologię dostępną w momencie przetwarzania danych.

**Czy pseudonimizacja umożliwia identyfikację?**

Dane osobowe poddane pseudonimizacji, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej, należy uznać za informacje o możliwej do zidentyfikowania osobie fizycznej.

W tej sprawie w wyniku wyodrębnienia z treści opublikowanego w BIP szkoły protokołu kontroli i nazwy pliku, UODO ustalił zakres danych dotyczących skarżącej oraz informacji odnoszących się do ucznia szkoły. W ocenie UODO dane i informacje dotyczące zarówno skarżącej, jak i małoletniego, udostępnione w zmodyfikowanej kopii protokołu kontroli w BIP, można przypisać odpowiednio tym osobowym. Dane obejmujące imię skarżącej w połączeniu z nazwą szkoły i klasy, do której uczęszcza jej dziecko, już samodzielnie pozwalają przypisać spseudonimizowane dane osobie fizycznej – skarżącej. Co istotne, w tej sprawie skarżąca jest jedynym rodzicem o tym imieniu wśród rodziców uczniów klasy, do której uczęszcza jej dziecko, które także zostało wymienione w protokole. W tym przypadku łatwo zidentyfikować dane osobowe skarżącej przy jednoczesnym braku ponoszenia kosztów. W analogiczny sposób możliwe jest przypisanie spseudonimizowanych danych dziecka, ponieważ jest jedynym uczniem klasy noszącym to konkretne imię, a jednocześnie jedną z dwóch osób o tym imieniu w zbiorze ogółu uczniów szkoły.

### Informacja publiczna uwzględnia zasady RODO

Szkoła jest zobowiązana udostępnić w BIP informację publiczną, obejmującą m.in. dokumentację przebiegu i efektów kontroli oraz wystąpienia, stanowiska, wnioski i opinie podmiotów ją przeprowadzających, do których zalicza się protokół kontroli doraźnej organu sprawującego nadzór pedagogiczny nad szkołą.

**Czy udzielanie informacji publicznej wymaga ochrony danych osobowych?**

Przy wywiązaniu się z obowiązku udzielania informacji publicznej, każdy administrator musi zachować zasady z zakresu ochrony danych osobowych.

Wszelkie formy przetwarzania danych osobowych muszą odbywać się wedle zasad wymienionych w art. 5 ust. 1 RODO. Dane osobowe powinny być m.in. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość") oraz być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych").

# 3 WYBRANE DECYZJE UODO

W ocenie UODO szkoła, publikując protokół kontroli na stronie internetowej, naruszyła zasadę minimalizacji danych, ponieważ udostępnione przez nią dane osobowe nie były adekwatne, stosowne ani ograniczone do celu.

Należy wskazać, że artykuł 5 ust. 2 ustawy o dostępie do informacji publicznej stanowi, że prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Ograniczenie to nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji oraz przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa. W niniejszej sprawie szkoła nie dochowała obowiązku wynikającego z przywołanego powyżej przepisu. W związku z powyższym Prezes UODO stwierdził, że szkoła naruszyła również zasadę zgodności z prawem przetwarzania danych osobowych.

## Konsekwencje

Organ nadzorczy upomniał szkołę w zakresie stwierdzonych naruszeń, mimo że w dniu wydania decyzji placówka usunęła dokument ze strony internetowej.

W związku z tym zdarzeniem dyrektor szkoły wprowadził w placówce praktykę polegającą na konsultacji z inspektorem ochrony danych dokumentów, które wymagają anonimizacji, przed ich publikacją. Ponadto, jak wskazała szkoła, IOD zaplanował przeprowadzenie dodatkowego szkolenia dla pracowników, które dotyczyć ma w szczególności kwestii anonimizacji danych i publicznego dostępu do danych szkoły.

## ZDANIEM WSA ORGAN NADZORCZY PRAWIDŁOWO ZEBRAŁ I OCENIŁ MATERIAŁ DOWODOWY

**Wojewódzki Sąd Administracyjny w Warszawie w wyroku z 15 listopada 2022 r. oddalił skargę Santander Bank Polska na decyzję UODO nakładającą na tego administratora karę pieniężną w wysokości ponad 545 tys. zł.**

Ustalenia UODO potwierdził WSA w Warszawie (sygn. II SA/Wa 546/22). Po przeprowadzeniu postępowania Urząd uznał, że doszło do naruszenia ochrony danych osobowych, ponieważ były pracownik banku, po zakończeniu zatrudnienia, w dalszym ciągu posiadał dostęp do profilu płatnika na Platformie Usług Elektronicznych ZUS (PUE ZUS). Jak wykazało postępowanie, osoba ta korzystała z przysługujących mu uprawień, logując się do platformy. W związku z tym, oprócz nałożenia administracyjnej kary pieniężnej, UODO nakazał zawiadomienie o naruszeniu osób, których dane dotyczą.

### Wysokie ryzyko

Organ nadzorczy podkreślił w wydanej w tej sprawie decyzji, że obowiązek zawiadomienia osoby nie jest uzależniony od materializacji negatywnych konsekwencji związanych z naruszeniem, ale od samej możliwości wystąpienia takiego ryzyka. Pogląd ten podzielił WSA. Zdaniem Sądu sama możliwość nieograniczonego dostępu przez byłego pracownika do danych znajdujących się na platformie ZUS, powoduje wysokie ryzyko dla praw i wolności osób. Sąd dodał, że o wysokim ryzyku świadczy zakres danych gromadzonych na platformie PUE ZUS, do którego miał dostęp były pracownik oraz fakt, że bank tolerował tę sytuację przez długi czas. W tej sprawie nie jest istotne, czy osoba nieuprawniona faktycznie zapoznała się z danymi osobowymi innych osób, lecz to, że wystąpiło takie ryzyko.

### Zawiadomienie osób o naruszeniu

Sąd odniósł się także do formy zawiadomienia o naruszeniu ochrony danych osób, których dane dotyczą. Bank umieścił jedynie ogólny komunikat na platformie komunikacji wewnętrznej, przypominając zasady przetwarzania danych osobowych. W ocenie Sądu nie sposób uznać, że administrator wywiązał się z obowiązku zawiadomienia w sposób prawidłowy. Opublikowany komunikat nie nawiązywał do konkretnego naruszenia, dlatego osoby, których to naruszenie dotyczyło, nie miały żadnych powodów, by powiązać go ze swoją sprawą, wyciągnąć z niego wnioski i odpowiednio zareagować.

### Były pracownik zaufanym odbiorcą?

Sąd nie wziął pod uwagę również argumentów administratora, który uznał swojego pracownika za tzw. odbiorcę zaufanego. W tym przypadku Sąd również przychylił się do stanowiska UODO.

# 4 NARUSZENIA I KONTROLE

Sąd dodał także, że „głównym celem RODO jest ochrona podstawowych praw i wolności osób fizycznych, w szczególności prawa do ochrony danych osobowych oraz że ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych. W przypadku jakichkolwiek wątpliwości… należy w pierwszej kolejności brać pod uwagę te wartości”.

Organ nadzorczy wskazał, że status odbiorcy zaufanego mogą posiadać podmioty, które działają w strukturach danej organizacji albo są np. dostawcą, z którego usług administrator stale korzysta. Pomiędzy takimi podmiotami istnieje wówczas więź faktyczna, a nierzadko prawna, która pozwala na ocenę stopnia zaufania stron. W tym przypadku były pracownik nie powinien być uznany za odbiorcę zaufanego, wobec czego bank powinien był zachować się w sposób bardziej ostrożny w przypadku ujawnienia danych osobie nieuprawnionej. W przedmiotowej sprawie, pomiędzy byłym pracownikiem a administratorem nie istniał już żaden stosunek obligacyjny. Ustanie zatrudnienia jest jednoznaczne bowiem z zerwaniem więzi prawnej, a o braku występowania odbiorcy zaufanego winien świadczyć już sam fakt pięciokrotnego zalogowania się do systemu przez byłego pracownika w przypadku braku uprawnień. WSA uznał także wymierzoną karę pieniężną za wyważoną i spełniającą kryteria prewencyjne i opresyjne.

# 5 NOWE TECHNOLOGIE

## INTELIGENTNE ZABAWKI. JAK ZADBAĆ O PRYWATNOŚĆ DZIECKA?

**W ostatnich latach na polskim rynku zaczęły pojawiać się inteligentne zabawki bazujące na Internecie Rzeczy (IoT) w postaci lalek, robotów czy dziecięcych zegarków, które bez wątpienia wzbudzają duże zainteresowanie wśród dzieci w różnym wieku. Wiele z nich ma wartość edukacyjną i wspomaga kreatywność dziecka, nic więc dziwnego, że są coraz częściej wybierane jako prezenty. Niestety, niejednokrotnie mogą one stanowić zagrożenie dla prywatności i ochrony danych. Na co więc zwrócić uwagę przed zakupem takiej zabawki, żeby się przed tym uchronić i cieszyć się wymarzonym prezentem?**

Dla najmłodszych urodzonych w epoce cyfrowej nowe technologie stają się nieodłącznym elementem ich życia codziennego. Niewątpliwie technologia cyfrowa oferuje wiele możliwości, a ich umiejętne wykorzystanie może pomóc w rozwijaniu wyobraźni i zdolności logicznego myślenia u dziecka. Tak jak w przypadku innych urządzeń wchodzących w skład Internetu Rzeczy inteligentne zabawki wyposażone są w mechanizmy ułatwiające komunikowanie się z najbliższym otoczeniem, co umożliwia zbieranie informacji z zainstalowanego w zabawce mikrofonu lub kamery. Zazwyczaj łączą się z Internetem przez Wi-Fi lub Bluetooth.

UODO przypomina, że tego typu zabawki: „(…) Wyposażone w technologie rozpoznawania mowy, wchodzą w interakcje z dzieckiem. Wielokrotnie wiąże się to z bezprawnym gromadzeniem danych o dziecku, co może stanowić zagrożenie dla jego prywatności, a także narazić go na problemy związane z cyberprzestępczością, w tym kradzież danych, bezprawne ich użycie bez wiedzy użytkownika czy oszustwo (…)”.

Komunikat UODO z 29 maja 2020 r. pt. **(Nie)bezpieczeństwo zabawek połączonych z Internetem.**

Dlatego decydując się na zakup inteligentnej zabawki i mając na uwadze potencjalne zagrożenia, należy pamiętać, że pośpiech i emocje nie są dobrym doradcą i warto poświęcić chwilę, żeby przeanalizować ją pod kątem ochrony danych i prywatności, żeby w pełni wykorzystać jej zalety. Warto mieć świadomość, że dzieci są bardzo podatne na zagrożenia. Nie zawsze wiedzą, jak chronić się przed niebezpieczeństwami wynikającymi z dzielenia się własnymi danymi osobowymi za pomocą nowych technologii. Dlatego niezwykle istotne jest uświadamianie dziecka, czym grozi przekazywanie danych do Internetu i jak postępować, żeby nie ponosić przykrych konsekwencji. Inteligentne zabawki bez wątpienia posiadają wiele walorów edukacyjnych i mogą pobudzać kreatywność i wyobraźnię, warto jednak przed ich zakupem upewnić się, że dane dziecka są bezpieczne i zrobiliśmy wszystko, żeby zminimalizować ryzyko wyrządzenia mu szkody, np. przez kradzież danych, bezprawne ich użycie bez wiedzy użytkownika czy oszustwo.

# 5 NOWE TECHNOLOGIE

## 8 podpowiedzi, jak korzystać z inteligentnych zabawek

1. W pierwszej kolejności upewnij się, że wiesz **jakie funkcje posiada inteligentna zabawka i w jaki sposób wchodzi w interakcję z dzieckiem**: Czy posiada wbudowaną kamerę? A może została wyposażona w funkcję rozpoznawania mowy? Czy może łączyć się z innymi urządzeniami?

2. Mając świadomość, jakie oferuje możliwości, należy zdawać sobie sprawę, że mogą one narazić dziecko na niepotrzebne ryzyko, dlatego **warto zasięgnąć fachowej opinii lub zapoznać się z recenzjami dostępnymi w Internecie**, szczególnie pod kątem ewentualnych problemów z bezpieczeństwem zabawki.

3. Kolejną istotną kwestią jest zweryfikowanie, **czy producenci inteligentnych zabawek zapewniają ochronę danych osobowych** na poziomie wymaganym przez przepisy obowiązujące w Unii Europejskiej. **Jakie dane zbiera zabawka i gdzie są one przechowywane?** Wiele zabawek już podczas instalacji wymaga podania szeregu informacji, takich jak imię, wiek dziecka, adres zamieszkania czy lokalizacja. Zanim jednak zdecydujemy się na ich przekazanie należy upewnić się, że firma jest godna zaufania oraz uważnie przeczytać warunki użytkowania i politykę prywatności, żeby sprawdzić w jakim celu producent lub inny podmiot prosi o ich podanie oraz czy zakres ten jest niezbędny.

4. Konieczne jest również zweryfikowanie, **czy komunikacja z serwerem jest szyfrowana, a zabawka jest odpowiednio zabezpieczona przed niepowołanym dostępem** przez osoby trzecie.

5. Zabawkę należy podłączać i używać wyłącznie w środowisku z dostępem do **bezpiecznej i zaufanej sieci WiFi.**

6. Należy również sprawdzić, czy producent zapewnia aktualizacje oprogramowania. Wiele zabawek ma wbudowany mechanizm automatycznej aktualizacji i w przypadku dostępnej nowszej wersji pobierają i instalują ją automatyczne. Warto jednak upewnić się, że aktualizacje pochodzą z wiarygodnego źródła.

7. Warto także zwrócić uwagę, **w jaki sposób można wyłączyć mikrofon lub kamerę** w przypadku, gdy zabawka nie jest używana.

8. Przed pozbyciem się jej należy **pamiętać o usunięciu danych** przywracając urządzenie do stanu fabrycznego.

# 6 SPRAWY MIĘDZYNARODOWE

## CHORWACJA: 2,2 MLN EURO ZA NARUSZENIE AŻ TRZECH ARTYKUŁÓW Z RODO

**Chorwacki organ nadzorczy nałożył administracyjną karę pieniężną na agencję windykacyjną B2 Kapital w wysokości 2,2 mln euro z powodu naruszenia art. 13, 28 i 32 RODO.**

W grudniu 2022 roku chorwacki organ nadzorczy otrzymał anonimową skargę, w której stwierdzono, że doszło do nieuprawnionego przetwarzania przez agencję windykacyjną dużej liczby danych osobowych dłużników. Wraz ze skargą organ otrzymał zestawienie danych, dostarczone na nośniku typu przenośna pamięć USB. Zestawienie to obejmowało następujące dane osobowe: imiona i nazwiska, daty urodzenia i osobiste numery identyfikacyjne – łącznie ponad 77 tys. osób fizycznych, które miały niespłacone długi w instytucjach kredytowych. Długi te zostały zakupione przez agencję windykacyjną na podstawie umowy cesji. Sprawę nagłośniły także media. Jak ustalono podczas podstępowania administrator nie poinformował osób, których dane dotyczą, w dokładny i jasny sposób o przetwarzaniu ich danych osobowych (polityka prywatności) w odniesieniu do podstawy prawnej, co jest sprzeczne z art. 13 ust. 1 RODO. Spowodowało to nieprzejrzyste przetwarzanie danych osobowych osób, których dane dotyczą. Wbrew art. 28 RODO administrator danych nie zawarł z podmiotem przetwarzającym umowy powierzenia przetwarzania danych osobowych w ramach usługi monitorowania zwykłej upadłości konsumenckiej, przez co zagrożone było bezpieczeństwo danych osobowych ponad 83 tys. osób, których dane dotyczą (osobistych numerów identyfikacyjnych).

Administrator nie zastosował odpowiednich środków technicznych i organizacyjnych przy przetwarzaniu danych osobowych, co jest sprzeczne z art. 32 ust. 2 RODO, w wyniku czego doszło do naruszenia bezpieczeństwa danych osobowych wszystkich osób, których dane dotyczą (co najmniej 132,6 tys. w momencie nadzoru), tj. imienia i nazwiska, daty urodzenia i osobistego numeru identyfikacyjnego, a w konsekwencji wszystkich danych osobowych z systemów przechowywania agencji windykacyjnej, które są informacjami finansowymi. Ustalono, że naruszenie trwa co najmniej od 2019 roku i do tej pory nie zostało usunięte, a wszystko to z powodu niestosowania właściwych środków ochrony.

Źródło: **decyzja organu nadzorczego**

# 6 SPRAWY MIĘDZYNARODOWE

## ORGAN NADZORCZY DS. OCHRONY DANYCH HOLANDII PROSI O WYJAŚNIENIA W SPRAWIE CHATGPT

**Holenderski organ ochrony danych jest zaniepokojony przetwarzaniem danych osobowych w organizacjach korzystających z tak zwanej generatywnej sztucznej inteligencji (AI), np. ChatGPT.**

Holenderski organ ochrony danych poprosił listownie o wyjaśnienia dotyczące chatbota ChatGPT producenta oprogramowania, OpenAI. Organ nadzorczy chciał wiedzieć, między innymi, w jaki sposób OpenAI przetwarza dane osobowe podczas szkolenia systemu bazowego. ChatGPT to chatbot, który może udzielać pozornie przekonujących odpowiedzi na wiele różnych pytań. Na przykład, użytkownicy mogą poprosić ChatGPT o odrobienie pracy domowej z matematyki lub napisanie kodu komputerowego albo zwrócić się o poradę w kwestiach związanych z relacjami lub kwestiami medycznymi. W samej Holandii 1,5 miliona osób skorzystało z chatbota w ciągu pierwszych 4 miesięcy od jego uruchomienia.

### Przeszkoleni w zakresie danych osobowych

ChatGPT opiera się na zaawansowanym modelu językowym (GPT) szkolonym z wykorzystaniem danych. Uczy się na danych zgromadzonych w Internecie, ale także poprzez przechowywanie i wykorzystywanie pytań zadawanych przez ludzi. Dane te mogą zawierać wrażliwe i bardzo osobiste informacje, Chat GPT przykładowo może udzielić porady dotyczącej kłótni małżeńskiej lub spraw medycznych. Holenderski organ ochrony danych chciał dowiedzieć się od OpenAI, czy pytania ludzi są wykorzystywane do szkolenia algorytmu, a jeśli tak, to w jaki sposób. Organ nadzorczy miał również pytania dotyczące sposobu, w jaki OpenAI gromadzi i wykorzystuje dane osobowe z Internetu. Ponadto organ nadzorczy zaniepokojony informacjami, które GPT wytwarza o osobach, ma obawy, że wygenerowane odpowiedzi na pytania mogą być nieodpowiednie, nieaktualne, a nawet obraźliwe i istnieje ryzyko utraty kontroli nad ich późniejszym zastosowaniem. Nie jest jasne, czy i w jaki sposób OpenAI może prostować lub usuwać te dane. Organy europejskie, zajmujące się ochroną danych osobowych, w trosce o swoich obywateli, postanowiły wypracować wspólne podejście do tematu ChatuGPT. W ramach partnerstwa w Europejskiej Radzie Ochrony Danych utworzyły Grupę zadaniową ds. Chat GPT, skupioną na wymianie informacji oraz koordynacji działań w tym zakresie.

### Nadzór

Algorytmy i sztuczna inteligencja często wykorzystują dane osobowe. Holenderski organ nadzorczy sprawuje nadzór nad tym, by stosowanie algorytmów było zgodne z RODO oraz by stale monitorować ryzyka i skutki z nim związane. Ponieważ algorytmy – z wykorzystaniem danych osobowych lub bez - można znaleźć we wszystkich sektorach, ważne jest stałe monitorowanie ryzyka i skutków.

Źródło: **decyzja organu nadzorczego**

## CO 3. POLAK ZETKNĄŁ SIĘ Z PRÓBĄ WYŁUDZENIA DANYCH, A CO 8. PADŁ JEGO OFIARĄ

**1/3 Polaków potwierdza, że spotkała się w ciągu ostatniego roku z próbą wyłudzenia ich danych osobowych poprzez fałszywy telefon, link bądź e-mail. 12 proc. padło ofiarą takiego oszustwa, a drugie tyle nie potrafi stwierdzić, czy taki fakt miał miejsce. Wyłudzenia to jednak niejedyny sposób, w który tracimy kontrolę nad swoimi danymi. 13,2 proc. doświadczyło ich wycieku z firm prywatnych i instytucji publicznych, a 22 proc. osób nie ma pewności co do tego, czy ich dane nie trafiły stamtąd w ręce przestępców. Takie wnioski płyną z najnowszego badania serwisu ChronPESEL.pl i Krajowego Rejestru Długów pod patronatem Urzędu Ochrony Danych Osobowych i Instytutu Prawa Ochrony Danych Osobowych.**

Jak wynika ze statystyk Urzędu Ochrony Danych Osobowych, liczba zgłaszanych naruszeń ochrony danych osobowych w ostatnich latach rośnie. W 2022 roku do UODO zgłoszono niemal 13 tys. takich przypadków, podczas gdy dwa lata wcześniej było ich 7,5 tys. Rzeczywista skala zagrożenia bezpieczeństwa danych osobowych jest jednak znacznie wyższa.

– Wiele osób może nie być świadomych tego, że ich dane osobowe trafiły w niepowołane ręce. Zwłaszcza, jeśli chodzi o te zgromadzone w różnych instytucjach czy firmach, nad którymi nie mamy kontroli. Możemy nawet nie pamiętać, że udostępnialiśmy je jakiemuś podmiotowi, więc informacja o wycieku z jego baz danych nas nie zaalarmuje. Dodatkowo część z nas ignoruje taki fakt, bo sądzi, że i tak nie może w tej sytuacji nic zrobić. A właśnie na to liczą przestępcy. Korzystają z naszej niewiedzy i nieostrożności, ale też poczucia braku odpowiedzialności za bezpieczeństwo swoich danych. Wyniki naszego badania pokazują, że mało kto sądzi, iż sam powinien o nie zadbać – mówi Bartłomiej Drozd, ekspert serwisu **ChronPESEL.pl.**

Według badania „Wiedza na temat bezpieczeństwa ochrony danych osobowych w Polsce” 1/4 Polaków sądzi, że potrafi wskazać, kto powinien zająć się neutralizacją negatywnych skutków wycieku wrażliwych danych. 37 proc. nie ma o tym pojęcia, a drugie tyle nie ma na ten temat zdania. Respondenci, zapytani o konkrety, w większości wskazują na podmiot, który jest odpowiedzialny

za taką sytuację oraz policję i prokuraturę. Tak sądzi 2/3 z nich. Często wymieniają też inspektorów ochrony danych i UODO. Najrzadziej wskazują na osoby, których dane zostały upublicznione. Wyniki te pokazują, że wciąż nie doceniamy własnej roli w procesie chronienia swoich danych osobowych.

### Chcemy wiedzieć, że doszło do wycieku, ale nie jak zneutralizować jego skutki

Od podmiotów odpowiedzialnych za wyciek danych oczekujemy przede wszystkim informacji o tym, że do takiej sytuacji doszło, jakie dane trafiły w niepowołane ręce (po 63,5 proc. wskazań) oraz wdrożenia działań zmniejszających ryzyko wystąpienia podobnych zdarzeń w przyszłości (60,2 proc.). W mniejszym stopniu interesują nas informacje do kogo nasze dane trafiły (54,8 proc.), jakie są możliwe skutki takiego wycieku (49,5 proc.) oraz rekomendacje działań, które powinniśmy sami podjąć, żeby jego konsekwencje były dla nas jak najmniej negatywne (45,4 proc.).

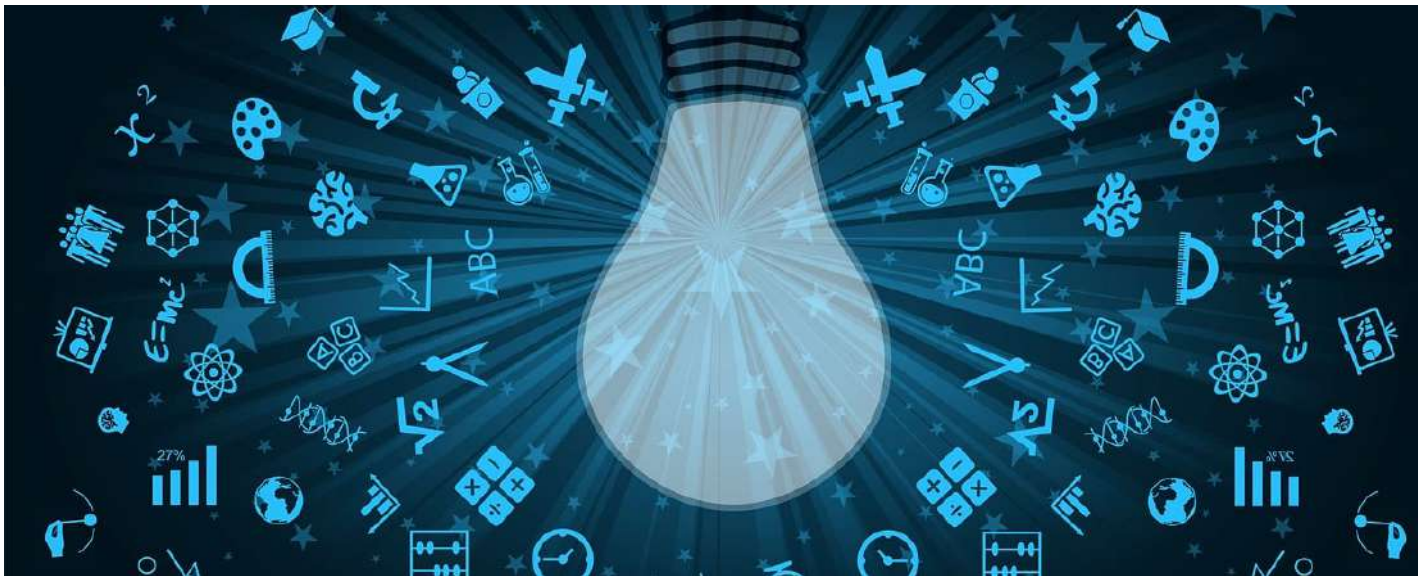
– To niestety ilustracja częstej postawy, że „to nie nasz kłopot", niech się martwi ten, kto zawinił. To oczywiście racja, że podmiot odpowiedzialny za brak należytej ochrony naszych danych powinien zrobić wszystko, żebyśmy przez to nie ucierpieli. Stąd zasadne są oczekiwania ponad połowy ankietowanych, że od takiej firmy bądź instytucji uzyskają wsparcie prawne czy pokrycie kosztów konsekwencji wycieku. Ale to nam komornik potem zajmie konto, jeśli ktoś na przykład założy na nasze dane fikcyjną firmę i wyłudzi z hurtowni towar za kilka milionów złotych. Po kilku latach procesu w końcu się wybronimy, ale stresu nikt nam nie zrekompensuje. Lepiej więc monitorować na bieżąco, czy ktoś nie używa naszego PESEL-u i reagować natychmiast, gdy zostaniemy o tym ostrzeżeni – dodaje Bartłomiej Drozd.

Na szczęście tylko co 3. ankietowany oczekuje w takiej sytuacji rabatu na usługi firmy, z której doszło do wycieku. To świadczy o tym, że coraz większa grupa Polaków rozumie, że ich dane to nie towar, którym można handlować i rozumie, że konsekwencje wycieku danych mogą mieć dla nich poważne skutki.

– Ogólne rozporządzenie o ochronie danych, czyli RODO, zapewnia właściwy balans pomiędzy prawami przedsiębiorców, administratorów a prawami osób, których dane dotyczą. Administratorzy muszą gwarantować ochronę przetwarzanych przez siebie danych osobowych oraz legitymować się podstawą do ich przetwarzania. RODO kładzie także nacisk na transparentność przetwarzania danych, czego wyrazem jest między innymi rozbudowanie obowiązku informacyjnego, dzięki któremu wiemy, kto i na jakiej podstawie przetwarza nasze dane. Z kolei w sytuacji, kiedy dochodzi do naruszenia ochrony danych, przykładowo w postaci wycieku, i zarazem istnieje wysokie ryzyko dla praw i wolności osoby, której dane dotyczą wynikające z naruszenia, administrator jest zobowiązany bez zbędnej zwłoki zawiadomić osobę o incydencie w sposób jasny i używając prostego języka. To bardzo ważne, ponieważ takie informacje umożliwią tej osobie podjęcie niezbędnych działań zapobiegawczych – zaznacza Adam Sanocki, Dyrektor Departamentu Komunikacji Społecznej oraz Rzecznik Prasowy UODO.

## W deklaracjach wypadamy nieźle

Kroki naprawcze, które powinny podjąć podmioty po naruszeniu ochrony danych osobowych, to jedno. Drugie, to nasze własne działania. Wbrew opinii wyrażonej przez badanych, osoby, których dane dotyczą, również powinni aktywnie zadbać o to, aby uchronić się przed konsekwencjami kradzieży tożsamości. Większość Polaków na pytanie „Jakie działania podejmujesz, aby zapewnić bezpieczeństwo swoim danym osobowym?" wskazuje przede wszystkim na ostrożność w podawaniu innym numeru PESEL (94 proc.), nie klika w linki z SMS-ów czy e-maili, nie otwiera wiadomości e-mailowych niewiadomego pochodzenia oraz zawsze niszczy dokumenty zawierające dane osobowe przed ich wyrzuceniem (po ok. 92 proc). Gorzej wypadamy, jeśli chodzi o bezpieczeństwo w sieci. Zainstalowany program antywirusowy na komputerze, laptopie lub tablecie ma 85 proc. osób. Na smartfonie używa go już niecałe 3/4 z nas. Podobny odsetek deklaruje, że nie powtarza tego samego hasła do logowania w różnych miejscach. Dodatkowo, prawie 70 proc. zawsze sprawdza, czy dane osobowe przekazywane firmom lub instytucjom mogą zostać dostarczone także ich biznesowym partnerom.



Rzecznik prasowy UODO zwraca uwagę, że odpowiednio chroniąc swoje dane osobowe, możemy ograniczyć ryzyko ich wykorzystania przez osoby do tego nieuprawnione.

– Pamiętajmy, aby zachować czujność podczas podawania danych przez Internet. Cieszy nas fakt, że działania edukacyjne przynoszą skutek i Polacy są ostrożniejsi w podawaniu danych w postaci numeru PESEL czy też nie otwierają wiadomości i załączników nieznanego pochodzenia. To jednak tylko kilka podstawowych zasad, które powinniśmy stosować w życiu codziennym. W dobie nowych technologii, dostępnych urządzeń wykorzystujących sztuczną inteligencję, przestępcy stosują coraz nowsze sposoby na pozyskiwanie naszych danych osobowych. Co świadczy o tym, jak cenną walutę stanowią wszelkie informacje na nasz temat – dodaje Adam Sanocki.

## Monitoruj własny PESEL

Bartłomiej Drozd zwraca jednak uwagę, że są to działania, które zabezpieczą nas przed ujawnieniem wrażliwych danych przez nas samych. Nie uchronią jednak przed negatywnymi skutkami wycieku danych z zasobów firm i instytucji, w których są już one zgromadzone. Tymczasem z takiego monitoringu własnego PESEL-u, który pozwala na błyskawiczną reakcję w razie jego wykorzystania przez przestępców, korzysta 42 proc. ankietowanych.

W badaniu serwisu ChronPESEL.pl i Krajowego Rejestru Długów niemal 33 proc. respondentów przyznało, że w ciągu ostatnich 12 miesięcy spotkało się z próbą wyłudzenia ich danych przez fałszywy telefon, SMS lub e-mail. 1/4 osób pamiętała też, że takiej sytuacji doświadczył ich znajomy bądź członek rodziny. 12,4 proc. badanych przyznało, że oszustom udało się wyłudzić takim sposobem ich dane. Dla podobnego odsetka osób (13,7 proc.) ofiarą był ktoś bliski. Kolejne 13,1 proc. Polaków mierzyło się z wyciekiem danych z prywatnych firm (7,5 proc.) i instytucji publicznych (5,6 proc.). Podobnie wskazywali w odniesieniu do swoich rodzin i znajomych. Niemal 6 proc. badanych doświadczyło też kradzieży danych w wyniku włamania na komputer lub telefon. 7,5 proc. wskazało, że przytrafiło się to osobie z jej otoczenia.

**Badanie „Wiedza na temat bezpieczeństwa ochrony danych osobowych w Polsce" zostało przeprowadzone w maju 2023 r. przez IMAS International na reprezentatywnej próbie 1007 Polaków na zlecenie serwisu ChronPESEL.pl i Krajowego Rejestru Długów Biura Informacji Gospodarczej pod patronatem Urzędu Ochrony Danych Osobowych oraz Instytutu Prawa Ochrony Danych Osobowych.**

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl