NR 1 - STYCZEŃ-LUTY 2022

NEWSLETTER RODO

W numerze m.in.:

- Nowe standardowe klauzule umowne jako mechanizm transferu danych do państwa trzeciego
- Profilowanie do kontroli UODO
- Ochrona danych osobowych osób pełniących funkcje publiczne
- Ochrona danych a ustawa o sygnalistach
- Odpłatny, prawnie uzasadniony interes administratora danych
- Ponowne wykorzystanie powierzonych danych
- Wyroki niemieckich sądów dotyczące plików cookie

Traple Konarski Podrecki & Wspólnicy

TKP

Profilowanie w planie kontroli sektorowych Prezesa UODO w 2022 r.

Katarzyna Syska

Prezes Urzędu Ochrony Danych Osobowych (UODO) opublikował plan kontroli sektorowych na 2022 r. Z planu wynika, że UODO skupi się m.in. na **przeprowadzaniu kontroli w bankach w zakresie profilowania danych osobowych klientów i potencjalnych klientów oraz sprawdzi sposoby informowania osób ubiegających się o kredyt o dokonanej ocenie kredytowej w związku z art. 70a ustawy Prawo bankowe**[1].

Ponadto Prezes UODO zapowiedział kontrole podmiotów przetwarzających dane osobowe przy użyciu aplikacji mobilnych – kontrole miałyby dotyczyć sposobów zabezpieczenia i udostępniania danych osobowych przetwarzanych w związku z użytkowaniem tych aplikacji.

Profilowanie danych osobowych przez banki

W komunikacie Prezesa UODO mowa jest o art. 70a Prawa bankowego. Zgodnie z tym przepisem banki i inne instytucje udzielające kredytów lub pożyczek mają obowiązek – na wniosek wnioskującego – przekazać mu wyjaśnienie dotyczące dokonanej oceny jego zdolności kredytowej. Wyjaśnienie takie powinno obejmować informacje na temat czynników (w tym danych osobowych wnioskującego), które miały wpływ na dokonaną ocenę zdolności kredytowej.

Kwestia profilowania jest uregulowana także w art. 105a ust. 1a Prawa bankowego. Zgodnie z tym przepisem banki (oraz inne instytucje udzielające kredytów lub pożyczek) mogą w celu oceny zdolności kredytowej i analizy ryzyka kredytowego podejmować decyzje w sposób całkowicie zautomatyzowany, w tym dokonywać profilowania danych osobowych. Warunkiem takiego przetwarzania danych jest zapewnienie osobie, której dotyczy decyzja podejmowana w sposób zautomatyzowany, prawa do: otrzymania stosownych wyjaśnień co do podstaw podjętej decyzji, uzyskania interwencji ludzkiej w celu podjęcia ponownej decyzji oraz wyrażenia własnego stanowiska.

Ponadto w art. 105a ust. 1b Prawa bankowego wskazany jest przykładowy (otwarty) katalog danych, które banki mogą przetwarzać w celu oceny zdolności kredytowej i analizy ryzyka kredytowego. Wśród tych danych znajdują się m.in.: adres zamieszkania, miejsce pracy, sytuacja finansowa, w tym dochody i wydatki, osoby pozostające na utrzymaniu, a także szczegółowe informacje dotyczące zobowiązania, w tym przebieg realizacji zobowiązania, stan zadłużenia oraz przyczyny ewentualnego niewykonania zobowiązania.

W tym kontekście należy pamiętać, że informacje o profilowaniu oraz zautomatyzowanym podejmowaniu decyzji powinny się znaleźć w klauzuli informacyjnej. Zgodnie z art. 13 ust. 2 lit. f oraz art. 14 ust. 2 lit. g RODO[2] podmiotowi danych należy przekazać informacje o fakcie zautomatyzowanego podejmowania decyzji (w tym o profilowaniu) oraz zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania (podejmowania zautomatyzowanych decyzji) dla podmiotu danych. Jak wynika z motywu 60 RODO, w przypadku profilowania należy poinformować podmiot danych o profilowaniu oraz jego konsekwencjach.

Przedmiotem kontroli UODO mogą więc być wszystkie powyższe kwestie.

[1] Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2021 r., poz. 2439)

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)..

Jak się przygotować na ewentualną kontrolę UODO?

W związku z zapowiedzią kontroli przetwarzania danych w zakresie profilowania i informowania o ocenie zdolności kredytowej z pewnością warto się przygotować na ewentualną weryfikację ze strony UODO.

W tym celu można przeprowadzić ograniczony audyt zgodności przetwarzania danych z wymogami prawnymi dotyczącymi profilowania, zautomatyzowanego podejmowania decyzji oraz informowania osób, których dane dotyczą, o przetwarzaniu ich danych osobowych oraz o wyniku oceny ich zdolności kredytowej.

Warto sprawdzić m.in.:

- podstawę prawną przetwarzania danych osobowych klientów lub potencjalnych klientów, w tym profilowania, w związku z oceną zdolności kredytowej;
- podstawę prawną zautomatyzowanego podejmowania decyzji – o ile występuje;
- treść klauzuli informacyjnej dla klientów i potencjalnych klientów – w szczególności czy prawidłowo wskazane są cele przetwarzania, informacje o profilowaniu i jego konsekwencjach, informacje o zautomatyzowanym podejmowaniu decyzji (w tym o zasadach ich podejmowania, ich znaczeniu i przewidywanych konsekwencjach), informacje o uprawnieniach związanych ze zautomatyzowanym podejmowaniem decyzji;
- realizację zasady minimalizacji danych, w tym czy do profilowania używane są tylko dane niezbędne do dokonania oceny zdolności kredytowej, a jeśli do profilowania wykorzystywane są dane spoza katalogu określonego w art. 105a ust. 1b Prawa bankowego, to czy jest to uzasadnione;
- sposób realizacji uprawnienia do otrzymania wyjaśnienia dotyczącego dokonanej oceny zdolności kredytowej, o którym mowa w art. 70a Prawa bankowego, w tym czy określono wzory taki wyjaśnień, czy istnieje wewnętrzna procedura realizacji tego uprawnienia, czy dotychczasowa realizacja tego uprawnienia była prawidłowa i czy nie było skarg ze strony osób, które z niego korzystały;
- sposób realizacji uprawnień związanych ze zautomatyzowanym podejmowaniem decyzji, tj. prawa do: otrzymania stosownych wyjaśnień co do podstaw podjętej decyzji, uzyskania interwencji ludzkiej w celu podjęcia ponownej decyzji oraz wyrażenia własnego stanowiska.

Nowe standardowe klauzule umowne jako mechanizm transferu danych do państwa trzeciego

Xawery Konarski

Jak wykazuje praktyka obrotu, podstawą prawną **ponad 90% transferów danych osobowych do państw trzecich (poza Europejski Obszar Gospodarczy) są tzw. standardowe klauzule umowne**.

Nowe standardowe klauzule - kalendarium

Decyzją Komisji Europejskiej nr 2021/914/UE zostały przyjęte nowe klauzule („Nowe SKU"), które z dniem 27 września 2021 r. zastąpiły dotychczasowe klauzule, zatwierdzone decyzją 2001/497/WE (i stanowiąca jej wariant decyzja nr 2004/915/WE) oraz decyzją 2010/87/UE.

Zgodnie z art. 4 ust.4 decyzji nr 2021/914/UE uznaje się, że umowy transferowe zawarte przed dniem 27 września 2021 r. na podstawie decyzji 2001/497/WE lub decyzji 2010/87/UE zapewniają odpowiednie gwarancje w rozumieniu art. 46 ust. 1 rozporządzenia (UE) 2016/679 do dnia 27 grudnia 2022 r., pod warunkiem że:

1. operacje przetwarzania stanowiące przedmiot umowy pozostaną niezmienione oraz,
2. stosowanie tych klauzul zapewnia, aby przekazywanie danych osobowych odbywało się z zastrzeżeniem odpowiednich zabezpieczeń.

Mimo, że w stosunku do umów transferowych zawartych przed 27.09.2021 r. obowiązuję okres przejściowy do dnia 27.12.2022 r., to sposób sformułowania powyższych warunków powoduję, że **w praktyce wcześniej konieczne będzie zastąpienie „starych" SKU „nowymi" SKU** (np. w sytuacji, gdy transferem zostaną objęte nowe dane). Będzie tak również dlatego, że sposób sformułowania wymogów w nowych klauzulach powoduje, że dotychczasowe umowy transferowe często nie będą spełniały wymogu „odpowiednich zabezpieczeń" w rozumieniu art.4 ust.4 decyzji nr 2021/914/UE.

Nowe SKU – najważniejsze zmiany w stosunku do dotychczasowych klauzul umownych

Do najważniejszych zmian wprowadzonych w nowych SKU zaliczyć należy:

1. nowymi SKU objętych jest więcej niż obecnie rodzajów transferów danych osobowych do państw trzecich (np. transfer pomiędzy procesorem i podprocesorem z państwa trzeciego, procesorem z EOG i administratorem z państwa trzeciego),
2. nowe SKU zawierają znacznie więcej postanowień niż stare SKU (podział na wspólne klauzule ogólne oraz klauzule szczegółowe w poszczególnych modułach),
3. stronami nowych SKU mogą być więcej niż dwa podmioty (zob. klauzula przystąpienia – nr 7),
4. nowe SKU zawierają elementy umowy powierzenia danych, określone w art.28 ust.3 i 4 RODO, brak jest więc konieczności zawierania odrębnych umów w tym zakresie,
5. odpowiedzialność za naruszenie ochrony danych osobowych, uregulowana jest zarówno w relacji pomiędzy stronami SKU, jak i w stosunku do podmiotów danych,
6. w klauzulach określona została nieograniczona odpowiedzialność eksportera danych za importera danych (zakres odpowiedzialności jest więc szerszy niż w przypadku odpowiedzialności administratora za procesora na gruncie RODO),
7. importer danych, a więc odbiorca danych w państwie trzecim stał się adresatem szeregu bezpośrednich obowiązków,
8. nowe SKU wprowadzają szczególne postanowienia ograniczające dostęp organów z państw trzecich do przekazywanych danych osobowych („defend-your-data"),
9. zwiększono uprawnienia organów nadzorczych odnośnie możliwości żądania dokumentów i informacji od eksportera i importera danych,
10. katalog środków technicznych i organizacyjnych został rozbudowany w stosunku do starych SKU (dotychczasowe środki mogą się okazać niewystarczające), ma to znaczenie między innymi przy dokonywaniu Transfer Impact Assesment (TIA), który to wymóg nadal obowiązuję również przy stosowaniu nowych klauzul.

Implementacja nowych SKU do umów handlowych

W praktyce spotyka się dwa warianty (sposoby) implementacji nowych SKU do umów handlowych:

- I wariant - wyselekcjonowanie postanowień ze SKU (klauzule ogólne, klauzule szczegółowe w poszczególnych modułach określonych w SKU) do nowej umowy handlowej),
- II wariant - do umowy handlowej dołączone są kompletne SKU, a w tzw. cover sheet wskazane jest które moduły stosują się do danych relacji pomiędzy stronami (np. w przypadku outsourcingu przetwarzania danych przez podmiot/eksportera danych z EOG: moduł nr 2 – powierzenie danych podmiotowi w państwie trzecim).

Mimo, że w niektórych postanowieniach (np. klauzula nr 7) mowa jest o „podpisaniu", w analizach dotyczących nowych SKU podkreśla się możliwość ich zawarcia w postaci elektronicznej (np. systemy podpisów typu "DocuSign" or "Adobe Sign„).

Ochrona danych osobowych osób pełniących funkcje publiczne Wyrok NSA z dnia 18 listopada 2021 r., III OSK 4193/21

Grzegorz Sibiga

W wyroku Naczelnego Sadu Administracyjnego (NSA) z dnia 18 listopada 2021 r. (III OSK 4193/21) stwierdzono, że ustawa o dostępie do informacji publicznej[1] wymaga udostępnienia danych osobowych (imion i nazwisk) uczestników postępowania w sprawach o naruszenie dyscypliny finansów publicznych (obwinionego i świadków), ponieważ są to osoby pełniące funkcje publiczne, a informacje w tym zakresie są związane z pełnioną funkcją. Wykładnia przepisów dostępowych – zdaniem sądu - ma sprzyjać sprawowaniu społecznej kontroli przez wszystkich obywateli. Natomiast RODO nie modyfikuje warunków ustanowionych w tej ustawie w sprawach wnioskowych o udostępnienie informacji publicznych będących danymi osobowymi.

Stan w sprawie

We wniosku do Międzyresortowej Komisji Orzekającej w Sprawach o Naruszenie Dyscypliny Finansów Publicznych (przy ministrze właściwym do spraw administracji publicznej) (MKO) zwrócono się m.in. o udostępnienie kopii orzeczenia tego organu kończącego postępowanie w I instancji w określonej przez wnioskodawcę sprawie. W odpowiedzi MKO przekazał zanonimizowany dokument – wnioskowane orzeczenie wraz z uzasadnieniem. W szczególności zanonimizowano dane obwinionego (jak się później okazało Dyrektora Narodowego Centrum Badań i Rozwoju) oraz osób zeznających w charakterze świadków (Zastępcy Dyrektora Narodowego Centrum Badań i Rozwoju oraz Dyrektora Działu Kontroli Projektów tej jednostki).

W wyniku wniesienia skargi na bezczynność MKO w wyroku Wojewódzki Sąd Administracyjny (WSA) w Warszawie uznano, że organ dopuścił się bezczynności i zobowiązano MKO do rozpatrzenia wniosku. Z kolei NSA w przedstawianym wyroku oddalił skargę kasacyjną MKO.

Znaczenie art. 86 RODO

W tej sprawie już WSA ustalił zakres stosowania RODO w sprawach wnioskowych o udostępnianie informacji publicznej stanowiących dane osobowe. Sąd powołał się na art. 86 RODO, zgodnie z którym dane osobowe zawarte w dokumentach urzędowych, które posiada organ lub podmiot publiczny lub podmiot prywatny w celu wykonania zadania realizowanego w interesie publicznym, mogą zostać przez ten organ lub podmiot ujawnione zgodnie z prawem Unii lub prawem państwa członkowskiego, któremu podlegają ten organ lub podmiot, dla pogodzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych na mocy RODO. Według sądu przepisy RODO nie formułują więc zakazu udostępniania danych osobowych znajdujących się w dokumentach publicznych, lecz mówią o konieczności pogodzenia dwóch wartości, tj. jawności życia publicznego i prawa do prywatności. Zdaniem sądu na gruncie polskiego ustawodawstwa kolizję tych dwóch interesów rozstrzyga art. 5 ust. 2 ustawy o dostępie do informacji publicznej.

[1] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2020 r. poz. 2176).

Funkcja publiczna - dane związane z pełnioną funkcją

Rozstrzygające znaczenie dla określania zakresu dostępności danych osobowych ma zatemart. 5 ust. 2 ustawy o dostępie do informacji publicznej. Zgodnie z tym przepisem 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 i mających związek z pełnieniem tych funkcji. Ustawa wprowadza więc zasadę, że nie jest chroniona prywatność osoby pełniącej funkcję publiczną (w tym jej dane osobowe), w sytuacji gdy żądane informacje mają związek z pełnioną przez nią funkcją.

Według NSA osoba, która została ukarana za naruszanie dyscypliny finansów publicznych jest osobą pełniącą funkcję publiczną, ponieważ odpowiedzialność za naruszenie dyscypliny finansów publicznych nie może być ponoszona przez każdego obywatela, ale wyłącznie przez osoby gospodarujące środkami publicznym. Oznacza to, że osoby, które podlegają odpowiedzialności z ustawy o odpowiedzialności za naruszenie dyscypliny finansów publicznych[2] spełniają podstawową przesłankę uznania ich za „osoby pełniące funkcje publiczne" w postaci związku sprawowanej funkcji z dysponowaniem majątkiem publicznym.

W wyroku NSA przychylił się do szerokiego rozumienia zwrotu „osoba pełniąca funkcje publiczne", w którym obejmuje on każdą osobę, która ma wpływ na kształtowanie spraw publicznych w rozumieniu art. 1 ust. 1 ustawy o dostępie do informacji publicznej, tj. na sferę publiczną.

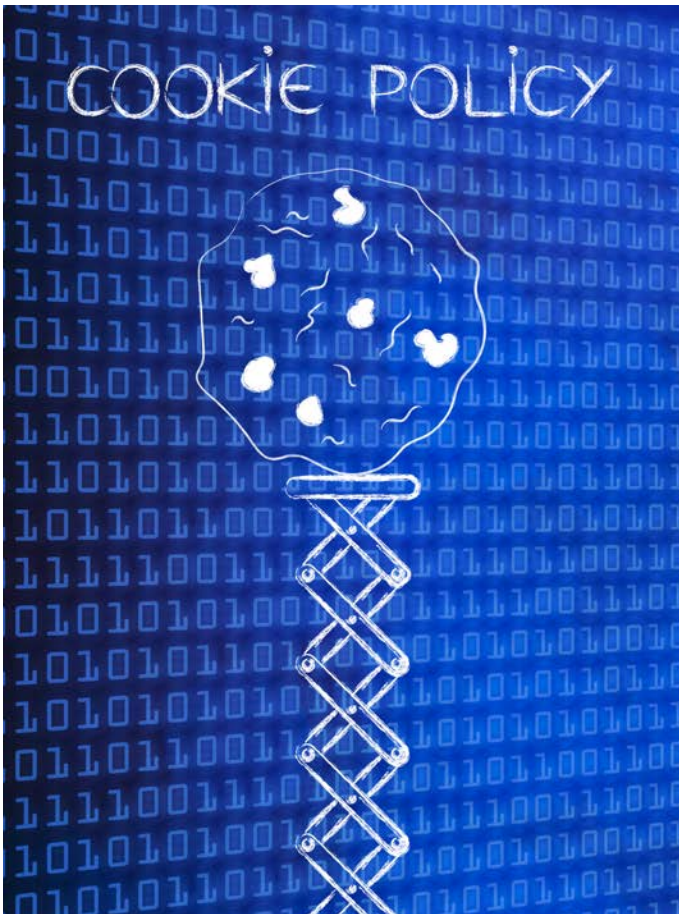
Sąd sfomułował jednocześnie generalny kierunek interpretacji przepisów o dostępie do informacji publicznej, które powinny służyć jak najszerszemu obywatelskiemu dostępowi do danych publicznych. Zatem normy regulujące zarówno tryb, jak i zasady dostępu do informacji publicznej winny być wykładane z poszanowaniem reguły *in dubio pro libertate*, a więc dążyć do ujawnienia danych, a nie do szukania podstaw, aby ograniczać ich dostępność, bowiem zasada jawności życia publicznego i transparentności działań władzy publicznej, które legły u podstaw obywatelskiego prawa do informacji publicznej, ma sprzyjać sprawowaniu społecznej kontroli przez wszystkich obywateli.

[2] Ustawa z dnia 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych (Dz. U. z 2021 r. poz. 289).

Niemieckie orzecznictwo dotyczące stosowania plików cookie

Mateusz Kupiec

Przetwarzanie danych osobowych za pomocą plików cookie na potrzeby m.in. analizowania zachowania użytkowników strony internetowej jest obecnie jednym z najbardziej wzbudzających zainteresowanie zagadnień. Coraz częściej na ten temat wypowiadają się nie tylko organy nadzorcze, lecz także sądy. W tekście przyglądam się dwóm ważnym orzeczeniom dotyczącym stosowania plików cookie, wydanym ostatnio przez niemieckie sądy.



Postanowienie Sądu Administracyjnego w Wiesbaden z dnia 1 grudnia 2021 r., sygn. akt 6 L 738/21.WI

Sąd Administracyjny w Wiesbaden orzekł, że jedna z heskich publicznych uczelni wyższych (Hochschule RheinMain) nie może na swojej stronie internetowej korzystać z usługi przedsiębiorstwa „A", umożliwiającej zebranie zgody użytkowników konkretnego serwisu na zapisanie plików cookie na ich urządzeniach końcowych.

Z ustaleń sądu wynika, że narzędzie przedsiębiorstwa „A" przetwarza pełny adres IP użytkownika końcowego na serwerach przedsiębiorstwa „B" (jako podwykonawcy) z siedzibą w Stanach Zjednoczonych Ameryki i w ten sposób dokonuje transferu danych do państwa trzeciego. Wobec tego w ocenie sądu:

- Korzystanie przez uczelnię z usługi przedsiębiorstwa „A" narusza przepisy o ochronie danych osobowych, ponieważ użytkownicy strony internetowej uczelni nie byli pytani o zgodę na przekazanie danych do USA. W banerze cookie nie zawarto także informacji o ewentualnych zagrożeniach dla prywatności użytkowników, wynikających z transferu danych do USA. Sąd, wydając wyrok, odwołał się do wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 16 lipca 2020 r. w sprawie Schrems II (C-311/18).
- Uczelnia i przedsiębiorstwo „A", oferujące narzędzie do zbierania zgód na instalowanie plików cookie, są współadministratorami w rozumieniu przepisów RODO. Zdaniem sądu w Wiesbaden świadczy o tym to, że uczelnia przekazywała dane użytkowników przedsiębiorstwu „A" w celu zarządzenia przez nie udzielonymi zgodami. Przedsiębiorstwo „A" było odpowiedzialne za projekt techniczny narzędzia i pomagało uczelni w określeniu sposobów przetwarzania, ponieważ decydowało o kategoriach gromadzonych danych.
- W analizowanym stanie faktycznym transfer do państwa trzeciego nie był konieczny do funkcjonowania strony internetowej uczelni.
- Dochodziło do przetwarzania danych osobowych, ponieważ użytkownika końcowego można jednoznacznie zidentyfikować na podstawie kombinacji klucza identyfikującego osobę odwiedzającą stronę internetową, który jest przechowywany w przeglądarce użytkownika, oraz przekazanego pełnego adresu IP.

Przedstawione orzeczenie nie jest jeszcze prawomocne, ale stanowi ważny krok w rozwoju dalszej praktyki stosowania przepisów danych osobowych w kontekście używania różnego rodzaju kodów śledzących. Wielu administratorów korzysta bowiem bezpośrednio lub pośrednio z usług podmiotów mających siedzibę poza EOG.

Pełna treść

Wyrok Sądu Okręgowego we Frankfurcie nad Menem z dnia 19 października 2021 r., sygn. akt 3-06 O 24/21

Na początku grudnia centrum ochrony przeciwko nieuczciwej konkurencji (Zentrale zur Bekämpfung unlauteren Wettbewerbs) poinformowało, że Sąd Okręgowy we Frankfurcie nad Menem orzekł 19 października 2021 r., iż umieszczanie technicznie zbędnych plików cookie bez uprzedniego uzyskania zgody użytkownika stanowi czyn nieuczciwej konkurencji.

Zdaniem Sądu podmiot zarządzający stroną internetową ponosi odpowiedzialność za błędy popełnione w tym zakresie przez dostawcę platformy do zarządzania plikami cookie.

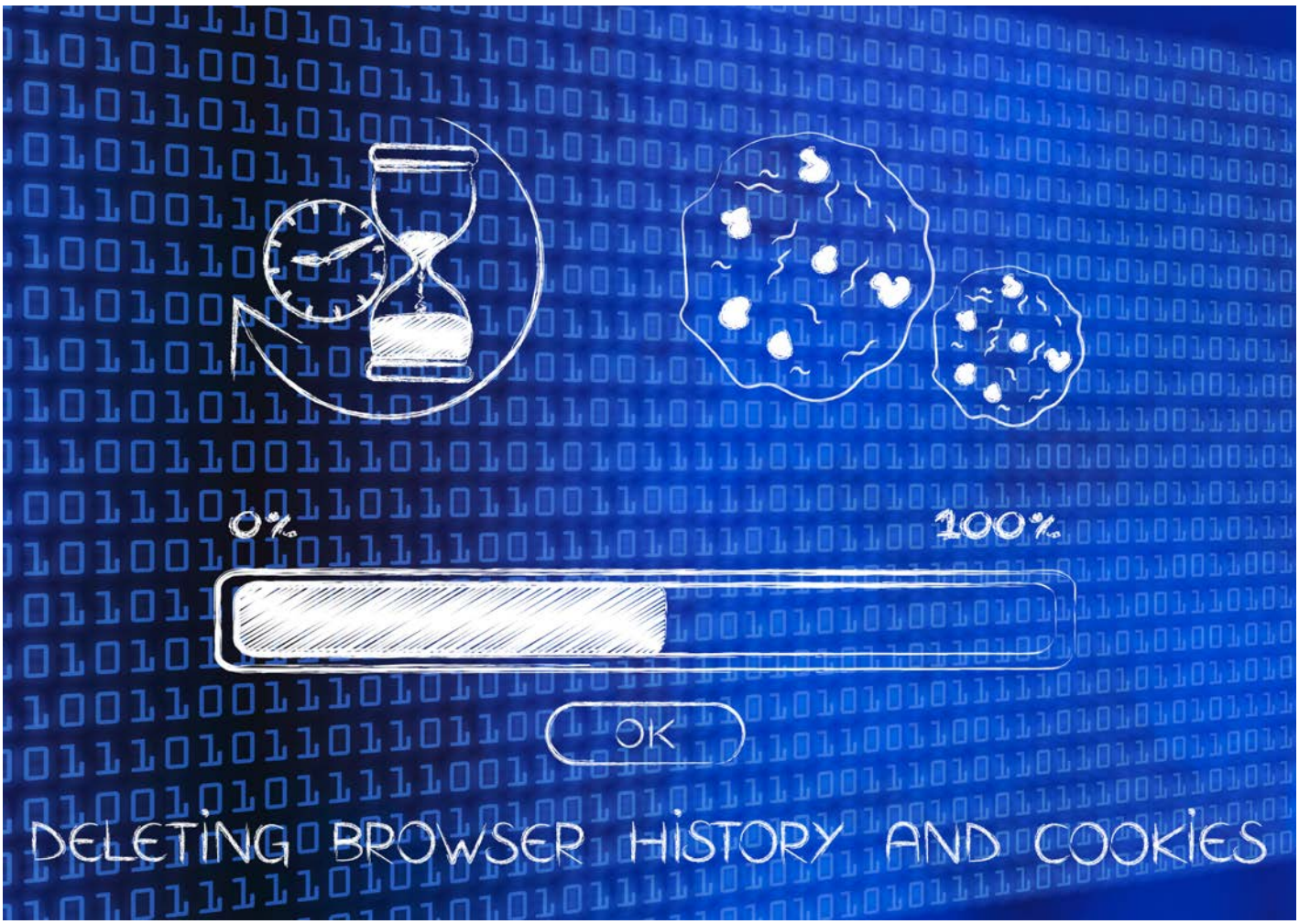
Sprawa, w której zapadło przedmiotowe rozstrzygnięcie, dotyczyła stosowania plików cookie przez przedsiębiorstwo z branży fitness. Wykorzystywane przez nie pliki cookie umożliwiały głównie dokonywanie pomiaru oglądalności i wyświetleń reklam, a także śledzenie użytkowników strony przedsiębiorstwa na potrzeby marketingu. Stosowane przez przedsiębiorstwo rozwiązania umożliwiały śledzenie użytkownika nawet po zamknięciu i ponownym uruchomieniu przeglądarki.

Wszystkie pliki cookie wykorzystywane przez przedsiębiorstwo były natychmiast zapisywane w przeglądarce użytkownika, gdy tylko wyświetlał on stronę przedsiębiorstwa (a więc zanim użytkownik mógł wejść w interakcję z banerem cookie).

Platforma do zbierania zgód, zintegrowana ze stroną przedsiębiorstwa, umożliwiała użytkownikom wybór plików cookie – lub wyłączenie niepotrzebnych – podzielonych na następujące grupy: „Statystyki", „Marketing" i „Usługi osób trzecich". Wybór dokonany przez użytkownika nie miał jednak żadnego znaczenia – na jego urządzeniu końcowym zawsze instalowane były wszystkie pliki cookie.

Sąd wskazał, że powyższe okoliczności były istotne z punktu widzenia prawa ochrony konkurencji, ponieważ gdyby użytkownicy wiedzieli o tym, iż rzekomo zdezaktywowane przez nich cookies w rzeczywistości nadal działały (wbrew ich woli), opuściliby stronę przedsiębiorcy.

Pełna treść wyroku



Ochrona danych osobowych w wewnętrznych systemach zgłaszania naruszeń prawa na gruncie projektowanej ustawy o sygnalistach

Patrycja Szurmak

Wstęp – ustawa o sygnalistach

Projekt ustawy o ochronie osób zgłaszających naruszenia prawa (dalej: „Ustawa o sygnalistach") z dnia 14 października 2021 r.[1], implementujący Dyrektywę Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (dalej: „Dyrektywa o sygnalistach")[2], kompleksowo reguluje kwestie związane z objęciem ochroną osób zgłaszających naruszenia prawa (tzw. sygnalistów) – zarówno w sektorze prywatnym, jak i w sektorze publicznym. Podstawowym celem projektowanej Ustawy o sygnalistach jest zapewnienie wdrożenia wymaganych Dyrektywą o sygnalistach środków ochrony osób zgłaszających nieprawidłowości, jak również wdrożenie rozwiązań organizacyjnych i instytucjonalnych do zapewnienia kanałów zgłaszania nieprawidłowości[3].

O jakich naruszeniach prawa mowa?

Projekt Ustawy o sygnalistach w art. 3 wskazuje, że naruszeniem prawa jest działanie lub zaniechanie niezgodne z prawem lub mające na celu obejście prawa, dotyczące dziedzin takich jak: zamówienia publiczne, zapobieganie praniu pieniędzy i finansowaniu terroryzmu, zdrowie publiczne, ochrona konsumentów, ochrona prywatności i danych osobowych. Należy wspomnieć, że art. 3 ust. 2 projektu Ustawy o sygnalistach wprowadza możliwość rozszerzenia katalogu zakresu naruszeń, które mogą być przedmiotem zgłoszenia wewnętrznego, o inne naruszenia, w szczególności dotyczące regulacji wewnętrznych lub standardów etycznych.

Jak można zgłaszać nieprawidłowości?

Projekt ustawy reguluje trzy tryby możliwego postępowania (zgłoszenia lub ujawnienia) w charakterze reakcji na powziętą informację o naruszeniu. Pierwszą możliwością jest zgłoszenie nieprawidłowości wewnątrz organizacji, drugą – skierowanie zgłoszenia do organu publicznego (w tym do wyznaczonego organu centralnego), trzecią zaś – ujawnienie publiczne.

W tym artykule rozważymy obowiązki związane z ochroną danych osobowych w ramach wewnętrznych systemów zgłaszania naruszeń prawa.

System zgłaszania naruszeń prawa a ochrona danych osobowych

Z punktu widzenia ochrony danych osobowych wdrożenie systemu zgłaszania naruszeń wewnętrznych w organizacji oznacza rozpoczęcie nowej czynności przetwarzania danych. Konieczne jest zatem zaprojektowanie i wdrożenie systemu zgłaszania naruszeń prawa zgodnie z przepisami ochrony danych osobowych.

Ustawa o sygnalistach wskazuje pewne obowiązki związane z ochroną danych osobowych wprost, ale nie czyni tego w sposób całościowy (kompleksowy). Jednak podstawowym przedmiotem Ustawy o sygnalistach nie są zagadnienia danych osobowych. Zastosowanie do tej ustawy będą miały przepisy ogólne, czyli przede wszystkim RODO[4].

Projektowana Ustawa o sygnalistach w obecnym kształcie wprowadza regulacje uszczegóławiające lub modyfikujące ogólne zasady ochrony danych osobowych wynikające z RODO.

Na początku należy ustalić, jaki jest status (administratora czy podmiotu przetwarzającego) podmiotu obowiązanego do

[1] Projekt dostępny na stronie: https://www.legislacja.gov.pl/projekt/12352401/katalog/12822845#12822845 (dostęp: 7.01.2022).
[2] Na marginesie warto wskazać, że termin na implementację Dyrektywy o sygnalistach minął 17 grudnia 2021 r. W tym artykule nie będziemy jednak analizować sytuacji bezpośredniego stosowania przepisów Dyrektywy o sygnalistach ze względu na upływ terminu na jej implementację, ale skoncentrujemy się na obowiązkach wynikających z projektu Ustawy o sygnalistach.
[3] Uzasadnienie do projektu ustawy, s. 1, https://www.legislacja.gov.pl/projekt/12352401/katalog/12822845#12822845 (dostęp: 7.01.2022).
[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Potwierdza to art. 17 Dyrektywy o sygnalistach.

wdrożenia wewnętrznego systemu zgłaszania naruszeń. W mojej ocenie jednoznaczne pozostaje, że taka osoba – jako podmiot decydujący o celach i środkach przetwarzania danych w ramach systemu zgłoszenia naruszeń – pełni rolę **administratora** danych przetwarzanych w systemie.

W ramach obsługi zgłoszeń naruszeń podmiot obowiązany będzie przetwarzać tzw. dane zwykłych kategorii, w szczególności dane naruszyciela, sygnalisty oraz innych osób zaangażowanych. Nie można wykluczyć, że w treści zgłoszenia sygnalista może również przekazać szczególne kategorie danych, o których mowa w art. 9 RODO.

W ramach obsługi zgłoszeń naruszeń podmiot obowiązany będzie przetwarzać tzw. **dane zwykłych kategorii**, w szczególności dane naruszyciela, sygnalisty oraz innych osób zaangażowanych. Nie można wykluczyć, że w treści zgłoszenia sygnalista może również przekazać **szczególne kategorie** danych, o których mowa w art. 9 RODO.

Administrator, wdrażając system zgłaszania naruszeń w organizacji, obowiązany jest dokonać implementacji zgodnie z wymogami przepisów sektorowych oraz wymogami określonymi w RODO.

Obowiązki ADO w związku z implementacją systemu zgłaszania naruszeń

Jedną z kluczowych zasad RODO jest wykazanie, że administrator przetwarza dane osobowe w ramach systemu zgłaszania naruszeń prawa zgodnie z podstawowymi zasadami przetwarzania danych osobowych (art. 5 ust. 2 RODO – zasada rozliczalności). W praktyce będzie to oznaczać, że administrator powinien przeprowadzić formalną analizę zgodności implementowanego systemu zgłaszania naruszeń pod kątem organizacyjnym oraz dokumentowym z przepisami związanymi z ochroną danych osobowych.

Punktem wyjścia do takiej formalnej analizy jest art. 5 RODO – wskazujący ogólne zasady ochrony danych. Należy pamiętać, że te ogólne zasady ochrony danych należy odpowiednio zmodyfikować, zgodnie z przepisami dotyczącymi ochrony danych określonymi w samej Ustawie o sygnalistach.

Poniżej w sposób kierunkowy zostaną przedstawione obowiązki wynikające z ogólnych zasad RODO, a w szczególności obowiązki wynikające z Ustawy o sygnalistach.

Do obowiązków administratora danych implementującego wewnętrzny system zgłaszania naruszeń należy:

1. Zapewnienie zgodności z prawem, rzetelności oraz przejrzystości przetwarzania (art. 5 ust. 1 lit. a RODO)

W praktyce oznacza to, że obowiązkiem administratora danych w ramach systemu zgłoszeń naruszeń będzie m.in.:

- Wprowadzenie odpowiednich podstaw przetwarzania danych osobowych w ramach przetwarzania danych w systemie zgłaszania naruszeń z uwzględnieniem regulacji ogólnych, tzn. art. 6 i 9 RODO, jak również art. 8 ust. 2 Ustawy o sygnalistach.

Ustawa o sygnalistach wprowadza podstawę prawną dla podmiotów obowiązanych do przetwarzania danych osobowych osoby, której dotyczy zgłoszenie (naruszyciela). Administrator będzie więc uprawniony do przetwarzania danych osobowych naruszyciela na podstawie art 6 ust. 1 lit c RODO – w związku z wypełnieniem ciążącego na administratorze danych obowiązku prawnego.

- Opracowanie przejrzystym językiem klauzul informacyjnych czy procedur wykonywania praw osób, których dane są przetwarzane.

Tutaj należy mieć na uwadze przede wszystkim art. 13 i 14 RODO, a także art. 8 ust. 2 zd. 2 Ustawy o sygnalistach. Ustawa o sygnalistach wskazuje, że administrator danych, przetwarzając dane osobowe naruszyciela, nie jest obowiązany do poinformowania naruszyciela, w ramach wykonywania wobec niego obowiązku informacyjnego, o źródle pochodzenia danych osobowych (a więc o tożsamości sygnalisty).

2. Przetwarzanie danych tylko w ograniczonym celu (art. 5 ust. 1 lit. b RODO)

Dane zebrane poprzez zgłoszenia sygnalisty mogą być przetwarzane tylko w ramach systemu zgłoszeń naruszeń.

3. Zapewnienie minimalizacji danych (art. 5 ust. 1 lit. c RODO)

Administrator, w ramach systemu zgłaszania naruszeń prawa, powinien opracować dokumentację oraz zaprojektować proces obsługi zgłoszeń w taki sposób, aby zbierane dane były adekwatne oraz niezbędne do celów realizowanych w ramach systemu zgłaszania naruszeń. Należy pamiętać, że relewantność danych należy oceniać w momencie ich pozyskiwania. W praktyce będzie to oznaczać, że administrator musi odpowiednio opracować dokumentację, w tym formularze zgłoszeń naruszeń, aby były one zgodne z zasadą minimalizacji danych.

4. Zapewnienie prawidłowości danych (art. 5 ust. 1 lit. d RODO)
Administrator, w ramach systemu zgłaszania naruszeń prawa, powinien zapewnić możliwość np. poprawienia czy uzupełnienia zgłoszenia przez sygnalistę – z zachowaniem poufności jego tożsamości.

5. Ograniczenie przechowywania danych w formie umożliwiającej identyfikację osoby, której dane dotyczą (art. 5 ust. 1 lit. e RODO)
Administrator, w ramach systemu zgłaszania naruszeń prawa, powinien przechowywać dane przez okres nie dłuższy, niż jest to niezbędne do celów prowadzonych postępowań wyjaśniających. Należy stosować odpowiednie okresy retencji – z uwzględnieniem art. 8 ust. 3 projektu Ustawy o sygnalistach.

Ustawa o sygnalistach wprowadza obowiązek przetwarzania danych osobowych nie dłużej niż przez 5 lat od dnia przyjęcia zgłoszenia. Należy zwrócić uwagę, że powyższy termin ustawowy dotyczy przetwarzania danych osobowych z przyjętego zgłoszenia. Dane osobowe, które nie mają związku ze zgłoszeniem czy są nadmiarowe, powinny być usuwane bez zbędnej zwłoki.

W praktyce oznacza to konieczność aktualizacji obecnych polityk retencji w stosunku do nowego procesu przetwarzania danych osobowych oraz konieczność zapewnienia archiwizacji czy usunięcia danych osobowych w przypadkach, kiedy dane nie są niezbędne.

6. Zapewnienie bezpieczeństwa danych (art. 5 ust. 1 lit. f RODO)
Administrator musi zapewnić odpowiednie bezpieczeństwo danych osobowych, w tym m.in. ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, utratą, zniszczeniem czy uszkodzeniem danych.

Przy doborze środków bezpieczeństwa przetwarzania danych w ramach systemu zgłaszania naruszeń nieprawidłowości administrator powinien uwzględnić regulacje sektorowe:

- Art. 30 ust. 3 Ustawy o sygnalistach określa wymóg, aby dane sygnalisty były przechowywane oddzielnie od nośnika informacji obejmującego zgłoszenie. Jednocześnie Ustawa o sygnalistach wskazuje, że w niektórych przypadkach zasadne jest usunięcie danych osobowych sygnalisty ze zgłoszenia.
- Art. 30 ust. 2 Ustawy o sygnalistach wprowadza obowiązek nadawania pisemnych upoważnień przez administratora danych osobom zaangażowanym w system zgłoszeń naruszeń w organizacji. Ustawa o sygnalistach wprowadza również ustawowy obowiązek zachowania w tajemnicy przez osoby zaangażowane w system zgłoszeń naruszeń informacji pozyskanych w związku z wykonywaną funkcją.
- Art. 32 ust. 1 Ustawy o sygnalistach określa wymóg zawarcia umowy z podmiotem, któremu administrator powierza czynności związane z obsługą systemu zgłoszeń naruszeń. W praktyce administrator chcący skorzystać z zewnętrznego podmiotu oferującego odpowiedni system informatyczny będzie musiał zawrzeć z nim umowę powierzenia przetwarzania, zgodnie z art. 28 RODO. Jednocześnie Ustawa o sygnalistach wskazuje, że administrator danych nie może przenieść na zewnętrzny podmiot odpowiedzialności za wypełnienie obowiązków związanych ze zgłoszeniami wewnętrznymi, w szczególności: zachowania poufności, udzielenia informacji zwrotnej czy konieczności podejmowania działań następczych.

Powyżej opisane wymogi wskazują w sposób ogólny obowiązki administratora danych związane z wdrożeniem systemu zgłaszania naruszeń prawa. Należy również pamiętać o szczegółowych obowiązkach, jakie wynikają z RODO lub z wytycznych czy z komunikatów Prezesa Urzędu Ochrony Danych Osobowych. Przede wszystkim należy pamiętać o komunikacie[5] Prezesa Urzędu Ochrony Danych Osobowych, który w pkt. 9 wskazuje, że: „Przetwarzanie danych dotyczących osób, których ocena i świadczone im usługi są uzależnione od podmiotów lub osób, które dysponują uprawnieniami nadzorczymi i/lub ocennymi", np. systemy służące do zgłaszania naruszeń (*whistleblowing*), wymaga przeprowadzenia formalnej oceny skutków dla ochrony danych (art. 35 RODO).

[5] Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony.

Odpłatny, prawnie uzasadniony interes administratora danych. Wnioski z wyroku NSA z dnia 30 listopada 2021 r., III OSK 4558/21

Patrycja Szurmak

Wstęp

Naczelny Sąd Administracyjny (NSA) w wyroku III OSK 4558/21 uznał, że historyczne informacje dotyczące pełnienia funkcji członka organów i wspólnika w spółkach prawa handlowego nadal mogą pozostać w sferze publicznego zainteresowania. Przetwarzanie danych historycznych w celach wspomagania rozwoju demokracji poprzez upowszechnienie praw obywatela w zakresie dostępu do informacji publicznej oraz ponownego wykorzystania informacji sektora publicznego jest prawnie uzasadnione. Co więcej, NSA wskazał, że nie ma znaczenia, czy prawnie uzasadniony interes administratora danych jest realizowany odpłatnie, czy nieodpłatnie.

Stan faktyczny

Podmiot danych wniósł skargę do Prezesa Urzędu Ochrony Danych Osobowych (PUODO) w przedmiocie przetwarzania jego danych osobowych przez Fundację Moje Państwo (dalej: „Fundacja") na potrzeby związane z funkcjonowaniem serwisu internetowego. Skarżący wniósł również sprzeciw wobec przetwarzania jego danych osobowych. Dodatkowo wniósł o zobowiązanie administratora danych (Fundacji) do usunięcia jego danych osobowych i całkowitego zaprzestania ich przetwarzania.

Organ w ramach postępowania wyjaśniającego ustalił następujące fakty:

- **Fundacja**. Fundacja, w ramach swojej statutowej działalności, działa na rzecz rozwoju demokracji poprzez upowszechnienie praw obywatela w zakresie dostępu do informacji publicznej. Realizacja ww. działań opiera się na tworzeniu rozwiązań informatycznych, które pozwalają w łatwiejszy sposób dotrzeć do obywateli. Fundacja umożliwia też wyszukiwanie czy tworzenie powiązań personalnych wraz ze wskazaniem powiązań historycznych w odpłatnej wersji serwisu.
- Zakres i źródło danych. W ramach postępowań wyjaśniających ustalono, że Fundacja przetwarza dane osobowe skarżącego jako aktualnego członka organów i wspólnika, a także informacje dotyczące byłych aktywności skarżącego jako członka organów i wspólnika w fundacji, sp. z o.o. w likwidacji, sp. k., sp. z o.o. sp. k., sp. j. i szeregu spółek z o.o. Fundacja przetwarza dane pobrane ze strony Krajowego Rejestru Sądowego oraz Monitora Sądowego i Gospodarczego.
- Cel przetwarzania. Organ ustalił, że Fundacja udostępnia dane osobowe w ramach swojego serwisu w celu wynikającym z przedmiotu działalności Fundacji, jakim jest wspomaganie rozwoju demokracji poprzez upowszechnienie praw obywatela w zakresie dostępu do informacji publicznej oraz ponownego wykorzystania informacji sektora publicznego.

Po przeprowadzeniu postępowania wyjaśniającego organ odmówił uwzględnienia wniosku podmiotu danych. PUODO uznał, że cele i zadania Fundacji mają bez wątpienia prawnie usprawiedliwiony charakter, a fakt, że administrator prowadzi swoją działalność w sposób częściowo odpłatny, świadczy o tym, że realizuje równolegle cel zarobkowy i informacyjny, czyniąc to z wykorzystaniem dopuszczonych prawem instrumentów. Organ wskazał, że przetwarzane przez Fundację dane osobowe skarżącego są danymi powszechnie dostępnymi, a zakres publikowanych w serwisie internetowym danych osobowych skarżącego jest adekwatny (nienadmierny) w kontekście realizowanego celu informacyjnego.

Na podstawie złożonej skargi przez podmiot danych Wojewódzki Sąd Administracyjny (WSA) w Warszawie podzielił ustalenia organu i podtrzymał decyzję PUODO. Podmiot danych złożył skargę kasacyjną od wyroku WSA, zaskarżając wyrok w całości.

Ustalenia Naczelnego Sądu Administracyjnego

NSA podtrzymał stanowisko WSA w Warszawie oraz PUODO, że działania Fundacji, polegające na przetwarzaniu danych osobowych skarżącego jako aktualnego członka organów i wspólnika, a także informacji dotyczących byłych aktywności skarżącego jako członka organów i wspólnika w celu wspomagania rozwoju demokracji poprzez upowszechnienie praw obywatela w zakresie dostępu do informacji publicznej oraz ponownego wykorzystania informacji sektora publicznego, znajdują podstawę w art. 6 ust. 1 lit. f RODO .

Kwestia oferowanych przez Fundację komercyjnych opracowań danych (w tym powiązań osobistych danej osoby w ramach innych podmiotów gospodarczych) nie ma wpływu na istnienie przesłanki przetwarzania danych osobowych na podstawie prawnie uzasadnionego interesu. NSA wskazał, że dane przetwarzane przez Fundację, pochodzące zarówno z aktualnych źródeł, jak i z poprzednich wpisów, zostały pozyskane legalnie.

Dodatkowo NSA potwierdził, że nie ma znaczenia, czy prawnie uzasadniony interes jest realizowany odpłatnie, czy nieodpłatnie. NSA wskazał, że RODO nie wprowadziło ani takiego wymogu, ani rozróżnienia. Pobieranie odpłatności za udzielenie informacji, które mają charakter historyczny (nie stanowią aktualnych wpisów), pomimo że istotnie zapewnia Fundacji możliwość uzyskania dochodu, nie wyklucza tego, że dalej realizuje ona prawnie uzasadniony interes, świadczący zarówno o legalności, jak i o adekwatności przetwarzania danych osobowych skarżącego, pozyskanych z jawnych źródeł.

W związku z powyższym NSA potwierdził brak podstaw do nakazania usunięcia danych skarżącego przez Fundację.

Pełna treść wyroku

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

Europejska Rada Ochrony Danych przyjęła wytyczne w sprawie relacji pomiędzy art. 3 i rozdziałem V RODO

Dominika Nowak

W wytycznych z dnia 18 listopada 2021 r. EROD sformułowała trzy kryteria kwalifikacji przetwarzania jako przekazywania danych osobowych do państwa trzeciego lub do organizacji międzynarodowej:

- administrator lub podmiot przetwarzający podlega RODO[1] w zakresie konkretnego przetwarzania;
- administrator lub podmiot przetwarzający będący eksporterem ujawnia poprzez transmisję lub w inny sposób dane osobowe innemu administratorowi, współadministratorowi lub podmiotowi przetwarzającemu, czyli importerowi;
- importer znajduje się w państwie trzecim lub jest organizacją międzynarodową, niezależnie od tego, czy ten importer podlega RODO w odniesieniu do danego przetwarzania zgodnie z art. 3 RODO.

W wytycznych omówione zostało każde z tych trzech kryteriów, w tym przywołano siedem pomocnych przykładów.

Jeżeli wszystkie kryteria określone przez EROD są spełnione, to następuje przekazanie danych do państwa trzeciego lub do organizacji międzynarodowej. W konsekwencji administrator lub podmiot przetwarzający musi w takiej sytuacji spełnić warunki z rozdziału V RODO i ukształtować przekazanie danych osobowych za pomocą instrumentów prawnych po ich przekazaniu do państwa trzeciego lub do organizacji międzynarodowej.

Warto podkreślić, że administratorzy i podmioty przetwarzające, których przetwarzanie podlega RODO zgodnie z art. 3 RODO, zawsze muszą przestrzegać rozdziału V RODO, gdy ujawniają dane osobowe administratorowi bądź podmiotowi przetwarzającemu w państwie trzecim lub organizacji międzynarodowej. Dotyczy to również ujawnienia danych osobowych przez administratora lub podmiot przetwarzający, którzy nie mają siedziby w UE, ale podlegają RODO zgodnie z art. 3 ust. 2 RODO, administratorowi lub podmiotowi przetwarzającemu w tym lub innym państwie trzecim.

EROD zwraca uwagę na potrzebę opracowania narzędzia transferu, gdy importer podlega RODO w zakresie danego przetwarzania zgodnie z art. 3 ust. 2 RODO, np. nowego zestawu standardowych klauzul umownych, który nie będzie powielał obowiązków wynikających z RODO, tylko uzupełni luki związane ze sprzecznymi przepisami krajowymi, z dostępem rządu państwa trzeciego do danych osobowych oraz trudnościami w egzekwowaniu i uzyskaniu zadośćuczynienia wobec podmiotów spoza UE.

Wytyczne

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

Raport ENISA dotyczący podnoszenia świadomości w zakresie cyberbezpieczeństwa w państwach członkowskich UE i wynikające z niego zalecenia

Andrzej Kaczmarek

Unia Europejska od dłuższego czasu podejmuje działania w zakresie informowania społeczeństwa o zagrożeniach w cyberprzestrzeni oraz wynikających z nich szkodach w postaci strat finansowych, wizerunkowych oraz braku zaufania społeczeństwa do czynności wykonywanych przy użyciu sieci informatycznej. Do działań tych należało utworzenie w 2004 r. Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA), której nazwę w 2019 r. na mocy rozporządzenia 2019/881[1] zmieniono na Agencję Unii Europejskiej ds. Cyberbezpieczeństwa, pozostawiając jej dotychczasowy akronim, oraz przyjęcie Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (nazywanej również dyrektywą NIS) – została ona wdrożona w Polsce ustawą o krajowym systemie cyberbezpieczeństwa[2]. Niezależnie od działań wynikających z ww. ustawy inicjatywy w sprawie wzmacniania bezpieczeństwa cyberprzestrzeni podejmowane były wcześniej. Pierwszym dokumentem w tym zakresie była Uchwała nr 111/2013 Rady Ministrów z dnia 25 czerwca 2013 r. w sprawie Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, której podstawowym celem było osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni państwa. Następnym krokiem było przyjęcie w maju 2017 r. Uchwały nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, która w październiku 2019 r. zastąpiona została Uchwałą nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024. Głównym jej celem jest zwiększenie odporności na cyberzagrożenia, podniesienie poziomu ochrony informacji w sektorze publicznym, militarnym i prywatnym. Cel ten ma być osiągnięty m.in. poprzez budowanie świadomości i kompetencji społecznych w zakresie bezpieczeństwa. Aby zrealizować te założenia, należy stworzyć i wdrożyć taki model funkcjonowania systemu edukacji akademickiej i doskonalenia zawodowego, który zapewni odpowiednie do wyzwań kwalifikacje pracowników oraz edukację obywateli w zakresie cyberbezpieczeństwa. We wszystkich krajach UE podejmowane są podobne działania, a ENISA – jako Agencja Unii Europejskiej ds. Cyberbezpieczeństwa – wspiera je, opracowując różnego rodzaju przewodniki, raporty i inne materiały. Do działań w tym obszarze należy wydawany corocznie raport pod nazwą ENISA Threat Landscape (ETL) na temat stanu zagrożeń cybernetycznych, w którym przedstawiane są najważniejsze zagrożenia, zaobserwowane trendy ich rozwoju i rozprzestrzeniania się, podmioty odpowiedzialne za te zagrożenia, a także sposoby reagowania na nie i środki zaradcze. Z przeprowadzonych przez ENISA badań wynika, że działania prowadzone w różnych państwach członkowskich w zakresie podnoszenia świadomości o zagrożeniach cyberbezpieczeństwa są bardzo zróżnicowane i nie zawsze przynoszą oczekiwane efekty. Wyniki tych badań i wnioski z nich płynące w postaci rekomendacji przedstawiono w omawianym poniżej raporcie ENISA, zatytułowanym „Podnoszenie świadomości kluczowym elementem narodowych strategii cyberbezpieczeństwa[3], który opublikowany został w listopadzie 2021 r.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie).

[2] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2020 r., poz. 1369).

[3] ENISA, *RAISING AWARENESS OF CYBERSECURITY. A Key Element of National Cybersecurity Strategies*, listopad 2021, https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity (dostęp: 14.01.2022).

1. Główne cele raportu „Podnoszenie świadomości kluczowym element narodowych strategii cyberbezpieczeństwa”

Głównym celem raportu jest wskazanie kierunku działań, jakie państwa członkowskie powinny podjąć, aby skutecznie przeciwstawić się stale rosnącej liczbie ataków cybernetycznych poprzez zwiększenie potencjału obronnego w postaci odpowiedniej wiedzy i świadomości swoich obywateli.

W tym kontekście ENISA już od dłuższego czasu corocznie organizuje warsztaty poświęcone krajowym strategiom bezpieczeństwa cybernetycznego: National Cybersecurity Strategies (NCSS). Ostatnie warsztaty odbyły się w listopadzie 2021 r. i poświęcone zostały postępom i dobrym praktykom stosowanym przez państwa członkowskie UE w zakresie podnoszenia świadomości w dziedzinie cyberbezpieczeństwa, które zawarto w wymienionym we wstępie raporcie.

W raporcie tym dogłębnie przeanalizowano metody i podejścia stosowane przez państwa członkowskie, obejmujące m.in. planowanie, działania w zakresie podnoszenia świadomości, wskaźniki wydajności i osiągnięte efekty. Poprzez określenie dobrych praktyk, wyzwań i wyciągniętych wniosków w raporcie zaproponowano również zalecenia dotyczące sposobów zwiększenia skuteczności krajowych działań w zakresie podnoszenia świadomości o zagrożeniach i sposobach ochrony przed atakami w cyberprzestrzeni.

1.1. Docelowi odbiorcy raportu

Raport adresowany jest do instytucji i organizacji zaangażowanych w podnoszenie świadomości w zakresie bezpieczeństwa cybernetycznego na poziomie krajowym, w tym do krajowych organów właściwych ds. bezpieczeństwa cybernetycznego, specjalistów ds. bezpieczeństwa (IT) oraz innych grup, które były organizatorami lub uczestnikami obchodów Europejskiego Miesiąca Cyberbezpieczeństwa[4] (EMBC) lub podobnych. Więcej informacji o organizowanych w Polsce akcjach w ramach obchodów EMBC dostępnych jest na stronie https://bezpiecznymiesiac.pl/. Materiał zawarty w raporcie może być przydatny również dla osób odpowiedzialnych za wyznaczanie kierunków działań i polityki, dążących do poprawy świadomości w zakresie bezpieczeństwa, w tym szczególnie dla osób odpowiedzialnych za realizację programów krajowych. W Polsce takim programem jest Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, za której realizację odpowiada minister właściwy ds. cyfryzacji.

1.2. Przedstawione badania

W raporcie przedstawiono przegląd działań mających na celu budowanie krajowych zdolności w zakresie podnoszenia świadomości bezpieczeństwa cybernetycznego. Pokazano najlepsze praktyki wielu państw członkowskich UE oraz omówiono znaczenie okresowych ocen, trendów i wyzwań dotyczących bezpieczeństwa cybernetycznego. Zaprezentowano także analizę metryk stosowanych do pomiaru behawioralnych aspektów bezpieczeństwa cybernetycznego oraz analizę rzeczywistych kampanii uświadamiających w tym zakresie. W ostatnim rozdziale, będącym podsumowaniem raportu, przedstawiono szereg zaleceń mających na celu zwiększenie skuteczności krajowych działań na rzecz podnoszenia świadomości o zagrożeniach w cyberprzestrzeni oraz przeciwdziałania im.

1.2. Przedstawione badania

W raporcie przedstawiono przegląd działań mających na celu budowanie krajowych zdolności w zakresie podnoszenia świadomości bezpieczeństwa cybernetycznego. Pokazano najlepsze praktyki wielu państw członkowskich UE oraz omówiono znaczenie okresowych ocen, trendów i wyzwań dotyczących bezpieczeństwa cybernetycznego. Zaprezentowano także analizę metryk stosowanych do pomiaru behawioralnych aspektów bezpieczeństwa cybernetycznego oraz analizę rzeczywistych kampanii uświadamiających w tym zakresie. W ostatnim rozdziale, będącym podsumowaniem raportu, przedstawiono szereg zaleceń mających na celu zwiększenie skuteczności krajowych działań na rzecz podnoszenia świadomości o zagrożeniach w cyberprzestrzeni oraz przeciwdziałania im.

2. Budowa potencjału w zakresie podnoszenia świadomości o zagrożeniach cyberbezpieczeństwa i jego skutkach

Analiza dokumentacji i wywiady wykazały, że w państwach członkowskich już od kilku lat przyjmowane były różne strategie w zakresie bezpieczeństwa cybernetycznego. Zauważono jednak, że o ile wcześniejsze strategie odnosiły się do tej kwestii powierzchownie lub deklaratywnie, o tyle obecnie istnieje wyraźna tendencja do opisywania konkretnych celów

[4] W Polsce akcje organizowane w ramach Europejskiego Miesiąca Cyberbezpieczeństwa, obchodzonego w październiku, koordynowane są przez NASK PIB (Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy).

podnoszenia świadomości oraz odpowiednich działań w bardziej szczegółowy sposób. Większość badanych krajów dostrzega znaczenie ścisłej współpracy różnych podmiotów przy prowadzeniu działań podnoszących świadomość. Przeprowadzone wywiady autorów raportu z państwami członkowskimi UE potwierdziły potrzebę wspólnego zaangażowania podmiotów publicznych i prywatnych na poziomie krajowym i regionalnym w celu zwiększenia skuteczności podejmowanych działań uświadamiających. W Polsce przykładem takiej współpracy jest Program Współpracy w Cyberbezpieczeństwie (PWCyber)[5].

Ważne są również inicjatywy lokalne. W odniesieniu do jednostek samorządu terytorialnego (JST) dużą szansę na wzmocnienie świadomości, a także wyposażenie JST w odpowiednie narzędzia ochrony przed cyberzagrożeniami daje w ostatnim czasie program Cyfrowa Gmina, z którego środki można wykorzystać na zakup szkoleń z zakresu cyberbezpieczeństwa oraz zaopatrzenie urzędów w programy wspierające cyfrowe bezpieczeństwo[6].

W raporcie podkreślono ponadto, że zapewnienie bezpieczeństwa cybernetycznego wymaga synergicznych działań w obszarze prawnym, organizacyjnym, technicznym i edukacyjnym. Elementem mającym istotne znaczenie dla skuteczności podejmowanych działań jest również wystarczające, spójne i ciągłe ich finansowanie oraz współpraca z mediami w zakresie wspierania nie tylko kampanii informacyjnych dotyczących cyberbezpieczeństwa, lecz także dziennikarzy w ich pracy. Przykładem takich rozwiązań jest Editor's Encryption Guide – podręcznik cyberbezpieczeństwa dla dziennikarzy wydany w Finlandii, w którym zawarto wskazówki m.in. na temat tego, jak chronić swoje przekazy i źródła przed atakami cybernetycznymi.

3. Oceny tendencji w zakresie bezpieczeństwa cybernetycznego i związanych z nim wyzwań

W raporcie zwraca się uwagę na regularne przeprowadzanie analiz i publikowanie informacji dotyczących tendencji i wyzwań związanych z cyberbezpieczeństwem. W opinii autorów raportu takie działania promują publiczną dyskusję na temat możliwego wpływu cyberataków nie tylko na konkretne systemy informatyczne będące celem ataku, lecz także na bezpieczeństwo narodowe jako całość.

Wskazano, że regularnie udostępniane oceny pomagają obywatelom uświadomić sobie, w jaki sposób każda osoba może się przyczynić do lepszej ochrony cyberprzestrzeni. Podkreślono, że skuteczne cyberbezpieczeństwo można osiągnąć głównie poprzez kompleksowe podejście – wysiłek, który wymaga wkładu wszystkich osób. Z przeprowadzonych badań wynika, że udostępnianie informacji na temat tendencji i wyzwań w zakresie cyberbezpieczeństwa w sposób przystępny i zrozumiały dla odbiorców nietechnicznych umożliwia dotarcie do szerszego ich grona, w tym do ogółu społeczeństwa oraz decydentów na szczeblu politycznym, organizacyjnym i społecznym.

Wśród dobrych praktyk wskazano m.in. działania Federalnego Urzędu Bezpieczeństwa Teleinformatycznego w Niemczech (BSI), który corocznie publikuje „Stan bezpieczeństwa IT w Niemczech". Dokument ten zawiera informacje o zagrożeniach cybernetycznych dotyczących ogółu użytkowników, jednak główny nacisk położony jest na przedsiębiorstwa i administrację państwową. Specjalny zespół ds. świadomości obywatelskiej w BSI wykorzystuje ten raport do pozyskiwania i wyodrębnienia informacji, które są szczególnie interesujące dla użytkowników ogólnych, i przekłada je na bardziej obrazowy i łatwy do zrozumienia styl komunikacji. Używa w tym celu infografik i innych środków, aby w ciekawy sposób zwrócić uwagę na najważniejsze zagrożenia bezpieczeństwa cybernetycznego dla ogółu użytkowników (takie jak phishing, ransomware itp.). Ponadto BSI na bieżąco publikuje wytyczne i różne dokumenty techniczne związane z bezpieczeństwem cybernetycznym. Na przykład w 2020 r. BSI wydał kilka wytycznych dotyczących pandemii COVID-19, takich jak zalecenia w sprawie bezpiecznego biura domowego i bezpiecznych zakupów online. Wśród tematów przewodnich znalazły się też silne hasła i dwuskładnikowe uwierzytelnianie w celu odpowiedniej ochrony ważnych danych przechowywanych na kontach internetowych.

[5] Więcej informacji na temat PWCyber można znaleźć na stronie: https://www.gov.pl/web/cyfryzacja/program-wspolpracy-w-cyberbezpieczenstwie-pwcyber--partnerstwo-publiczno-prywatne-na-rzecz-krajowego-systemu-cyberbezpieczenstwa (dostęp: 14.01.2022).
[6] Więcej informacji na temat programu Cyfrowa Gmina można znaleźć na stronie: https://www.gov.pl/web/cyfryzacja/ruszyl-program-cyfrowa-gmina (dostęp: 14.01.2022).

W Polsce CSIRT Państwowego Instytutu Badawczego publikuje coroczny raport pt. „Krajobraz bezpieczeństwa polskiego Internetu”[7], który zawiera statystyki zagrożeń cyberbezpieczeństwa, a także roczne raporty dotyczące działalności zespołu Dyżurnet.pl[8]. Reaguje on na anonimowe zgłoszenia otrzymywane od internautów o potencjalnie nielegalnych materiałach, głównie związanych z seksualnym wykorzystywaniem dzieci. Dodatkowo przekazywane są informacje o cyberzagrożeniach, analizy ekspertów oraz rekomendacje, które publikowane są również na rządowym portalu internetowym prowadzonym przez Departament Cyberbezpieczeństwa Kancelarii Prezesa Rady Ministrów[9].

4. Pomiary zachowań dotyczących cyberbezpieczeństwa

W raporcie podkreśla się, że istnieją regularne badania opinii publicznej, takie jak Eurobarometr, które mogą służyć jako użyteczny punkt wyjścia do działań na rzecz podnoszenia świadomości. Oprócz danych z Eurobarometru w celach planowania kampanii informacyjnych można wykorzystać statystyki krajowe oraz zbiorcze dane z krajowych CERT-ów i organów ścigania na temat incydentów bezpieczeństwa w sieci i cyberprzestępczości. Dane te pomagają w dostosowaniu kampanii uświadamiających do aktualnych wyzwań i potrzeb.

W opinii autorów raportu ważnym czynnikiem sukcesu w podnoszeniu świadomości obywateli jest połączenie operacyjnej i społecznej perspektywy. Najlepszym sposobem na połączenie tych perspektyw, jak podano w raporcie, jest włączenie jednostek rządowych, które są odpowiedzialne za perspektywę operacyjną, do działań mających na celu podnoszenie świadomości społecznej w zakresie cyberbezpieczeństwa. Jako dobre przykłady wskazuje się niemieckie BSI, Urząd ds. Systemu Informatycznego w Estonii oraz Centre for Information Security w Norwegii, które łączą te elementy, jak pokazano wcześniej w przykładzie dotyczącym działań BSI.

5. Planowanie kampanii informacyjnych

W raporcie podkreśla się, że kampanie uświadamiające na temat cyberbezpieczeństwa wymagają starannego wyważenia, aby zwrócić uwagę na zagrożenia obecne w cyberprzestrzeni, przy jednoczesnym budowaniu zdolności do zachowania bezpieczeństwa danych osobowych i utrzymania zaufania do usług cyfrowych. W kampaniach informacyjnych ważne jest wykorzystanie różnych kanałów komunikacji w celu dotarcia do wszystkich grup docelowych odbiorców, aby nikt nie został pominięty, w tym osoby starsze oraz o niższym wykształceniu i niższym statusie społeczno-ekonomicznym. W tym celu należy odjąć próbę współpracy z różnymi podmiotami, które chcą pomóc w rozpowszechnianiu treści zwiększających świadomość w zakresie cyberbezpieczeństwa w swoich społecznościach. W raporcie podane zostały, jako dobre praktyki, przykłady akcji informacyjnych organizowanych w różnych krajach Unii Europejskiej.

6. Wnioski i zalecenia

Wnioski z przeprowadzonych badań i analiz przedstawiono w podziale na cztery obszary. Są one następujące:

6.1. W obszarze budowania zdolności do podnoszenia świadomości:

- Opracować narodową strategię podnoszenia świadomości, w tym przypisać właściwe role i zadania zaangażowanym podmiotom.
- Wspierać podmioty zaangażowane w realizację programu podnoszenia świadomości cyberbezpieczeństwa aktami prawnymi.
- Rozważyć powierzenie centralnej roli koordynacyjnej w zakresie działań na rzecz podnoszenia świadomości jednej instytucji.
- Zaangażować podmioty publiczne i prywatne na szczeblu krajowym i regionalnym, aby synergicznie działały we wszystkich obszarach: prawnym, organizacyjnym, technicznym i edukacyjnym, a także zapewnić współpracę między administracją publiczną a sektorem prywatnym.
- Zapewnić spójne i ciągłe finansowanie.

[1] Zob. https://en.nask.pl/eng/reports/reports/3835,CERT-2019-Report-PL.html (dostęp: 14.01.2022).
[2] Zob. https://en.dyzurnet.pl/publications (dostęp: 14.01.2022).
[3] Zob. https://www.gov.pl/web/baza-wiedzy/aktualnosci (dostęp: 14.01.2022).

6.2. W obszarze regularnej oceny trendów i wyzwań cyberbezpieczeństwa:

- Zapewnić regularne publikowanie analiz i raportów na temat środowiska zagrożeń w cyberprzestrzeni oraz wspierać koncepcję, że cyberbezpieczeństwo wymaga wspólnego wkładu i działania na poziomie państwowym i indywidualnym.
- Zwracać uwagę, aby informacje o trendach i zagrożeniach cyberbezpieczeństwa były dostępne również dla odbiorców nietechnicznych, co pozwoli na dotarcie do szerokiego ich grona, w tym do decydentów na poziomie politycznym, organizacyjnym i społecznym.

6.3. W obszarze pomiaru zachowań związanych z bezpieczeństwem:

- Zbierać dane ilościowe dotyczące zachowań związanych z cyberbezpieczeństwem w całym społeczeństwie. Wykorzystywać w tym celu badania opinii publicznej i statystyki. Mogą one dostarczyć użytecznych i niezbędnych spostrzeżeń w celu planowania bardziej ukierunkowanych i skutecznych działań, pozwalających osiągnąć pomyślne wyniki.
- Wykorzystywać istniejące regularne badania opinii publicznej dotyczące bezpieczeństwa cybernetycznego, takie jak np. Eurobarometr, a także systematycznie gromadzone, zagregowane dane pochodzące od krajowych zespołów CERT i organów ścigania na temat incydentów bezpieczeństwa i przestępstw w sieci, aby pomóc w określeniu tendencji i budowaniu świadomości.
- Wykorzystać badania opinii publicznej i statystyki, aby zrozumieć, w jaki sposób ludzie postrzegają ryzyko, i użyć tych informacji do przeprowadzenia skutecznych kampanii uświadamiających.

6.4. W obszarze planowania kampanii uświadamiających:

- Zaangażować ekspertów ds. komunikacji społecznej i marketingu w celu odpowiedniego sformułowania komunikatów, tj. w taki sposób, aby główne argumenty były zrozumiałe i nie mogły być łatwo podważone.
- Dobrą praktyką ogólnounijną jest organizowanie kampanii uświadamiających w październiku, który jest Europejskim Miesiącem Cyberbezpieczeństwa, a następnie ich kontynuowanie przez cały rok, gdyż działania mające na celu zaangażowanie obywateli w podnoszenie świadomości o zagrożeniach bezpieczeństwa w sieci powinny być prowadzone przez cały rok.

Realizacja przez administratora obowiązków z zakresu bezpieczeństwa danych osobowych

Dominika Nowak

Stan faktyczny

W maju 2020 r. Politechnika Warszawska zgłosiła Prezesowi UODO naruszenie ochrony danych osobowych, które następnie zostało uzupełnione. Naruszenie ochrony danych osobowych polegało na tym, że nieznana i nieuprawniona osoba pobrała z zasobów sieci informatycznej Politechniki bazę danych zawierającą dane osobowe studentów i wykładowców oraz kandydatów na studia – łącznie 5013 osób. Naruszenie dotyczyło następujących danych: imię, nazwisko, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer PESEL, adres e-mail, nazwa użytkownika i/lub hasło, nazwisko rodowe matki, seria i numer dowodu osobistego, numer telefonu. Politechnika Warszawska, w związku z wysokim ryzykiem naruszenia praw i wolności osób fizycznych, zawiadomiła wszystkie osoby o naruszeniu ochrony danych. W maju 2021 r. Prezes UODO wszczął postępowanie administracyjne w tej sprawie.

Rozstrzygnięcie

W decyzji z dnia 9 grudnia 2021 r. (DKN.5130.2559.2020) Prezes UODO nałożył na Politechnikę Warszawską administracyjną karę pieniężną w wysokości 45 000 zł za naruszenie przepisów art. 5 ust. 1 lit. f, art. 5 ust. 2, art. 24 ust. 1, art. 25 ust. 1 oraz art. 32 ust. 1 i 2 RODO , polegające na niezrealizowaniu obowiązków wynikających z RODO, tj.:

- niezastosowanie odpowiednich środków technicznych i organizacyjnych mających zapewnić zdolność do ciągłego zapewnienia poufności usług przetwarzania, brak regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających na celu zapewnienie bezpieczeństwa danych osobowych w systemie informatycznym, a tym samym nieuwzględnienie ryzyka związanego z przetwarzaniem danych osobowych;
- brak uwzględnienia ryzyka związanego z przetwarzaniem w aplikacji haseł użytkowników w postaci skrótu, co nie daje dostatecznej gwarancji bezpieczeństwa i w przypadku niezastosowania innych środków technicznych i organizacyjnych stanowi o narażeniu osób, których dane dotyczą, na zwiększenie ryzyka naruszenia praw lub wolności osób fizycznych w razie naruszenia zasady poufności;
- brak analizy zasadności 4-tygodniowego przechowywania logów maszyny wirtualnej, na której znajdował się system informatyczny, oraz brak analizy zasadności szczegółowego dziennika zdarzeń w aplikacji, co przesądza o niewłaściwym wdrożeniu środków technicznych i organizacyjnych zapewniających zdolność do szybkiego i skutecznego stwierdzenia wystąpienia naruszenia.

Należy zwrócić uwagę, że Prezes UODO umorzył postępowanie w zakresie naruszenia art. 34 ust. 1 RODO.

Komentarz

Z decyzji Prezesa UODO wynikają następujące wnioski:

- administrator powinien być w stanie udowodnić, że przeprowadził analizę ryzyka, co oznacza, że powinna być ona udokumentowana przez administratora;
- zastosowanie środków technicznych i organizacyjnych bez przeprowadzenia analizy ryzyka może skutkować tym, że wdrożone rozwiązania nie będą skuteczne ani adekwatne;
- zabezpieczenia danych osobowych na podstawie analizy ryzyka powinny być regularnie aktualizowane i dostosowywane do postępu technologii – przykładowo zabezpieczenie haseł może nie być skuteczne, jeżeli istnieją już techniki przełamywania tych zabezpieczeń.

Pełna treść decyzji

Ponowne wykorzystanie danych powierzonych przez administratora przez podmioty przetwarzające do własnych celów

Patrycja Szurmak

Wstęp

12 stycznia 2022 r. francuski organ ochrony danych (Commission nationale de l'informatique et des libertés, CNIL) wydał wytyczne dotyczące ponownego wykorzystywania danych osobowych przez podmioty przetwarzające do ich własnych celów zgodnie z RODO[1].

Co do zasady

Zgodnie z art. 4 pkt 8 oraz art. 28 ust. 3 lit. a RODO podmiot przetwarzający przetwarza dane osobowe w imieniu administratora i na podstawie udokumentowanego polecenia. Podmiot przetwarzający nie może przetwarzać powierzonych danych do własnych celów (na własny rachunek).

Potrzeba rynku

Usługodawcy (podmioty przetwarzające) czasami chcą ponownie wykorzystać przetwarzane w imieniu administratora dane np. w celu ulepszenia swoich usług lub produktów czy zaprojektowania nowych usług i produktów. Przykładowo dostawca oprogramowania biurowego chciałby analizować, w jaki sposób użytkownicy oprogramowania korzystają z usług dostawcy, aby mógł on ulepszać, rozwijać lub personalizować swoje produkty i usługi. Dostawcy usług mogą również potrzebować danych osobowych należących do swoich klientów, aby wspierać rozwój modeli uczenia maszynowego oprogramowania dostawcy.

Wytyczne CNIL

CNIL wskazuje, że ponowne wykorzystanie danych osobowych do własnych celów przez podmiot przetwarzający jest możliwe, jednak pod warunkiem, że:

- ponowne wykorzystanie danych jest zgodne z pierwotnym celem przetwarzania (**test kompatybilności**);
- administrator danych udzielił podmiotowi przetwarzającemu **pisemnego upoważnienia**.

Test kompatybilności

Przeprowadzenie testu zgodności jest wymagane, gdy podmiot przetwarzający chce do własnych celów ponownie wykorzystać dane otrzymane od administratora, a takiego przetwarzania nie legitymizuje zgoda udzielona przez daną osobę fizyczną lub nie odbywa się ono na podstawie prawa Unii Europejskiej bądź państwa członkowskiego.

Podmiot przetwarzający, chcąc przetwarzać dane w innym celu niż ten, w którym otrzymał je od administratora, musi ocenić, czy cel dalszego przetwarzania danych jest zgodny z pierwotnym celem przetwarzania. CNIL wskazuje, że przy przeprowadzaniu testu kompatybilności można posiłkować się takimi kryteriami, jak:

- związek między pierwotnym i dalszym celem przetwarzania;
- kontekst, w którym zebrano dane osobowe, w szczególności relacja między osobami, których dane dotyczą, a administratorem danych;
- charakter danych osobowych i ustalenie, czy chodzi o dane wrażliwe;
- potencjalne konsekwencje dalszego przetwarzania;
- zabezpieczenia, takie jak szyfrowanie, pseudonimizacja lub anonimizacja.

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

W wytycznych CNIL stwierdza, że „w przypadku, gdy podmiot przetwarzający chce ponownie wykorzystać dane w celu ulepszenia swoich usług przetwarzania w chmurze, takie ponowne wykorzystanie można uznać za zgodne z pierwotnym przetwarzaniem, z zastrzeżeniem odpowiednich gwarancji, takich jak anonimizacja danych, jeśli te dane identyfikujące nie są konieczne". CNIL wyjaśnia również, że w przypadku ponownego wykorzystania danych przez podmiot przetwarzający do celów marketingowych test kompatybilności byłby trudny do przejścia.

Jeżeli nowy cel przetwarzania nie spełnia testu kompatybilności, administrator danych nie może udzielić pisemnego upoważnienia do dalszego przetwarzania danych. W przypadku gdy test kompatybilności wykaże zgodność między pierwotnym celem a celem planowanym przez podmiot przetwarzający, administrator danych może się zgodzić na dalsze przetwarzanie danych.

Pisemne upoważnienie

Jak wskazuje CNIL, test kompatybilności należy przeprowadzić dla konkretnej operacji przetwarzania, biorąc pod uwagę cele i cechy każdej operacji przetwarzania, do której podwykonawca chce ponownie wykorzystać dane. W konsekwencji udzielenie pisemnej ogólnej zgody nie będzie zapewniało zgodności takiego przetwarzania. CNIL wskazuje również, że upoważnienie do przetwarzania pierwotnego administratora danych musi być sporządzone na piśmie, w tym w formie elektronicznej.

Podmiot przetwarzający jako samodzielny administrator danych

Jeżeli pierwotny administrator udzieli upoważnienia do przetwarzania, to podmiot przetwarzający staje się administratorem wobec danych przetwarzanych w tym nowym celu. W związku z tym nowy administrator zobowiązany jest przetwarzać te dane osobowe zgodnie z przepisami RODO, a w szczególności określić:

- podstawę prawną przetwarzania danych osobowych w nowym celu;
- sposób powiadamiania podmiotów danych, których dane przetwarza w ramach nowego celu (być może we współpracy z administratorem);
- odpowiedni okres przetwarzania danych (retencje danych);
- procedurę realizacji praw podmiotów danych;
- odpowiednie środki zapewniające bezpieczeństwo przetwarzania danych.

FAQ DSK dotyczące przetwarzania danych osobowych pracowników w czasach pandemii

Mateusz Kupiec

Pandemia COVID-19 trwa już prawie dwa lata. W tym czasie wielu pracodawców zdecydowało się przeciwdziałać rozprzestrzenianiu się koronawirusa w zakładach pracy, aby zachować ciągłość działania oraz chronić życie i zdrowie pracowników. Zauważywszy liczne wątpliwości pracodawców związane z realizacją przepisów o ochronie danych osobowych przy podejmowaniu takich działań, niemiecka konferencja Niezależnych Organów Ochrony Danych Federacji i Krajów Związkowych (dalej: DSK) opublikowała pod koniec grudnia 2021 r. zestaw odpowiedzi na najczęstsze pytania dotyczące przetwarzania danych osobowych pracowników w czasach pandemii koronawirusa (dalej: „FAQ"). Ustalenia DSK mogą również pomóc polskim pracodawcom stosować środki przeciwdziałające pandemii koronawirusa w miejscu pracy w sposób zgodny z wymogami RODO. Zalecenia są następujące:

- DSK dopuszcza przetwarzanie danych osobowych zatrudnionych na potrzeby prowadzenia tzw. dzienników kontaktów w celu przeciwdziałania rozwojowi pandemii. Zdaniem DSK podstawą takiego przetwarzania jest prawnie uzasadniony interes pracodawcy. Jednym z aspektów walki z pandemią jest bowiem umożliwienie pracodawcom, po tym, jak zostaną oni poinformowani przez pracownika, że zachorował na COVID-19, podjęcia próby zidentyfikowania jego kontaktów zawodowych lub wewnętrznych, poinformowania ich o ryzyku zakażenia wirusem i – jeśli to konieczne – zastosowania wewnętrznych środków ostrożności.
- DSK co do zasady odrzuca możliwość publikowania personaliów pracowników, u których stwierdzono zakażenie koronawirusem (pozytywny wynik testu), wśród zespołu.
- W ocenie DSK nie jest konieczne ujawnianie nazwisk pracowników, u których stwierdzono pozytywny wynik testu na obecność koronawirusa, aby chronić interesy pracodawcy; z reguły dotyczy to również ujawniania (ewentualnych) kontaktów takich pracowników z innymi członkami zespołu.
- Zdaniem DSK indywidualne osoby mogą zostać zapytane o kontakt z chorym pracownikiem, a następnie poinformowane o możliwym zakażeniu – bez upubliczniania nazwiska pracownika.
- Według DSK tylko w wyjątkowych sytuacjach pracodawca może przetwarzać dane osobowe zatrudnionego znajdujące się w zaświadczeniu lekarskim przedłożonym na potrzeby zwolnienia pracownika z obowiązku zakrywania ust i nosa w miejscu pracy. Takie przypadki określa prawo poszczególnych krajów związkowych w Niemczech. Niemniej DSK zauważa, że pracodawca nie musi żądać osobnego zaświadczenia od zatrudnionego – w zależności od zawartości znanej pracodawcy z innych źródeł historii chorób zatrudnionego może mu wystarczyć zapoznanie się z dostępną dokumentacją zatrudnienia, taką jak zwolnienie z przyczyn zdrowotnych.
- Zdaniem DSK pracodawcy mogą ustalać terminy szczepień dla swoich pracowników i w tym kontekście przetwarzać ich dane osobowe za ich zgodą – spełniającą wymogi RODO.
- Dane dotyczące zdrowia[1], które pracownicy są zobowiązani ujawnić w związku ze szczepieniami, powinny być przedstawione wyłącznie osobom wykonującym szczepienia – np. poprzez samodzielne przekazywanie przez zatrudnionych formularzy zawierających niezbędne dane dotyczące zdrowia osobom wykonującym szczepienia (lekarz zakładowy, punkt szczepień).
- DSK stanowczo krytykuje dokonywanie adnotacji w aktach osobowych pracownika o zgłoszeniu się przez niego do szczepienia przeciwko koronawirusowi.

Chociaż FAQ DSK nie omawia wszystkich problemów związanych z przetwarzaniem danych osobowych pracowników podczas pandemii, to publikacja ta stanowi ważny zbiór wskazówek dla administratorów starających się zapewnić ciągłość działania swojej organizacji w tych niepewnych i zmiennych czasach. W niniejszym tekście pominięto część FAQ o przetwarzaniu danych o odbyciu szczepienia przeciwko koronawirusowi, ponieważ dotyczy ona wewnętrznych przepisów w Niemczech.

Całość dokumentu

[1] Dla przypomnienia: zgodnie z art. 4 pkt 15 RODO „»dane dotyczące zdrowia« oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia".

PUBLIKACJE

„Standardowe klauzule umowne między administratorami a podmiotami przetwarzającymi wprowadzone decyzją Komisji Europejskiej z 4.6.2021 r." – artykuł autorstwa adw. dr hab. Grzegorza Sibigi, prof. INP PAN i adw. Katarzyny Syski, który ukazał się w dodatku specjalnym do Monitora Prawniczego pt. „Działania instytucji i organów Unii Europejskiej w ochronie danych osobowych" (dodatek MoP 23/2021).

„Ochrona danych osobowych i prywatności podczas stosowania plików cookie w świetle wytycznych i opinii Grupy Roboczej Art. 29 oraz Europejskiej Rady Ochrony Danych" - artykuł autorstwa Dominiki Nowak, który ukazał się w dodatku specjalnym do Monitora Prawniczego pt. „Działania instytucji i organów Unii Europejskiej w ochronie danych osobowych" (dodatek MoP 23/2021).

„O potrzebie przyjęcia nowego podejścia do ochrony danych osobowych dzieci przez EROD. Uwagi w świetle Opinii nr 2/2009 Grupy Roboczej Art. 29 o ochronie danych osobowych dzieci" artykuł autorstwa Mateusza Kupca, który ukazał się w dodatku specjalnym do Monitora Prawniczego pt. „Działania instytucji i organów Unii Europejskiej w ochronie danych osobowych" (dodatek MoP 23/2021).

Z tekstami członków Zespołu Ochrony Danych, które ukazały się w dodatku specjalnym do Monitora Prawniczego pt. **„Działania instytucji i organów Unii Europejskiej w ochronie danych osobowych" (dodatek MoP 23/2021)** pod red. G. Sibiga, można zapoznać się w bazie informacji prawnej Legalis lub w czasopiśmie, które jest dostępne pod linkiem.

Czytaj więcej

„Analiza ryzyka jako element bezpieczeństwa przetwarzania danych w kancelariach prawnych" oraz **„Poczta elektroniczna"** – rozdziały współautorstwa m.in. adw. dr hab. prof. INP PAN Grzegorza Sibigi, adw. Katarzyny Syski i r.pr. Dominiki Nowak, które ukazały się w monografii pt. „Analiza ryzyka i bezpieczeństwo danych w kancelariach prawnych" pod red. D. Lubasza.

Czytaj więcej

„Publiczna dostępność na podstawie przepisów o dostępie do informacji publicznej informacji i dokumentów dotyczących stosowania RODO przez administratora w orzecznictwie sądów administracyjnych" - artykuł autorstwa adw. dr hab. Grzegorza Sibigi, prof. INP PAN, który ukazał się w nr 4(52)/2021 Gdańskich Studiów Prawniczych pod red. Wojciecha R. Wiewiórowskiego.

Czytaj więcej

„Dane osobowe internautów to waluta XXI wieku" – wywiad z adw. Xawerym Konarskim, który ukazał się w Rzeczpospolitej w dniu 28 stycznia 2022 r.

Czytaj więcej

W nr 4/2021 ABI Expert ukazały się artykuły:

- **„Znaczenie i przyszłość prawa do przenoszenia danych"** - artykuł autorstwa Mateusza Kupca;
- **„Prawo ochrony danych osobowych w Chińskiej Republice Ludowej"** - artykuł współautorstwa Mateusza Kupca;
- **„Interpretacje krajowych sądów"** - artykuł autorstwa Mateusza Kupca.

NAGRODA

Z satysfakcją informujemy, że w dniu 28.01.2022 r. partnerowi naszej kancelarii, mec. Xawery Konarski, została wręczona przez Prezesa Urzędu Ochrony Danych Osobowych Jana Nowaka doroczna Nagroda im. Michała Serzyckiego, GIODO III kadencji.

Nagroda została przyznana za wieloletnie promowanie wartości ochrony danych osobowych i prawa do prywatności. Powyższe wyróżnienie stanowi kolejne już potwierdzenie pozycji naszego zespołu RODO, czego dowodem są zajmowane od lat wysokie pozycje w polskich i zagranicznych rankingach.

W 2020 roku Nagrodę im. Michała Serzyckiego, GIODO III kadencji otrzymał również adw. dr hab. prof. INP PAN Grzegorz Sibiga - Partner w Kancelarii kierujący Zespołem Ochrony Danych.

Czytaj więcej

WYDARZENIA

Konferencja - 26.01.2022 r.

Udział adw. Xawerego Konarskiego oraz adw. prof. INP PAN dr. hab. Grzegorza Sibiga w konferencji „Wyzwania i standardy dla Inspektorów ochrony danych w 2022 r.” organizowanej przez SABI - Stowarzyszenie Inspektorów Ochrony Danych z okazji Dnia Inspektora Ochrony Danych.

Konferencja - 15.12.2021 r.

Wykład adw. Xawerego Konarskiego „Nowe zasady transferu danych osobowych do państw trzecich na podstawie standardowych klauzul umownych” przeprowadzony podczas webinarium organizowanego przez MMC Polska.

Konferencja - 16.12.2021 r.

Wystąpienie adw. dr hab. prof. INP PAN Grzegorza Sibiga podczas wydarzenia „Podsumowanie najważniejszych dla IOD wydarzeń w 2021 r.” organizowanego przez SABI – Stowarzyszenie Inspektorów Ochrony Danych.

Konferencja - 7.12.2021 r.

Wystąpienia adw. Xawerego Konarskiego, adw. dr. hab. prof. INP PAN Grzegorza Sibiga (który również pełnił rolę moderatora całej Konferencji) i adw. Katarzyny Syski podczas VII Konferencji Ochrony Danych Osobowych: „Działania instytucji i organów Unii Europejskiej w ochronie danych osobowych” organizowanej przez Wydawnictwo C.H.Beck.

ZESPÓŁ RODO

Xawery Konarski
Adwokat, Senior Partner
xawery.konarski@traple.pl

Prof. INP PAN dr hab. Grzegorz Sibiga
Adwokat, Partner
grzegorz.sibiga@traple.pl

dr inż. Andrzej Kaczmarek
Of counsel
andrzej.kaczmarek@traple.pl

Katarzyna Syska
Adwokatka, Senior Associate
katarzyna.syska@traple.pl

Dominika Nowak
Radczyni prawna, Senior Associate
dominika.nowak@traple.pl

Patrycja Szurmak
Radczyni prawna, Associate
mateusz.kupiec@traple.pl

Bartłomiej Żeromski
Associate
bartlomiej.zeromski@traple.pl

Mateusz Kupiec
Junior Associate
mateusz.kupiec@traple.pl

Redaktor newslettera:
Mateusz Kupiec

Pytania prosimy kierować na adres:
rodo@traple.pl