URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 05/05/25

www.uodo.gov.pl

SPIS TREŚCI

Szanowni Państwo,

kampania wyborcza przed wyborami prezydenckimi była kolejną lekcją ochrony danych osobowych. Sztab jednego z kandydatów ujawnił dane osobowe, w tym dane o stanie zdrowia, obywatela, którego historia miała związek z działaniami kandydata na prezydenta. Potem drugi kandydat powtórzył publicznie nazwisko tej osoby. Tymczasem, osoba, której dane zostały udostępnione, nie wyraziła zgody na ich ujawnienie. Nie przemawia za takim ujawnieniem także żaden interes publiczny. Sprawę dotyczącą wątpliwości związanych z nieruchomością, czy umowami można było wyjaśnić publicznie bez ujawniania danych osobowych człowieka.

Z tych też powodów zmuszony byłem zająć się tymi i kolejnymi sprawami, w których mogło dojść do bezpodstawnego przetwarzania danych osobowych w przestrzeni publicznej.

Powyższe przypadki stanowią dowód, że nadal w sferze publicznej zbyt mało wagi przywiązujemy do ochrony danych osobowych, że ich znaczenie może ujść naszej uwadze, zwłaszcza gdy angażujemy się w realizację jakiegoś słusznego często celu. Tymczasem o danych osobowych nie można zapominać nigdy. Krzywda wyrządzona drugiemu człowiekowi przez nieopatrzne ich ujawnienie może być nie do naprawienia.

Na straży naszych danych i naszego prawa do prywatności stoi RODO – unijne rozporządzenie ogólne o ochronie danych osobowych. Stosowane jest ono już od siedmiu lat – właśnie minęła kolejna rocznica. „RODO jest sojusznikiem rozwoju – bo jest on niemożliwy bez zaufania, a ono wiąże się z ochroną danych” – przekonujemy w okolicznościowym nagraniu w serwisie YouTube. „Dziś już wszyscy lepiej dbamy o dane. To już nie jest temat specjalistyczny”.

RODO ma jednak opinię prawa specjalistycznego i zbyt obciążającego na przykład małe i średnie przedsiębiorstwa czy organizacje pozarządowe. Nasze stanowisko jest jasne: problemem nie jest RODO, ale przede wszystkim zbyt formalistyczny sposób jego stosowania w praktyce. Prawo ochrony danych jest elastyczne właśnie dlatego, że jest oparte na analizie ryzyka, a nie na rygorystycznym wypełnianiu mnóstwa szczegółowych zaleceń.

Wyjaśnianie, jak stosować RODO, może pomóc – a nie przeszkadzać – w prowadzeniu działalności organizacyjnej i w biznesie, i stanowi jedno z zadań Urzędu Ochrony Danych Osobowych. W maju w ramach akcji „UODO rusza w kraj” wraz ze współpracownikami odwiedziłem Wielkopolskę.

O tym, jak stosować RODO, rozmawialiśmy tam z przedstawicielami administracji oraz z przedsiębiorcami.

Współorganizowaliśmy specjalne szkolenie dla inspektorów ochrony danych instytucji kościelnych (naszym partnerem był Kościelny Inspektor Ochrony Danych i Fundacja Konferencji Episkopatu Polski Bona Fama). Zorganizowaliśmy też seminarium o ochronie danych razem z Zakładem Ubezpieczeń Społecznych. Rozmawialiśmy o tym, jak minimalizować zagrożenia dla danych, które niesie automatyczne ich przetwarzanie.

27 maja mieliśmy zaszczyt wręczyć nagrody laureatom kolejnej edycji ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa". Statuetką „Złotego Pióra" zostały uhonorowane warsztaty projektowe połączone z tworzeniem gry planszowej „Odoland. Gra o Twoje dane osobowe" Zespołu Szkół nr 1 im. Stanisława Staszica w Kwidzynie.

Cel tego konkursu to: promowanie zasad ochrony danych osobowych wśród dzieci i młodzieży, popularyzacja wiedzy o ochronie danych osobowych wśród uczniów, podkreślenie istotnej roli tematyki ochrony prywatności i danych osobowych w życiu każdego człowieka.

Tak jak w każdym miesiącu podkreślaliśmy to, że dane osobowe są wszędzie i dotyczą każdej dziedziny życia.

- Zwróciłem więc uwagę, że pomysł nagrywania zabiegów leczenia endometriozy będzie oznaczać głęboką ingerencję w prywatność, i projektowane przepisy trzeba doprecyzować tak, by zminimalizować zagrożenie dla danych.
- Także planowane zmiany w rejestracji do lekarza muszą uwzględniać ochronę danych osobowych. Rejestracja wspierana przez system informatyczny wykorzystujący nasze dane biometryczne (głos) ułatwi nam życie, ale wymaga odpowiednich zabezpieczeń i precyzji w projektowanych przepisach.
- Zwróciłem uwagę, że po wyroku TSUE doprecyzowania wymagają przepisy o dostępie do informacji publicznej. Chodzi o sytuację, kiedy prawo do informacji publicznej koliduje z prawem do ochrony prywatności. Przepisy w takiej sytuacji powinny dawać zainteresowanym realną ochronę.
- Włączyliśmy się w prace Ministerstwa Sprawiedliwości nad zakresem danych świadków, które są pozyskiwane i przetwarzane w postępowaniach karnych. Zmiany prawa są konieczne ze względu na coraz szersze możliwości techniczne dotyczące zbierania i przetwarzania takich danych.

Świadomość znaczenia danych osobowych wzrasta, choć nie zawsze wyciągamy z tego właściwe wnioski. Przykładem jest interwencja w Polskim Związku Piłki Nożnej po tym, jak uzależnił on udział dzieci w turnieju piłkarskim od tego, czy rodzice wyrażą zgodę na przetwarzanie danych osobowych swoich pociech. Poprosiłem o wyjaśnienie, jaka była podstawa prawna takiego działania i po co PZPN-owi wizerunki dzieci. Wkrótce, 1 czerwca, obchodzić będziemy Dzień Dziecka. Pamiętajmy więc szczególnie tego dnia, że wizerunek naszych dzieci jest drogocenny i powinniśmy chronić go codziennie.

Mirosław Wróblewski
Prezes UODO

Drodzy Czytelnicy!

Z uwagi na wszechobecny temat wyborów polecam Państwu ponowną lekturę materiału z „Biuletynu UODO" z czerwca 2024 r. „Ochrona danych osobowych w procesie wyborczym". Tegoroczna rywalizacja o stanowisko prezydenta, pokazała, jak łatwo – niestety – politycy zapominają o ochronie danych osobowych, która jest prawem każdego z nas.

W majowym numerze skupiamy się jednak na innych istotnych kwestiach. Znów gościmy na naszych łamach parę głównodowodzących, tym razem Departamentu Współpracy Międzynarodowej – Marię Owczarek, dyrektorkę departamentu oraz Krzysztofa Króla – zastępcę dyrektorki DWM. Opowiadają m.in. o współpracy organów nadzorczych, o ich roli w procesie certyfikacji czy wspólnych wysiłkach EROD w znalezieniu porozumienia w sprawach związanych ze sztuczną inteligencją.

O tym jak ważne jest zachowanie czujności podczas publikacji nagrań w internecie, przekonał się pewien pracownik restauracji. W trakcie realizacji promocyjnego nagrania na platformę TikTok nie zauważył, że w kadrze widać terminal płatniczy z danymi klienta. W efekcie liczne dane zostały publicznie udostępnione. Prezes UODO po skardze obywatela upomniał restauratora.

Urząd Ochrony Danych Osobowych konsekwentnie zwraca uwagę, że brak regularnych aktualizacji oprogramowania może prowadzić do poważnych naruszeń bezpieczeństwa danych osobowych. Dowodzą tego przytoczone w tym wydaniu periodyku decyzje Prezesa UODO, na mocy których administratorów ukarano administracyjną karą pieniężną lub upomnieniem, jak również orzecznictwo.

W marcu tego roku Europejska Rada Ochrony Danych opublikowała podsumowanie dotychczasowych wytycznych dotyczących naruszeń ochrony danych osobowych. Za dokumentem przedstawiamy najważniejsze zagadnienia poruszone w publikacji EROD i przykładowe scenariusze naruszeń ochrony danych osobowych, a także działań, jakie należy podjąć w ich następstwie.

EROD wydała również sprawozdanie za rok 2024. Zawiera ono przegląd prac Rady przeprowadzonych w 2024 r. i przybliża kluczowe wydarzenia w minionym okresie, takie jak przyjęcie strategii na lata 2024-2027, wzrost liczby opinii zgodności z art. 64 ust. 2 oraz podjęte wysiłki na rzecz zapewnienia ochrony danych osobowych.

Niektóre sklepy tytoniowe we Francji zainstalowały kamery z systemami opartymi na sztucznej inteligencji, aby oszacować wiek klientów i zapobiec sprzedaży produktów zabronionych nieletnim. W celu przeanalizowania zgodności tych systemów, które mają znaczący wpływ na prawa i wolności, francuski organ ochrony danych (CNIL) organizuje prace w porozumieniu z zaangażowanymi podmiotami.

W tym numerze piszemy również o kontrolach francuskiego organu ochrony danych. W 2025 r. CNIL skupi się na danych gromadzonych za pośrednictwem aplikacji mobilnych, cyberbezpieczeństwie władz lokalnych i przetwarzaniu danych przez administrację więzienną.

Informujemy o karze w wysokości 530 milionów euro, jaką Irlandzki Organ Ochrony Danych (DPC) nałożył na TikToka. Dochodzenie zostało wszczęte przez DPC, wiodący organ nadzorczy dla TikToka, w celu zbadania zgodności z prawem przekazywania przez platformę danych osobowych jej użytkowników w Europejskim Obszarze Gospodarczym do Chińskiej Republiki Ludowej. Ponadto w dochodzeniu zbadano, czy przekazywanie informacji użytkownikom w związku z takimi transferami spełniało wymogi przejrzystości TikToka zgodnie z wymogami RODO.

UODO bierze udział w konkursie Komisji Europejskiej, istotnym dla szczególnej ochrony danych osobowych dzieci.
W kwietniu 2025 r. Urząd złożył wniosek o dofinansowanie projektu Safe DigitAl Environment For ChildrEn – awareness campaign – SAFE, dotyczącego przeprowadzenia kampanii edukacyjnej w zakresie podnoszenia świadomości na temat bezpiecznego środowiska cyfrowego dla dzieci. Trzymajcie kciuki, żeby KE doceniła nasze wysiłki.

Ja z kolei, z okazji święta dzieci, życzę im, by czuły się ważne i kochane oraz znały swoje przywileje. Niech dorośli pamiętają, że macie prawo do tajemnicy, intymności i dorastania w świecie – tym realnym oraz cyfrowym, w którym możecie czuć się bezpieczni, jeśli zachowacie odpowiednią ostrożność i będziecie przestrzegać zasad, które UODO konsekwentnie przekazuje.

Karol Witowski
Rzecznik Prasowy UODO

WYMIENIAMY SIĘ WIEDZĄ I SPOSTRZEŻENIAMI Z INNYMI ORGANAMI NADZORCZYMI


Z Marią Owczarek, dyrektorką Departamentu Współpracy Międzynarodowej oraz z Krzysztofem Królem, zastępcą dyrektorki, rozmawiał Karol Witowski, Rzecznik Prasowy UODO.

Od 1 stycznia, w ramach reorganizacji w UODO, wyodrębniony w nowej strukturze został Departament Współpracy Międzynarodowej, którego została Pani dyrektorką. Czym zajmuje się Departament?

Maria Owczarek: Nowoutworzony Departament Współpracy Międzynarodowej – poza dotychczasowymi zadaniami, związanymi ze współpracą międzynarodową Prezesa UODO, którą realizowaliśmy wcześniej w ramach właściwości Departamentu Współpracy Międzynarodowej i Edukacji – objął także nowe zadania (należące dotąd do innych departamentów), związane z certyfikacją i transferami danych do państw trzecich i organizacji międzynarodowych. W ramach departamentu wydzielony został także Wydział ds. Postępowań Transgranicznych, który zajmuje się prowadzeniem postępowań w ramach mechanizmu kompleksowej współpracy (tzw. One-Stop-Shop), których prowadzenie należało wcześniej do Departamentu Skarg.

Nowa struktura pozwoliła skupić wszystkie sprawy dotyczące współpracy międzynarodowej w jednym miejscu. Umożliwiło nam to jeszcze lepszą organizację pracy Urzędu na forach europejskich i międzynarodowych współpracy, a także bardziej efektywną i skuteczną współpracę z innymi organami ochrony danych w ramach Europejskiej Rady Ochrony Danych (EROD).

Za nami 7 lat stosowania RODO. W wywiadzie dla biuletynu sprzed 2 lat powiedziała Pani, że jednym z największych sukcesów rozporządzenia jest wzmocnienie pozycji europejskich organów nadzorczych i współpraca między nimi, dzięki narzędziom, które zagwarantowało RODO i za sprawą ustanowienia EROD. Czy przez te dwa lata coś się zmieniło?

1 ROZMOWA Z EKSPERTEM

M.O.: W dalszym ciągu stoję na stanowisku, że jednym z najważniejszych osiągnięć RODO jest wzmocnienie roli europejskich organów ochrony danych oraz ich współpracy, co zostało umożliwione dzięki narzędziom wprowadzonym przez RODO i utworzeniu EROD. Tak jak wspominałam w poprzednim wywiadzie, na początku EROD koncentrowała się na opracowywaniu wytycznych, które miały na celu wyjaśnienie kluczowych zasad RODO oraz dostarczenie jasnej interpretacji pojęć w nim zawartych. W związku z tym, że RODO było nowością, ważne dla nas – organów ochrony danych – było przedstawienie spójnej i jasnej interpretacji przepisów, która zagwarantuje ich jednolite stosowanie w UE. Obecnie EROD kontynuuje prace nad wytycznymi, ale aktualnie skupia się bardziej na wzmocnieniu współpracy pomiędzy organami, monitorowaniu egzekwowania przepisów, a także na promowaniu narzędzi rozliczalności, takich jak wiążące reguły korporacyjne, kodeksy postępowania czy certyfikacja.

W poprzednim wywiadzie wspominała Pani także o wyzwaniach dla współpracy organów wynikających z różnic w krajowych postępowaniach administracyjnych i związanej z tym inicjatywie organów ochrony danych, tzw. „liście życzeń", której efektem są trwające obecnie prace nad rozporządzeniem proceduralnym. Na jakim etapie są prace nad rozporządzeniem i co zmieniło się od czasu, gdy ostatnio o tym rozmawialiśmy?

M.O.: Tak jak mówiłam, organy nadzorcze same zidentyfikowały przeszkody proceduralne, które ich zdaniem są trudne do wyeliminowania na poziomie stosowania RODO i wskazały potrzebę wprowadzenia zmian. W następstwie swojego oświadczenia w sprawie współpracy w zakresie egzekwowania prawa Europejska Rada Ochrony Danych przesłała Komisji Europejskiej wykaz aspektów proceduralnych, wymagających dalszej harmonizacji na szczeblu UE, w celu zmaksymalizowania pełnej skuteczności mechanizmów współpracy ustanowionych w RODO (tzw. „lista życzeń").

Następnie Komisja opublikowała wniosek dotyczący rozporządzenia ustanawiającego dodatkowe zasady proceduralne, odnoszące się do egzekwowania RODO, w sprawie którego EROD i Europejski Inspektor Ochrony Danych (EIOD) przedstawili zalecenia we wspólnej opinii.

EROD z zadowoleniem przyjęła cel wniosku, jakim jest lepsza ochrona praw podstawowych poprzez szybsze, sprawniejsze i skuteczniejsze procedury egzekwowania prawa. Jednocześnie podkreśliła, że wprowadzenie wszelkich nowych kroków proceduralnych i dodatkowych zadań organów nadzorczych spowoduje zapotrzebowanie na dodatkowe zasoby organów.

1 ROZMOWA Z EKSPERTEM

Z tego powodu EROD wezwała prawodawców UE, a także Komisję Europejską i państwa członkowskie do podjęcia niezbędnych działań w celu zapewnienia, aby EROD i jej członkowie dysponowali zasobami niezbędnymi do skutecznego wdrożenia RODO i przepisów proceduralnych.

W kwietniu 2024 r. Parlament Europejski i Rada wprowadziły poprawki do projektu rozporządzenia do wniosku Komisji Europejskiej dotyczącego rozporządzenia ustanawiającego dodatkowe przepisy proceduralne dotyczące egzekwowania RODO, w odpowiedzi na które EROD w październiku 2024 r. przyjęła oświadczenie.

W oświadczeniu z 2024 r. EROD przyjęła stanowisko Parlamentu Europejskiego i ogólne podejście Rady do wniosku. EROD zauważyła, że prawodawcy uwzględnili niektóre zalecenia zawarte we wspólnej opinii, ale zaleciła dalsze zajęcie się niektórymi elementami, aby nowe rozporządzenie mogło osiągnąć swoje cele, tj. usprawnić współpracę i poprawić egzekwowanie RODO. Ponadto EROD podkreśliła, że duża liczba odniesień do prawa krajowego w nowym rozporządzeniu nie byłaby zgodna z duchem zwiększonej harmonizacji i dlatego należy jej unikać.

W szczególności EROD przypomniała o potrzebie ustanowienia podstawy prawnej i zharmonizowanej procedury polubownego rozstrzygania sporów, przedstawiając zalecenia mające na celu zapewnienie osiągnięcia konsensusu w sprawie podsumowania kluczowych kwestii w najbardziej efektywny sposób. EROD z zadowoleniem przyjęła również włączenie dodatkowych terminów proceduralnych, przypominając jednocześnie, że muszą one być realistyczne.

Podczas gdy EROD przyjęła cel osiągnięcia większej przejrzystości, wprowadzenie wspólnych akt sprawy, zgodnie z propozycją Parlamentu Europejskiego, wymagałoby – zdaniem organów – złożonych zmian w systemach zarządzania dokumentami i komunikacji stosowanych na szczeblu europejskim i krajowym.

EROD przyjęła także poprawkę Rady umożliwiającą wiodącemu organowi ochrony danych rezygnację z tzw. wzmocnionej współpracy w prostych i nieskomplikowanych sprawach, ale podkreśla potrzebę dalszego wyjaśnienia zakresu możliwości skorzystania z takiej procedury rezygnacji.

Jak powiedziała Przewodnicząca EROD Anu Talus, w komunikacie opublikowanym po posiedzeniu plenarnym: „Projekt rozporządzenia ma potencjał, aby znacznie usprawnić egzekwowanie RODO poprzez zwiększenie efektywności rozpatrywania spraw. Potrzebna jest większa harmonizacja na poziomie UE, aby zmaksymalizować pełną skuteczność mechanizmów współpracy i spójności RODO”.

Aktualnie, podczas Polskiej Prezydencji przy Radzie UE, trwają końcowe tak zwane „trójstronne” negocjacje między Parlamentem Europejskim, państwami członkowskimi i Komisją Europejską.

1 ROZMOWA Z EKSPERTEM

Czekamy z niecierpliwością na efekt negocjacji i przyjęcie ostatecznego tekstu rozporządzenia, które – mam nadzieję – nie tylko ułatwi współpracę pomiędzy organami, ale przede wszystkim przyczyni się do lepszej i skuteczniejszej ochrony praw osób, których dane dotyczą.

Pozostając w temacie współpracy organów, Meta niedawno ogłosiła plany w zakresie wykorzystywania danych upublicznionych przez użytkowników do szkolenia systemów generatywnej sztucznej inteligencji w Europie. Jak wygląda współpraca dot. weryfikacji działania mechanizmu sprzeciwu przez Prezesa Urzędu z pozostałymi organami nadzorczymi, będącymi członkami EROD?

M.O.: Działanie mechanizmu wyrażenia sprzeciwu było weryfikowane przez organy nadzorcze na bieżąco od samego początku od kiedy jest on dostępny, czyli od 16 kwietnia 2025 r. Z zebranych przez nas dotychczas informacji wynika, że do użytkowników usług Meta trafiły wiadomości elektroniczne lub powiadomienia na platformach społecznościowych dotyczące planowanego przetwarzania, a mechanizm sprzeciwu jest również dostępny z poziomu centrum prywatności w aplikacjach Meta.

Otrzymaliśmy również skargę w związku z planowanym w zeszłym roku przetwarzaniem danych przez Metę. Skarga została złożona w ramach skoordynowanej akcji organizacji NOYB. Skargi dotyczące przetwarzania przez Meta są rozpatrywane przez irlandzki organ nadzorczy, jako wiodący organ nadzorczy, który jest właściwy z uwagi na lokalizację w UE głównej siedziby Mety w Irlandii.

Działania Meta w kontekście zgodności z przepisami RODO są przedmiotem współpracy między organami nadzorczymi, a w szczególności irlandzkim organem oraz przedstawicielami Meta. Polski organ nadzorczy również w niej uczestniczy.

Europejska Rada Ochrony Danych wypowiadała się w przedmiocie zgodności z RODO takiego przetwarzania w Opinii EROD 28/2024 w sprawie niektórych aspektów ochrony danych związanych z przetwarzaniem danych osobowych w kontekście modeli sztucznej inteligencji – odnoszącej się m.in. do tego, kiedy może być ono oparte na podstawie uzasadnionego interesu. Obecny kształt planów przedstawionych przez spółkę Meta jest wynikiem między innymi tej właśnie opinii. W przypadku wystąpienia w przyszłości okoliczności, które wskazywałyby na niezgodność takiego przetwarzania z ustaleniami opinii EROD oraz zasadami RODO, organy nadzorcze będą podejmować działania zgodnie z przysługującymi uprawnieniami i procedurami współpracy.

W związku z planami Meta, niemiecki organ nadzorczy w Hamburgu zwrócił się do tej spółki z pismem o wyjaśnienia w tej sprawie. Pismo to może doprowadzić do zastosowania tzw. trybu pilnego, przewidzianego w art. 66 RODO. Na jego podstawie hamburski organ tymczasowo może podjąć

działania (na okres do trzech miesięcy), mające na celu ochronę praw lub wolności osób. W ich efekcie EROD może wydać opinie lub decyzje.

Z tego właśnie mechanizmu w zeszłym roku skorzystał Prezes UODO wobec Meta i zakazał publikowania postów wykorzystujących dane osobowe Pana Rafała Brzoski oraz jego żony Pani Omeny Mensah.

Nowym zadaniem Departamentu Współpracy Międzynarodowej jest także certyfikacja. W związku z tym mam pytanie, jaką rolę odgrywają organy nadzorcze w procesie certyfikacji? Przybliżał Pan to zagadnienie uczestnikom serii webinariów „Certyfikacja w ochronie danych", jednak dla szerszego grona odbiorców temat może się wydawać skomplikowany.

Krzysztof Król: Zacznijmy od przedstawienia uczestników certyfikacji w Polsce. Po pierwsze mamy podmioty certyfikujące. To one są odpowiedzialne za dokonanie właściwej oceny przed udzieleniem lub cofnięciem certyfikacji dotyczącej czynności przetwarzania przez dany podmiot wnioskujący o certyfikację – danego administratora lub podmiot przetwarzający.

Ponieważ ocena czynności przetwarzania jest zadaniem trudnym, wymagającym znacznej wiedzy fachowej oraz odpowiedniej metodologii, RODO przedstawia dalsze uregulowania względem przyznawania certyfikacji. Podmioty certyfikujące muszą zostać akredytowane, zanim będą mogły działać. Zgodnie z RODO akredytacja ta dokonywana może być przez krajowe jednostki akredytujące albo organy nadzorcze. Samodzielna akredytacja przez organ nadzorczy nie została przyjęta przez polskiego ustawodawcę, zatem w Polsce akredytuje krajowa jednostka akredytująca, czyli Polskie Centrum Akredytacji (PCA).

Niemniej jednak organ ochrony danych pełni znaczącą rolę w procesie certyfikacji. Po pierwsze określa krajowe wymogi akredytacji podmiotów certyfikujących. W Polsce dodatkowe wymogi akredytacji podmiotów certyfikujących zostały zatwierdzone przez Prezesa UODO 8 grudnia 2023 r. i są dostępne na stronie Urzędu. Akredytacja podmiotów certyfikujących jest dokonywana na podstawie właśnie tych wymogów oraz standardu ISO/IEC 17065/2012.

Z kolei podmioty certyfikujące udzielają certyfikacji na podstawie danych kryteriów certyfikacji tworzonych przez właścicieli systemu certyfikacji. Kryteria certyfikacji muszą zostać zatwierdzone przez organy ochrony danych. Dany organ nadzorczy ocenia kryteria certyfikacji oraz przygotowuje projekt decyzji w przedmiocie ich zatwierdzenia. Następnie projekt zostaje przekazany Europejskiej Radzie Ochrony Danych, która wydaje opinię dotyczącą zatwierdzenia takich kryteriów.

1 ROZMOWA Z EKSPERTEM

Po uwzględnieniu tej opinii organ nadzorczy zatwierdza kryteria. Zatem udział organów nadzorczych jest niezbędny zarówno przy zatwierdzaniu kryteriów certyfikacji, jak i przy tworzeniu dodatkowych wymogów, na podstawie których dokonywana jest akredytacja podmiotów certyfikujących. Ponadto organ nadzorczy może sam udzielać certyfikacji na podstawie własnego systemu certyfikacji lub też opracować system certyfikacji i powierzyć procedurę certyfikacji podmiotom certyfikującym.

Jakie są działania UODO dot. certyfikacji w ochronie danych osobowych na forum europejskim i krajowym?

K.K.: Na forum krajowym UODO jest zaangażowane w szerzenie wiedzy i promowanie certyfikacji jako mechanizmu wykazywania zgodności z RODO. Przykładem takich działań jest chociażby wspomniana seria webinariów. W jednym z tych webinariów uczestniczył przedstawiciel Polskiego Centrum Akredytacji, z kolei przedstawicielka Urzędu Ochrony Danych Osobowych wzięła udział w podcaście prowadzonym przez PCA.

Nawiązanie relacji z Polskim Centrum Akredytacji, która umożliwia wymianę informacji, współpracę przy projektach jest kolejnym ważnym działaniem na polu krajowym budującym grunt pod sprawne przeprowadzanie certyfikacji RODO w Polsce. Właściwie ten grunt został już przygotowany, bo zatwierdzone zostały również dodatkowe wymogi akredytacji podmiotów przetwarzających. Jesteśmy więc gotowi na pierwsze zgłoszenia od podmiotów chcących uczestniczyć w certyfikacji dot. ochrony danych np. poprzez opracowywanie systemów certyfikacji.

Na forum europejskim prężnie działamy w ramach podgrup Europejskiej Rady Ochrony Danych. Wymieniamy się wiedzą i spostrzeżeniami z innymi organami nadzorczymi, wspólnie dokonujemy oceny kryteriów certyfikacji na potrzeby opinii EROD w przedmiocie zatwierdzenia kryteriów certyfikacji. W ramach EROD rozmawiamy też o sposobach współpracy z organizacją zrzeszającą krajowe jednostki akredytujące – European Accreditation oraz między organami ochrony danych w przypadku certyfikacji obejmującej swym zakresem więcej niż jedno państwo. Pracujemy również nad zatwierdzaniem europejskich znaków jakości w dziedzinie ochrony danych osobowych mających zasięg ogólnoeuropejski.

Dziękuję Państwu za rozmowę.

M.O., K.K.: Dziękujemy bardzo, o wszystkich aktywnościach departamentu współpracy międzynarodowej będziemy informować na stronie UODO (w aktualnościach i zakładce EROD), a także na łamach biuletynu. Zachęcamy też do śledzenia aktywności organów ochrony danych na stronie EROD.

OPROGRAMOWANIE TRZEBA REGULARNIE AKTUALIZOWAĆ

Regularna aktualizacja oprogramowania to wynikający z RODO obowiązek administratora i podmiotu przetwarzającego. Powinna ona stanowić integralny element każdej strategii ochrony danych osobowych. Zaniedbania w tym obszarze mogą prowadzić do poważnych naruszeń bezpieczeństwa danych, a w konsekwencji do odpowiedzialności prawnej z tego tytułu.

W świetle ogólnego rozporządzenia o ochronie danych (RODO) administrator oraz podmiot przetwarzający zobowiązani są do zapewnienia bezpieczeństwa przetwarzanych danych osobowych. W tym celu – stosownie do art. 24 ust. 1 RODO – powinni wdrożyć środki techniczne i organizacyjne odpowiednie do zidentyfikowanego ryzyka. Środki te powinny być w razie potrzeby poddawane przeglądom i uaktualniane. Również art. 32 ust. 1 lit. d RODO wprost wskazuje na konieczność regularnego testowania, mierzenia i oceniania skuteczności wdrożonych zabezpieczeń.

Na konieczność utrzymywania aktualnego oprogramowania wskazują również przepisy ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, a także Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Fundamentalne znaczenie aktualizacji

Zagrożenia cybernetyczne nieustannie ewoluują, a przestępcy są coraz lepiej zorganizowani i kreatywni w swoich działaniach. W miarę jak opracowują coraz bardziej zaawansowane i wyrafinowane sposoby i techniki ataków, programiści wydają aktualizacje oprogramowania, których głównym celem jest naprawa wykrytych luk bezpieczeństwa i wprowadzenie nowych funkcji ochronnych. Korzystanie z najnowszych wersji oprogramowania jest zatem niezbędne dla skutecznej ochrony danych osobowych przed nieuprawnionym dostępem, uszkodzeniem czy utratą.

Ponadto aktualizacje:

• dostosowują oprogramowanie do aktualnych regulacji prawnych dotyczących ochrony danych,

• poprawiają ogólną wydajność systemu, co zmniejsza ryzyko awarii mogących prowadzić do utraty danych,

• zapewniają lepszy dostęp do pomocy technicznej, co może być istotne w przypadku wystąpienia incydentu bezpieczeństwa,

• zawierają optymalizacje, które znacząco zwiększają efektywność działania, eliminują znane błędy wpływające na stabilność pracy oraz wprowadzają dodatkowe funkcjonalności zwiększające użyteczność programów,

Instalacja najnowszych aktualizacji powinna odbywać się na bieżąco, z chwilą ich pojawienia się. Dzięki temu minimalizujemy ryzyko wykorzystania luki w zabezpieczeniach do ataków hakerskich.

Naruszenia bezpieczeństwa spowodowane brakiem aktualizacji

Urząd Ochrony Danych Osobowych konsekwentnie zwraca uwagę, że regularne aktualizowanie programów antywirusowych, oprogramowania typu firewall, przeglądarek, a także innych aplikacji i całych systemów operacyjnych stanowi nieodzowny element zapewniający bezpieczną pracę i ochronę danych osobowych.

Brak regularnych aktualizacji oprogramowania może prowadzić do poważnych naruszeń bezpieczeństwa danych osobowych.

Dowodzą tego m.in. sprawy prowadzone w UODO. W jednej z nich (DKN.5131.56.2022) przyczyną wystąpienia ataku ransomware było wykorzystanie istniejącej w systemie teleinformatycznym podatności spowodowanej niezaktualizowaniem bazy wirusów programu antywirusowego. W innej (DKN.5112.35.2021) – brak aktualizacji oprogramowania. Kolejne przykłady (DKN.5130.2815.2020, DKN.5131.34.2022) dotyczą naruszeń bezpieczeństwa, do których doszło na skutek korzystania z systemu operacyjnego, który utracił wsparcie producenta.

Regularne testowanie i ocena skuteczności środków bezpieczeństwa

Oprócz samego aktualizowania oprogramowania, równie istotne jest regularne testowanie, mierzenie i ocenianie skuteczności wdrożonych środków technicznych i organizacyjnych. Obowiązek ten wynika bezpośrednio z art. 32 ust. 1 lit. d) RODO i jest podstawowym obowiązkiem każdego administratora oraz podmiotu przetwarzającego.

Administrator zobowiązany jest do weryfikacji zarówno doboru, jak i poziomu skuteczności stosowanych środków technicznych na każdym etapie przetwarzania danych. Kompleksowość tej weryfikacji powinna być oceniana przez pryzmat adekwatności do istniejących ryzyk oraz proporcjonalności w stosunku do aktualnego stanu wiedzy technicznej, kosztów wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania.

Jak wskazał Wojewódzki Sąd Administracyjny w Warszawie w wyroku z 27 lutego 2024 r. (sygn. akt II SA/Wa 1404/23) „wdrożenie przez administratora środków technicznych i organizacyjnych nie jest działaniem jednorazowym, ale powinno przybrać postać procesu, w ramach którego administrator dokonuje przeglądu i w razie potrzeby uaktualnia przyjęte wcześniej zabezpieczenia. Prawodawca unijny nie wskazuje terminu, w jakim powinien zostać przeprowadzony przegląd czy aktualizacja, pozostawiając w tym zakresie swobodę administratorowi, który w razie dostrzeżenia potrzeby powinien dokonać przeglądu i ewentualnego uaktualnienia".

Z kolei Wojewódzki Sąd Administracyjny w Warszawie w wyroku z 10 kwietnia 2025 r. (sygn. akt II SA/Wa 1266/24) podtrzymującym decyzję Prezesa UODO nakładającą na spółkę karę finansową zwrócił uwagę, że na żadnym etapie postępowania, spółka ta „nie twierdziła ani nie wykazywała, że prowadzi regularne testowanie, mierzenie i ocenianie przyjętych środków technicznych i organizacyjnych. Odwoływała się jedynie do przeprowadzonego audytu w związku z przedłużeniem ważności posiadanego przez spółkę certyfikatu ISO/IEC 27001:2013. Organ nie kwestionował, że taki audyt został w spółce przeprowadzony, jednak stał na stanowisku, że jego przeprowadzenie nie może zastąpić realizacji obowiązku regularnego testowania, mierzenia i oceniania wynikającego z art. 32 ust. 1 lit. d) rozporządzenia nr 2016/679. Tę ocenę organu Sąd w całości podziela.

Z akt administracyjnych nie wynika, by spółka tego rodzaju działania regularnie podejmowała, co w konsekwencji doprowadziło, do niezastosowania przez spółkę odpowiednich środków technicznych i organizacyjnych odpowiadających ustalonemu prawidłowo poziomowi ryzyka dla praw i wolności osób fizycznych. Sam fakt zawarcia w dokumentach spółki wskazań co do konieczności prowadzenia regularnych testów nie oznacza, że tego rodzaju testy były prowadzone, a skarżącą takiej okoliczności nie wykazała."

Odpowiedzialność administratora za aktualizację

Pełną odpowiedzialność za zapewnienie odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych ponosi administrator. Zatem to jego obowiązkiem jest regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, w tym aktualizowanie używanego oprogramowania.

W przypadku naruszenia ochrony danych osobowych spowodowanego brakiem aktualności oprogramowania administrator może zostać pociągnięty do odpowiedzialności administracyjnej. Prezes Urzędu Ochrony Danych Osobowych, korzystając ze swoich uprawnień, może m.in. udzielić mu upomnienia lub nałożyć karę pieniężną, której wysokość zależy od wielu czynników, w tym od

charakteru i wagi naruszenia oraz od działań podjętych przez administratora w celu zminimalizowania szkody.

Administrator musi również liczyć się z odpowiedzialnością cywilną. Każdej osobie, która uważa, że naruszone zostały jej określone w RODO prawa, przysługuje bowiem możliwość ich ochrony przed sądem cywilnym. Ma ona także prawo żądać odszkodowania za naruszenie przepisów o ochronie danych osobowych, które spowodowało szkodę majątkową lub niemajątkową.

Potwierdzają to nie tylko wymienione wyżej decyzje Prezesa UODO, na mocy których administratorów ukarano administracyjną karą pieniężną lub upomnieniem, ale również orzecznictwo.

Trybunał Sprawiedliwości Unii Europejskiej w wyroku z 14 grudnia 2023 r. (C-340/21) wskazał, że administrator danych może ponieść odpowiedzialność za szkodę niemajątkową osoby, której dane zostały udostępnione w wyniku ataku hakerskiego. Co istotne, Trybunał uznał, że nawet sama obawa o skutki wycieku danych osobowych może być uznana za szkodę niemajątkową w rozumieniu RODO, co otwiera drogę do dochodzenia roszczeń odszkodowawczych przez osoby, których dane zostały narażone na ryzyko w wyniku zaniedbań administratora.

Praktyczne zalecenia dotyczące aktualizacji oprogramowania i sprzętu

Mając na uwadze obowiązki administratora oraz potencjalne konsekwencje zaniedbań w obszarze aktualizacji oprogramowania, warto przyjąć systematyczne podejście do tego zagadnienia. Przede wszystkim należy regularnie monitorować dostępność aktualizacji dla wszystkich używanych systemów operacyjnych, aplikacji i urządzeń, a także wdrażać je niezwłocznie po ich opublikowaniu przez producenta.

Szczególną uwagę należy zwrócić na aktualizacje dotyczące bezpieczeństwa, które usuwają znane luki w zabezpieczeniach. Producenci oprogramowania regularnie publikują informacje o wykrytych podatnościach oraz wydają odpowiednie poprawki. Dlatego śledzenie tych komunikatów powinno stanowić element procedur bezpieczeństwa w każdej organizacji przetwarzającej dane osobowe.

W przypadku systemów operacyjnych należy również pamiętać o terminach końca wsparcia technicznego. Korzystanie z systemu, który utracił wsparcie producenta, oznacza brak dostępu do krytycznych aktualizacji bezpieczeństwa, co istotnie zwiększa ryzyko naruszenia ochrony danych. W takiej sytuacji administrator powinien rozważyć migrację do nowszych wersji lub wykorzystanie alternatywnych rozwiązań, które nadal otrzymują aktualizacje bezpieczeństwa. Korzystanie z nieaktualnych systemów operacyjnych, po zakończeniu wsparcia technicznego, może zostać uznane za naruszenie art. 32 RODO i skutkować nałożeniem kary administracyjnej przez organ nadzorczy.

Podsumowując, regularne testowanie, mierzenie i ocenianie skuteczności wdrożonych środków bezpieczeństwa oraz regularne aktualizacje oprogramowania i sprzętu stanowią nie tylko dobrą praktykę w zakresie cyberbezpieczeństwa, ale również prawny obowiązek administratora danych wynikający z przepisów RODO. Zaniedbania w tym obszarze mogą prowadzić do poważnych naruszeń bezpieczeństwa danych osobowych, a w konsekwencji skutkować odpowiedzialnością administratora z tego tytułu. Dlatego też systematyczne podejście do aktualizacji powinno stanowić integralny element każdej strategii ochrony danych osobowych.

fot. pixabay

UPOMNIENIE DLA RESTAURACJI ZA UJAWNIENIE DANYCH KLIENTA W FILMIE REKLAMOWYM

Kręcąc filmik promocyjny na TikToka pracownik restauracji nie zauważył, że w kadrze widać terminal płatniczy z danymi klienta. W efekcie jego imię, nazwisko, numer telefonu i dokładny adres dostarczenia zamówienia wraz z kodem pocztowym oraz kodem dostępu do klatki schodowej został publicznie udostępniony.

Prezes UODO po skardze obywatela upomniał restauratora.

Klient zamawiał posiłek w restauracji za pośrednictwem portalu oferującego usługę zamawiania jedzenia online. Do ujawnienia jego danych doszło, jak wyjaśniła restauracja, w wyniku „niedopatrzenia i błędu pracownika, który nagrywał filmik promocyjny i nie zorientował się, iż na terminalu są widoczne dane osobowe; wynikało to prawdopodobnie z faktu, iż dane te są widoczne przez bardzo krótki czas, wręcz ułamek sekundy, a ich użycie i prezentacja nie były w żadnej mierze zamiarem ani celem spółki ani też filmiku promocyjnego”.

Kiedy tylko restauracja dowiedziała się od skarżącego, że ujawniła jego dane, filmik natychmiast usunęła. Podkreśliła, że był to jednorazowy incydent.

Prezes UODO uznał, że incydent ten stanowił naruszenie przepisów RODO. Mając jednak na uwadze, że filmik został niezwłocznie usunięty, a dane osobowe skarżącego nie są już przetwarzane, postępowanie zakończono udzieleniem upomnienia.

Sygnatura sprawy: DS.523.1470.2023

JAK POSTĘPOWAĆ Z NARUSZENIAMI OCHRONY DANYCH OSOBOWYCH? – PODSUMOWANIE EROD

W marcu tego roku Europejska Rada Ochrony Danych (EROD) opublikowała podsumowanie dotychczasowych wytycznych dotyczących naruszeń ochrony danych osobowych. Dokument stanowi kompleksowy przewodnik po najważniejszych zagadnieniach.

Naruszenia ochrony danych osobowych i ich konsekwencje

Zgodnie z RODO, naruszeniem ochrony danych osobowych jest naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do przetwarzanych danych osobowych[1]. Takie zdarzenie może skutkować poważnymi konsekwencjami, takimi jak:

- utrata kontroli nad danymi osobowymi,
- ograniczenie praw,
- dyskryminacja,
- kradzież lub sfałszowanie tożsamości,
- straty finansowe,
- nieuprawnione odwrócenie pseudonimizacji (czyli ponowne ustalenie tożsamości osoby na podstawie danych, które wcześniej zostały w ten sposób zabezpieczone),
- naruszenie dobrego imienia,
- naruszenie poufności danych osobowych chronionych tajemnicą zawodową.

Rodzaje naruszeń ochrony danych osobowych

EROD wyróżnia trzy podstawowe rodzaje naruszeń ochrony danych osobowych:

[1] Więcej na temat definicji „naruszenia ochrony danych osobowych” w Biuletynie UODO nr 1/03/23, str. 27.

• naruszenia poufności – przypadkowe lub bezprawne ujawnienie lub dostęp do danych osobowych;

• naruszenia integralności – przypadkowa lub bezprawna modyfikacja danych osobowych;

• naruszenia dostępności – przypadkowe lub bezprawne utracenie lub zniszczenie danych osobowych[2].

Lepiej zapobiegać, niż leczyć

Zarządzanie bezpieczeństwem przetwarzania zaczyna się od wdrożenia odpowiednich środków technicznych i organizacyjnych. EROD podkreśla, że nawet mimo stosowania zabezpieczeń, w organizacjach nadal może dochodzić do naruszeń ochrony danych osobowych. Ryzyko ich występowania można jednak znacznie ograniczyć, stosując skuteczne działania zapobiegawcze, np.:

• regularne szkolenia personelu z zakresu ochrony danych osobowych,

• korzystanie z aktualnego oprogramowania antywirusowego,

• wdrażanie polityk kontroli dostępu i regularny przegląd przyznawanych dostępów,

• stosowanie uwierzytelniania wieloskładnikowego przy dostępie do wrażliwych[3] danych,

• szyfrowanie dysków,

• regularne tworzenie i testowanie kopii zapasowych,

• automatyczne blokowanie komputerów przy braku aktywności.

Jak reagować na naruszenia ochrony danych osobowych?

Wykrywanie

W przypadku naruszenia ochrony danych osobowych kluczowa jest szybka i skuteczna reakcja. EROD wskazuje, że organizacje powinny dysponować wewnętrznymi mechanizmami wykrywania i reagowania na incydenty, w tym ich właściwej oceny w świetle obowiązków wynikających z RODO. Ważne jest również prawidłowe uregulowanie współpracy z podmiotami przetwarzającymi[4].

---

[2] Więcej na temat rodzajów naruszeń ochrony danych osobowych w Biuletynie UODO nr 3/05/23, str. 25.

[3] „Wrażliwość" to ogólna, opisowa cecha danych osobowych – może być stopniowalna i zależy od kontekstu. EROD posługuje się tym pojęciem (np. w obszarze analizy ryzyka) niezależnie od terminu „szczególnych kategorii danych", odnoszącego się do konkretnego, zamkniętego katalogu określonego w art. 9 RODO.

[4] Więcej na temat roli podmiotu przetwarzającego w przypadku naruszenia ochrony danych osobowych w Biuletynie UODO nr 01/01/24, str. 19.

4 NARUSZENIA I KONTROLE

Dokumentowanie

EROD zaznacza, że każde „stwierdzone" naruszenie ochrony danych osobowych powinno zostać udokumentowane w wewnętrznym rejestrze[5].

Zgłaszanie organowi nadzorczemu

Jeżeli naruszenie ochrony danych osobowych prawdopodobnie wiąże się z ryzykiem dla praw lub wolności osób fizycznych, administrator powinien zgłosić je organowi nadzorczemu w ciągu 72 godzin od jego „stwierdzenia". Zgłoszenie powinno zawierać:

• opis charakteru naruszenia ochrony danych osobowych,

• imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,

• opis możliwych konsekwencji naruszenia ochrony danych osobowych,

• opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków[6].

Jeżeli zgłoszenie następuje po upływie 72 godzin, konieczne jest wyjaśnienie przyczyn opóźnienia.

Zawiadamianie osób, których dane dotyczą

Osoby, których dane dotyczą, muszą zostać zawiadomione o naruszeniu ochrony danych osobowych, jeśli prawdopodobnie wiąże się ono z wysokim ryzykiem dla ich praw lub wolności. Zawiadomienie powinno nastąpić jak najszybciej i zostać dokonane przez bezpieczne kanały komunikacji.

Przykłady EROD

Dokument przedstawia przykładowe scenariusze naruszeń ochrony danych osobowych, a także działań, jakie należy podjąć w ich następstwie. EROD podkreśla jednak, że są to przykłady uproszczone, zachęcając do zapoznania się z pełną wersją wytycznych przed podjęciem decyzji w podobnej sytuacji.

---

[5] Więcej na temat dokumentowania naruszeń ochrony danych osobowych w Biuletynie UODO nr 12_01/12_01/24_25, str. 27.

[6] Więcej na temat informacji, jakie należy zawrzeć w zgłoszeniu, w Biuletynie UODO nr 10/10/23, str. 18.

4 NARUSZENIA I KONTROLE

Przykład 1

Kontekst i cele przetwarzania: Organizacja przechowuje zaszyfrowaną kopię archiwum danych osobowych na pendrive. Nośnik zostaje skradziony podczas włamania.

Jak reagować: Jeśli dane są zaszyfrowane nowoczesnym algorytmem, istnieją kopie zapasowe, a klucz deszyfrujący nie został skompromitowany, zgłoszenie naruszenia ochrony danych osobowych może nie być wymagane. Jeżeli jednak w przyszłości okaże się, że klucz został skompromitowany, zgłoszenie stanie się konieczne. W każdym przypadku naruszenie należy udokumentować.

Przykład 2

Kontekst i cele przetwarzania: Agent ubezpieczeniowy otrzymuje plik Excel, w którym przez błąd konfiguracyjny może zobaczyć dane około dwudziestu osób spoza swojej grupy klientów. Agent, objęty tajemnicą zawodową, jest jedynym odbiorcą wiadomości. Zgodnie z umową, niezwłocznie informuje administratora, który koryguje błąd, przesyła poprawną wersję pliku i prosi o usunięcie pierwotnej wiadomości oraz pisemne potwierdzenie usunięcia, co zostaje wykonane.

Jak reagować: Naruszenie ochrony danych osobowych dotyczy wyłącznie poufności, obejmuje ograniczoną liczbę osób i nie obejmuje danych wrażliwych. Dzięki odpowiedniej reakcji zdarzenie prawdopodobnie nie spowoduje ryzyka dla praw lub wolności osób fizycznych. Zgłoszenie do organu nadzorczego i zawiadomienie osób, których dane dotyczą, nie jest wymagane, ale incydent musi zostać udokumentowany.

Przykład 3

Kontekst i cele przetwarzania: System informatyczny szpitala zostaje zaatakowany przez ransomware, który szyfruje dużą część danych. Zewnętrzna firma specjalizująca się w cyberbezpieczeństwie monitoruje sieć i analizuje logi. Dochodzenie potwierdza brak wycieku danych.

Jak reagować: Pomimo istnienia kopii zapasowych, naruszenie ochrony danych osobowych powoduje znaczące zakłócenia, w tym odwołanie lub opóźnienie zabiegów medycznych i obniżenie jakości usług. Wysokie ryzyko dla praw lub wolności osób fizycznych wymaga zgłoszenia do organu nadzorczego oraz zawiadomienia osób, których dane dotyczą. Dokumentacja incydentu jest obowiązkowa.

4 NARUSZENIA I KONTROLE

Przykład nr 4

Kontekst i cele przetwarzania: Administrator świadczy usługę online, która staje się celem cyberataku. Dochodzi do wycieku danych osobowych użytkowników.

Jak reagować: Zgłoszenie do organu nadzorczego jest wymagane, jeżeli naruszenie ochrony danych osobowych prawdopodobnie wywoła ryzyko dla praw lub wolności osób fizycznych. Obowiązek zawiadomienia użytkowników zależy od kategorii danych i potencjalnej wagi skutków incydentu. Dokumentacja jest obowiązkowa.

Gdzie znaleźć więcej informacji?

Dokument w języku angielskim można pobrać ze strony internetowej EROD.

Zachęcamy także do lektury poradnika Prezesa UODO dotyczącego naruszeń ochrony danych osobowych, dostępnego na stronie internetowej UODO.

fot. publikacja EROD

RAPORT ROCZNY EROD 2024: OCHRONA DANYCH OSOBOWYCH W ZMIENIAJĄCYM SIĘ KRAJOBRAZIE

Europejska Rada Ochrony Danych (EROD) opublikowała sprawozdanie za rok 2024. Zawiera ono przegląd prac EROD przeprowadzonych w 2024 r. i odzwierciedla ważne kamienie milowe, takie jak przyjęcie strategii na lata 2024-2027, wzrost liczby opinii zgodności z art. 64 ust. 2 oraz podjęte wysiłki na rzecz zapewnienia ochrony danych osobowych.

Przewodnicząca EROD Anu Talus powiedziała: „Patrząc wstecz na pracę wykonaną w ciągu ostatniego roku, z dumą prezentuję nasze osiągnięcia. W 2024 r. potwierdziliśmy nasze zaangażowanie w ochronę podstawowych praw osób fizycznych do prywatności i ochrony danych w szybko zmieniającym się krajobrazie cyfrowym.

Przyjęliśmy nową strategię i nadal odgrywaliśmy kluczową rolę w dostarczaniu wskazówek i zapewnianiu spójnego stosowania ogólnego rozporządzenia o ochronie danych (RODO) w całej Europie. Aby pomóc w zrozumieniu i wdrożeniu praw i obowiązków w zakresie ochrony danych, rozszerzyliśmy nasze działania informacyjne, poświęcając szczególną uwagę firmom i osobom niebędącym ekspertami. Ponadto przejęliśmy kolejne role w ramach nowych przepisów cyfrowych”.

Nowa strategia EROD

Strategia EROD na lata 2024-2027 określa kluczowe priorytety i działania mające na celu wzmocnienie i modernizację ochrony danych w całej Europie, zapewnienie spójnego egzekwowania RODO oraz sprostanie pojawiającym się wyzwaniom, w tym współpracy międzyregionalnej. Strategia pomaga również wzmocnić globalną obecność EROD poprzez współpracę z globalnymi partnerami i reprezentowanie unijnego modelu ochrony danych na kluczowych forach międzynarodowych.

Główna rola EROD w zapewnianiu wytycznych i porad prawnych

Liczba spójnych opinii przyjętych na podstawie art. 64 ust. 2 RODO znacznie wzrosła. W 2024 r. Rada przyjęła osiem opinii na jego podstawie, w tym w sprawie modeli „Zgoda lub zapłata” stosowanych przez duże platformy internetowe, rozpoznawania twarzy na lotniskach oraz wykorzystywania danych osobowych do szkolenia modeli sztucznej inteligencji. Opinie te dotyczą kwestii ogólnego zastosowania i zapewniają spójność przed egzekwowaniem przepisów.

5 SPRAWY MIĘDZYNARODOWE

EROD aktywnie uczestniczyła w dyskusjach legislacyjnych, wydając oświadczenia podkreślające kwestie i skutki związane z ochroną danych. Przyjęła m.in. oświadczenia w sprawie projektu rozporządzenia proceduralnego dotyczącego egzekwowania RODO oraz w sprawie roli organów ochrony danych w ramach ustawy o sztucznej inteligencji.

EROD rozszerzyła również swoje ogólne wytyczne, aby pomóc organizacjom w osiągnięciu i utrzymaniu zgodności z RODO. W tym celu w 2024 r. Rada przyjęła cztery nowe wytyczne, takie jak wytyczne dotyczące uzasadnionego interesu i przekazywania danych organom państw trzecich.

Proaktywne zaangażowanie interesariuszy

W 2024 r. EROD kontynuowała współpracę z zainteresowanymi stronami w celu wspierania otwartego dialogu i wzajemnego zrozumienia między organami regulacyjnymi, przedstawicielami branży, organizacjami społeczeństwa obywatelskiego i instytucjami akademickimi. Aby zebrać istotne spostrzeżenia od organizacji posiadających fachową wiedzę na tematy związane z ochroną danych, Rada rozpoczęła konsultacje publiczne w sprawie przyjętych wytycznych i zorganizowała dwa wydarzenia dla zainteresowanych stron, związane z nadchodzącymi wytycznymi w sprawie modeli „Zgoda lub zapłata” oraz z przygotowaniem opinii w sprawie modeli sztucznej inteligencji.

Wkład we współpracę między organami regulacyjnymi

Nowe przepisy cyfrowe, w tym ustawa o rynkach cyfrowych (DMA), ustawa o usługach cyfrowych (DSA), ustawa o sztucznej inteligencji, ustawa o zarządzaniu danymi (DGA) i ustawa o danych, opierają się na RODO. Aby zapewnić spójność stosowania RODO i tych aktów, EROD aktywnie przyczyniła się do współpracy międzyregulacyjnej, angażując się we współpracę z partnerami europejskimi i międzynarodowymi, w tym z Urzędem UE ds. Sztucznej Inteligencji i grupą wysokiego szczebla ds. aktu o rynkach cyfrowych.

Uczynienie RODO zrozumiałym i praktycznym dla wszystkich

Ponadto EROD kontynuowała swoje wysiłki w celu dostarczenia informacji na temat RODO szerszemu gronu odbiorców niebędących ekspertami poprzez przedstawienie ich w jasnym i nietechnicznym języku. W tym celu Rada udostępniła Przewodnik ochrony danych dla małych przedsiębiorstw w 18 językach. Uruchomiła również serię streszczeń wytycznych EROD, aby pomóc osobom i organizacjom niebędącym ekspertami w łatwiejszym zidentyfikowaniu najważniejszych punktów do rozważenia.

Źródło: Komunikat Europejskiej Rady Ochrony Danych

CNIL ROZPOCZYNA PROCES KONSULTACJI WS. KAMER „ROZSZERZONYCH" DO SPRAWDZANIA WIEKU W PUNKCIE SPRZEDAŻY

Niektóre sklepy tytoniowe we Francji wdrożyły kamery oparte na sztucznej inteligencji, aby oszacować wiek klientów i zapobiec sprzedaży produktów zabronionych nieletnim. W celu przeanalizowania zgodności tych systemów, które mają znaczący wpływ na prawa i wolności, francuski organ ochrony danych (CNIL) organizuje prace w porozumieniu z zaangażowanymi podmiotami.

Pogodzenie ochrony małoletnich z zachowaniem praw i wolności

Część punktów sprzedaży we Francji wykorzystuje „rozszerzone" systemy kamer, aby zapobiec sprzedaży produktów zabronionych nieletnim (tytoń, alkohol itp.), w oparciu o algorytm sztucznej inteligencji. W praktyce, w momencie zakupu, kamery te skanują twarz osoby w celu ustalenia, czy jest ona niepełnoletnia czy dorosła i informują o tym sprzedawcę za pomocą wskaźnika świetlnego (np. zielonego lub czerwonego światła).

Korzystanie z tych urządzeń ma podwójny cel w interesie publicznym: ochronę młodych ludzi i ochronę zdrowia publicznego.

Nie bez znaczenia jest jednak fakt, że weryfikacja ta odbywa się za pomocą zautomatyzowanego algorytmu przetwarzania obrazu, co może wiązać się z ryzykiem naruszenia ochrony danych osobowych i prywatności osób fizycznych.

Z tego powodu CNIL chce przeanalizować zgodność tych urządzeń z obowiązującymi przepisami dotyczącymi ochrony danych osobowych (RODO oraz francuską ustawą o ochronie danych).

Podejście to stanowi kontynuację wcześniejszych prac nad wdrażaniem „rozszerzonych" kamer w przestrzeni publicznej i nad weryfikacją wieku online.

Aby zbadać zgodność tych systemów w sposób możliwie najbardziej kompleksowy, CNIL zorganizuje szereg spotkań konsultacyjnych, w których wezmą udział zainteresowane strony lub podmioty mogące dostarczyć przydatnych informacji na potrzeby tej pracy, w szczególności:

• producenci urządzeń weryfikujących wiek;

• organizacje podlegające obowiązkom związanym z zakazem sprzedaży produktów niedozwolonych osobom nieletnim;

• organizacje zajmujące się ochroną nieletnich i zdrowiem publicznym;

• organizacje zrzeszające osoby zajmujące się ochroną konsumentów oraz praw i wolności cyfrowych.

CNIL opublikuje wnioski ze swoich prac na swojej stronie internetowej do lata 2025 r.

Źródło: Komunikat francuskiego organu nadzorczego

fot. pixabay

KONTROLE CNIL W 2025 R.: APLIKACJE MOBILNE, ADMINISTRACJA WIĘZIENNA, CYBERBEZPIECZEŃSTWO

W 2025 r. francuski organ ochrony danych (CNIL) podczas swoich kontroli skupi się na danych gromadzonych za pośrednictwem aplikacji mobilnych, cyberbezpieczeństwie władz lokalnych i przetwarzaniu danych przez administrację więzienną.

Zbieranie danych za pomocą aplikacji mobilnych

Francuzi pobierają obecnie około trzydziestu aplikacji mobilnych rocznie. Stały się one najważniejszym cyfrowym narzędziem w codziennym życiu i są źródłem masowego przetwarzania danych osobowych (bankowość, geolokalizacja, reklama itp.).

Po opublikowaniu w październiku ubiegłego roku zalecenia w sprawie aplikacji mobilnych, CNIL przeprowadzi w tym roku serię kontroli różnych podmiotów w ekosystemie, w szczególności wydawców aplikacji i dostawców zestawów do tworzenia oprogramowania.

Audyty będą koncentrować się przede wszystkim na kwestiach uwzględnionych w rekomendacjach, w tym na konfiguracji zestawów do tworzenia oprogramowania i dostępie do danych telefonu poprzez zarządzanie uprawnieniami.

Kontrole te będą dotyczyć zarówno podmiotów prywatnych, jak i publicznych, zwłaszcza w obliczu rosnącej liczby usług publicznych oferujących aplikację mobilną do codziennych zadań administracyjnych.

Cyberbezpieczeństwo władz lokalnych

Cyberbezpieczeństwo jest jednym z głównych priorytetów planu strategicznego CNIL na lata 2025-2028. W ciągu ostatnich kilku lat doszło do szeregu cyberataków obejmujących dużą część populacji. W 2024 r. CNIL otrzymała 5 629 powiadomień o naruszeniach, o 20% więcej niż w 2023 r. Biorąc pod uwagę ryzyko kradzieży danych osobowych, w szczególności danych bankowych lub zdrowotnych, cyberbezpieczeństwo stanowi prawdziwe wyzwanie dla społeczeństwa.

Wśród zainteresowanych podmiotów szczególnie narażone są władze lokalne. Przetwarzają one duże ilości danych, z których część jest wrażliwa (zarządzanie stanem cywilnym użytkowników, wypłata świadczeń socjalnych, dane finansowe lub usługi online do płacenia mandatów za parkowanie).

CNIL postanowiła zatem monitorować środki wdrażane przez władze lokalne w celu ochrony danych użytkowników. Oprócz tych kontroli CNIL będzie nadal zwiększać wysiłki na rzecz podnoszenia świadomości i zapewniania wsparcia władzom lokalnym w zakresie cyberbezpieczeństwa.

Poprzez te dwa działania CNIL pragnie również przygotować się do stosowania dyrektywy NIS2, która jest obecnie transponowana, a która przewiduje wzrost umiejętności i nowe wymagania dla władz lokalnych w zakresie bezpieczeństwa IT.

Dane przetwarzane przez administrację więzienną

Zgodnie z danymi Ministerstwa Sprawiedliwości, 77 800 osób przebywa obecnie w zakładach karnych we Francji. Wszystkie informacje dotyczące osób podlegających środkom ograniczającym lub pozbawienia wolności są rejestrowane w skomputeryzowanej bazie danych „Gestion nationale des personnes écrouées pour le suivi individualisé et la sécurité" („GENESIS"). Zawiera ona szczególnie wrażliwe informacje związane z zarządzaniem życiem w areszcie i reintegracją tych osób.

Ponadto zakłady karne muszą dołożyć większych starań, aby zapewnić bezpieczeństwo swoich instalacji informatycznych i wykorzystywanych w nich środków komunikacji.

Podczas swoich kontroli CNIL sprawdzi warunki, w jakich przetwarzane są dane więźniów, a także wszystkie środki bezpieczeństwa wprowadzone przez zakłady karne.

Prawo do usunięcia danych

W ramach czwartego działania skoordynowanych ram egzekwowania prawa CNIL i jego europejskie odpowiedniki będą przeprowadzać kontrole warunków wdrażania prawa do usunięcia danych. Celem tego działania jest harmonizacja skutecznego stosowania RODO i koordynacja między organami nadzorczymi.

Źródło: Komunikat francuskiego organu nadzorczego

IRLANDZKI ORGAN OCHRONY DANYCH NAŁOŻYŁ NA TIKTOKA KARĘ W WYSOKOŚCI 530 MILIONÓW EURO I NAKAZAŁ PODJĘCIE ŚRODKÓW NAPRAWCZYCH W NASTĘPSTWIE DOCHODZENIA W SPRAWIE PRZEKAZYWANIA DANYCH UŻYTKOWNIKÓW Z EOG DO CHIN

Irlandzki Organ Ochrony Danych (DPC) ogłosił swoją ostateczną decyzję w następstwie dochodzenia w sprawie TikTok Technology Limited. Dochodzenie zostało wszczęte przez DPC, wiodący organ nadzorczy dla TikToka, w celu zbadania zgodności z prawem przekazywania przez platformę danych osobowych jej użytkowników w EOG do Chińskiej Republiki Ludowej. Ponadto w dochodzeniu zbadano, czy przekazywanie informacji użytkownikom w związku z takimi transferami spełniało wymogi przejrzystości TikToka zgodnie z wymogami RODO.

Decyzja, która została podjęta przez komisarzy ds. ochrony danych, dr Desa Hogana i Dale'a Sunderlanda, o której powiadomiono TikToka, stwierdza, że naruszył RODO w zakresie przekazywania danych użytkowników z EOG do Chin oraz wymogi dotyczące przejrzystości.

Decyzja obejmuje:

• kary administracyjne w łącznej wysokości 530 milionów euro,

• nakaz zobowiązujący TikToka do zapewnienia zgodności przetwarzania danych w ciągu 6 miesięcy,

• nakaz zawieszenia transferów danych do Chin, jeśli przetwarzanie nie zostanie dostosowane w tym terminie.

Zastępca komisarza DPC Graham Doyle skomentował:

„RODO wymaga, aby wysoki poziom ochrony zapewniany w Unii Europejskiej był kontynuowany w przypadku, gdy dane osobowe są przekazywane do innych krajów.

Przekazywanie danych osobowych przez TikToka do Chin naruszyło RODO, ponieważ nie zweryfikował, nie zagwarantował i nie wykazał, że dane osobowe użytkowników z EOG, do których zdalny dostęp

mieli pracownicy w Chinach, były objęte poziomem ochrony zasadniczo równoważnym z poziomem gwarantowanym w UE.

W wyniku niepodjęcia przez TikToka niezbędnych ocen, nie zajął się potencjalnym dostępem chińskich władz do danych osobowych EOG na mocy chińskich przepisów antyterrorystycznych, kontrwywiadowczych i innych przepisów zidentyfikowanych przez TikToka jako istotnie odbiegające od standardów UE".

W dniu 21 lutego 2025 r. DPC przedłożył projekt decyzji w ramach mechanizmu współpracy RODO, zgodnie z wymogami art. 60 RODO. Nie zgłoszono żadnych zastrzeżeń do projektu decyzji DPC. Organ irlandzki jest wdzięczny za współpracę i pomoc w tej sprawie ze strony innych organów nadzorczych UE/EOG.

Błędne informacje przekazane w toku dochodzenia

W trakcie dochodzenia TikTok informował DPC, że nie przechowuje danych użytkowników z EOG na serwerach zlokalizowanych w Chinach. Jednak w kwietniu 2025 r. poinformował DPC o problemie, który odkrył w lutym 2025 r., w którym ograniczone dane użytkowników z EOG były w rzeczywistości przechowywane na serwerach w Chinach, wbrew dowodom złożonym w dochodzeniu. TikTok poinformował DPC, że odkrycie to oznaczało, że przedstawił w dochodzeniu niedokładne informacje.

Zastępca komisarza Doyle dodał, że:

„DPC bardzo poważnie traktuje ostatnie wydarzenia dotyczące przechowywania danych użytkowników z EOG na serwerach w Chinach. Chociaż TikTok poinformował DPC, że dane zostały już usunięte, rozważamy, jakie dalsze działania regulacyjne mogą być uzasadnione, w porozumieniu z naszymi równorzędnymi organami ochrony danych w UE".

Organ irlandzki opublikuje pełną decyzję i dalsze powiązane informacje w odpowiednim czasie.

Źródło: Komunikat irlandzkiego organu nadzorczego

UODO BIERZE UDZIAŁ W KONKURSIE KE, ISTOTNYM DLA SZCZEGÓLNEJ OCHRONY DANYCH OSOBOWYCH DZIECI

W kwietniu 2025 r. UODO złożył wniosek o dofinansowanie projektu Safe DigitAl Environment For ChildrEn – awareness campaign – SAFE, dotyczącego przeprowadzenia kampanii edukacyjnej w zakresie podnoszenia świadomości na temat bezpiecznego środowiska cyfrowego dla dzieci.

UODO przygotował wniosek w odpowiedzi na nabór „Rights of the child and children's participation CERV-2025-CHILD" prowadzony przez Komisję Europejską w ramach programu Citizens, Equality, Rights and Values Programme (CERV). Projekt powstał, by wspierać, promować i wdrażać kompleksowe polityki mające na celu ochronę praw dzieci, w tym prawa do uczestnictwa, a także zapewnienie dzieciom bezpiecznego środowiska cyfrowego.

W związku z wytycznymi Strategii UE w zakresie praw dziecka, Europejskiej strategii na rzecz lepszego internetu dla dzieci (BIK+), wymaganiami szczególnej ochrony danych osobowych dzieci wskazanymi w Ogólnym rozporządzeniu o ochronie danych (RODO), a także obowiązkami, jakie nakłada Akt o usługach cyfrowych (DSA) w kontekście ochrony małoletnich w internecie, w ramach projektu UODO zaplanował kampanię edukacyjną skierowaną do dzieci, rodziców, opiekunów i nauczycieli na temat m.in. bezpieczeństwa online i praw cyfrowych. Opracowane materiały edukacyjne zostaną zamieszczone na stronie internetowej projektu.

Chcemy zwiększyć świadomość nt. praw dzieci na kierunkach ICT

Projekt obejmuje również działania prowadzące do zwiększenia świadomości, a także integracji praw dzieci i prawodawstwa cyfrowego UE w ramach edukacji na kierunkach ICT (technologii informacyjnych i komunikacyjnych).

Planowane jest przeprowadzenie ankiety skierowanej do studentów i profesorów ICT, która oceni ich świadomość i postrzeganie praw dzieci w przestrzeni cyfrowej. Przeprowadzona zostanie analiza programów nauczania na kierunkach technologii informacyjnych i komunikacyjnych, która pozwoli ocenić, w jakim stopniu obecne programy szkoleniowe uwzględniają standardy UE, wskazane w RODO czy DSA. W oparciu o te spostrzeżenia, konsorcjum wspólnie opracuje podręcznik dla przyszłych specjalistów ICT, oferujący wskazówki dla uczelni technicznych, w jaki sposób włączyć

prawa dziecka i zobowiązania prawne UE w obszarze ochrony danych osobowych, do programów nauczania.

Dodatkowo, planowane jest podjęcie działań w porozumieniu z Rzecznikiem Praw Dziecka i Parlamentarną Komisją Do Spraw Dzieci i Młodzieży (DIM) w celu zapewnienia, że potrzeby dzieci są traktowane priorytetowo w polityce cyfrowej. Projekt zakończy międzynarodowa konferencja, na której podsumowane zostaną podjęte w ramach projektu działania. Konsorcjum zaprezentuje wyniki i wnioski z przeprowadzonych badań. Konferencja będzie pewnego rodzaju forum dyskusyjnym dla sektora ICT na temat potrzeby stworzenia bezpiecznego środowiska cyfrowego dla dzieci.

W przypadku pozytywnej oceny wniosku, UODO będzie mógł rozpocząć projekt na początku 2026 r. Partnerami projektu są: bułgarski organ ochrony danych (CPDP) oraz Vrije Universiteit Brussel (VUB). Inicjatywę poparł francuski organ ochrony danych (CNIL), który zadeklarował wsparcie UODO na etapie wdrażania projektu.

Projekt wpisuje się w kierunek działań UODO obejmujący ochronę danych osobowych dzieci, które Urząd realizuje również m.in. we współpracy z Rzeczniczką Praw Dziecka czy sejmową Komisją do Spraw Dzieci i Młodzieży.

Jednocześnie zgodnie z planem kontroli sektorowych na 2025 rok, Urząd rozpoczął kontrolę podmiotów / administratorów przetwarzających dane osobowe dzieci.

fot.pixabay

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl