NR 4 - PAŹDZIERNIK-LISTOPAD 2020

NEWSLETTER RODO

Temat numeru -

Wytyczne EROD w sprawie pojęć administratora, współadministratora oraz procesora

Tematy artykułów:

- Dodatkowe środki ochrony w przypadku transferu danych osobowych do państwa trzeciego
- Wytyczne EROD dot. targetowania w mediach społecznościowych
- Ochrona danych osobowych przetwarzanych w systemach AI
- Najnowsze decyzje organów nadzorczych

Traple Konarski Podrecki & Wspólnicy

TKP

Wytyczne EROD w sprawie pojęć administratora, współadministratora oraz podmiotu przetwarzającego

r.pr. Dominika Nowak, dr Iga Małobęcka-Szwast

Podczas 37. posiedzenia plenarnego, które odbyło się 2 września 2020 r., Europejska Rada Ochrony Danych (EROD) przyjęła Wytyczne 7/2020, w których wyjaśnia pojęcia administratora, współadministratora i podmiotu przetwarzającego na gruncie RODO. Wytyczne zostały przekazane do konsultacji publicznych.

Uwagi wstępne

Choć RODO[1], podobnie jak dyrektywa 95/46/WE[2], posługuje się pojęciami administratora i podmiotu przetwarzającego, to od momentu rozpoczęcia stosowania RODO nie było jasne, w jakim stopniu wprowadziło ono zmiany w zakresie tych pojęć. W szczególności wątpliwości budziły pojęcie współadministrowania, o którym mowa w art. 26 RODO, oraz obowiązki podmiotów przetwarzających.

Warto podkreślić, że pojęcia administratora, współadministratora i podmiotu przetwarzającego odgrywają kluczową rolę w stosowaniu RODO – określają one, kto jest odpowiedzialny za zgodność przetwarzania danych osobowych z zasadami oraz w jaki sposób i wobec kogo osoby, których dane dotyczą, mogą wykonywać swoje uprawnienia z RODO.

EROD, wychodząc naprzeciw tym wątpliwościom i chcąc przyczynić się do zapewnienia spójnej interpretacji tych pojęć w ramach EOG, przyjęła przedmiotowe Wytyczne.

Nowe wytyczne składają się z dwóch głównych części:

- pierwsza część wyjaśnia pojęcia: administratora, współadministratora i podmiotu przetwarzającego;
- druga natomiast wyjaśnia główne konsekwencje przydzielenia roli administratora, współadministratora lub podmiotu przetwarzającego.

EROD podkreśla, że „administrator", „współadministrator" i „podmiot przetwarzający" to pojęcia **funkcjonalne**, co oznacza, że mają one na celu podział obowiązków zgodnie z rzeczywistą rolą stron, jak również **autonomiczne**, czyli powinny być interpretowane przede wszystkim zgodnie z unijnym prawem ochrony danych osobowych.

Pojęcie administratora danych

Zgodnie z art. 4 pkt 7 RODO „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

Administrator to podmiot, który decyduje o najważniejszych elementach przetwarzania. Określa cele i sposoby przetwarzania, czyli w jakim celu (dlaczego?) i w jaki sposób (jak?)

[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).
[2] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

dane osobowe są przetwarzane. Administrator musi decydować zarówno o celach, jak i o sposobach (środkach) przetwarzania, jednak niektóre bardziej praktyczne aspekty wdrożenia można pozostawić podmiotowi przetwarzającemu.

Jeśli chodzi o określenie środków, EROD dokonuje rozróżnienia między środkami istotnymi (essential means) i środkami innymi niż istotne (non-essential means). Środki istotne są ściśle powiązane z celem i zakresem przetwarzania i ich określanie jest zastrzeżone wyłącznie dla administratora. Przykłady takich środków obejmują określanie:

- rodzaju przetwarzanych danych osobowych („Jakie dane będą przetwarzane?");
- czasu trwania przetwarzania („Jak długo będą przetwarzane?");
- kategorii odbiorców („Kto ma do nich dostęp?");
- kategorii osób, których dane dotyczą („Czyje dane osobowe są przetwarzane?").

Środki inne niż istotne dotyczą bardziej praktycznych aspektów wdrożenia przetwarzania danych, takich jak wybór określonego typu sprzętu lub oprogramowania lub szczegółowe środki bezpieczeństwa, o których może decydować procesor.

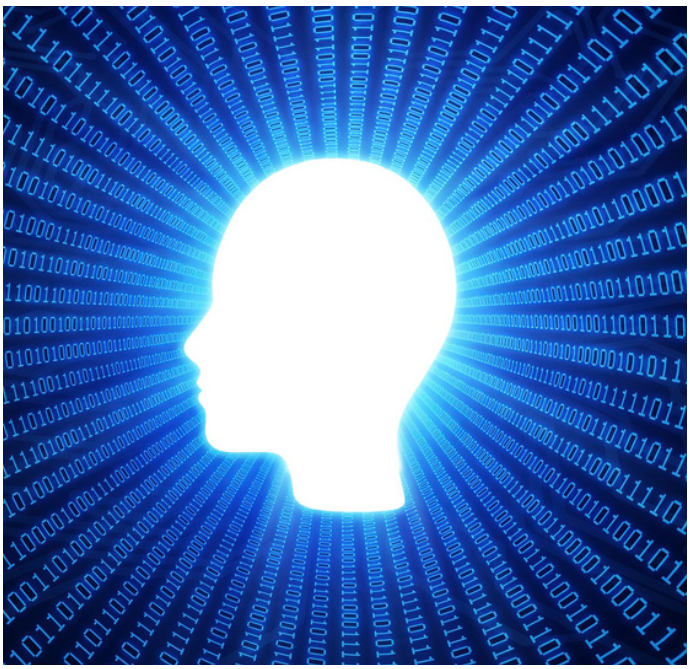
EROD zwraca jednak uwagę, że niezależnie od powierzenia przetwarzania administrator pozostaje odpowiedzialny za wdrożenie odpowiednich środków technicznych i organizacyjnych, aby zapewnić i móc wykazać, że przetwarzanie odbywa się zgodnie z RODO (art. 24). Czyniąc to, administrator musi wziąć pod uwagę charakter, zakres, kontekst i cele przetwarzania, a także ryzyko naruszenia praw i wolności osób fizycznych. Z tego powodu administrator musi być w pełni poinformowany o zastosowanych przez procesora środkach technicznych i organizacyjnych. Aby administrator był w stanie wykazać zgodność przetwarzania z prawem, zaleca się udokumentowanie przynajmniej niezbędnych środków technicznych i organizacyjnych w umowie lub w innym prawnie wiążącym instrumencie między administratorem a procesorem.

Administrowanie danymi może wynikać z ustawy bądź z analizy elementów faktycznych lub okoliczności sprawy. W wielu wypadkach warunki umowy mogą pomóc w identyfikacji administratora, chociaż nie można uznawać ich za decydujące we wszystkich okolicznościach. Innymi słowy – to, że umowa określa dany podmiot jako administratora danych, nie oznacza, że podmiot ten jest rzeczywiście administratorem.

W przypadku pewnych czynności przetwarzania administrowanie danymi można postrzegać jako naturalnie związane z rolą danego podmiotu (np. pracodawca względem pracowników, wydawca względem subskrybentów lub stowarzyszenie względem członków).

EROD wskazuje, że nie jest konieczne, aby administrator faktycznie miał dostęp do przetwarzanych danych osobowych, aby można było go uznać za administratora. Podmiot, który powierza czynności przetwarzania i czyniąc to, ma decydujący wpływ na określenie celu i (istotnych) sposobów przetwarzania, powinien być traktowany jako administrator, mimo że nigdy nie będzie miał faktycznego dostępu do danych.

EROD zauważa również, że zasadniczo nie ma ograniczeń co do rodzaju podmiotu, który może pełnić rolę administratora danych. W praktyce jednak będzie to zwykle organizacja jako taka, a nie osoba fizyczna w organizacji odpowiedzialna za podejmowanie pewnych decyzji (np. dyrektor generalny, pracownik lub członek zarządu).



Pojęcie podmiotu przetwarzającego

Podmiot przetwarzający to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Istnieją dwa podstawowe warunki uznania za podmiot przetwarzający: (1) odrębność od administratora i (2) przetwarzanie danych osobowych w imieniu administratora.

W grupie spółek jedna firma może być podmiotem przetwarzającym, a inna administratorem, ponieważ obie firmy są oddzielnymi podmiotami.

Jednocześnie dział w firmie nie może co do zasady być podmiotem przetwarzającym dla innego działu w ramach tego samego podmiotu.

Przetwarzanie danych osobowych w imieniu administratora wymaga przede wszystkim, aby odrębny podmiot przetwarzał dane osobowe na rzecz (na korzyść) administratora. Takie przetwarzanie musi się odbywać w imieniu administratora, ale inaczej niż pod jego bezpośrednim zwierzchnictwem lub kontrolą – działanie „w imieniu" oznacza służenie czyimś interesom i przypomina prawne pojęcie „delegowania".

Przetwarzanie „w imieniu" oznacza również, że podmiot przetwarzający nie może przetwarzać danych inaczej niż zgodnie z instrukcjami administratora. Instrukcje te mogą jednak pozostawić pewien stopień swobody co do tego, jak najlepiej służyć interesowi administratora, co umożliwia procesorowi wybór najbardziej odpowiednich środków technicznych i organizacyjnych.

Podmiot przetwarzający naruszy jednak RODO, jeśli wykroczy poza instrukcje administratora i zacznie określać własne cele i sposoby przetwarzania. Podmiot przetwarzający zostanie wówczas uznany za administratora w odniesieniu do tego przetwarzania i może podlegać sankcjom za wykraczanie poza instrukcje administratora.

EROD przypomina, że nie każdy usługodawca, który przetwarza dane osobowe w ramach świadczenia usługi, jest „podmiotem przetwarzającym" w rozumieniu RODO. Rola podmiotu przetwarzającego nie wynika z charakteru danego podmiotu, który przetwarza dane, ale z jego konkretnych działań podejmowanych w określonym kontekście.

To, czy dana działalność jest równoznaczna z przetwarzaniem danych osobowych w imieniu administratora, będzie zależało od charakteru danej usługi. EROD wskazuje, że w praktyce, gdy świadczona usługa nie jest ukierunkowana konkretnie na przetwarzanie danych osobowych lub gdy takie przetwarza-nie nie stanowi kluczowego elementu usługi, usługodawca może mieć możliwość samodzielnego określenia celów i środków tego przetwarzania, które są wymagane w celu świadczenia usługi. W takiej sytuacji usługodawcę należy postrzegać jako odrębnego administratora, a nie jako podmiot przetwarzający. EROD podkreśla jednak, że każdy przypadek przetwarzania trzeba oceniać odrębnie, aby ustalić rzeczywis-ty stopień wpływu, jaki każdy podmiot wywiera na określanie celów i sposobów przetwarzania

Relacja między administratorem a podmiotem przetwarzającym

Administrator może korzystać wyłącznie z podmiotów przetwarzających, które dają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi RODO (art. 28 ust. 1 RODO).

Elementami, które należy wziąć w tym zakresie pod uwagę, mogą być:

- wiedza ekspercka podmiotu przetwarzającego (np. wiedza techniczna w zakresie środków bezpieczeństwa i naruszeń danych);
- niezawodność procesora;
- zasoby procesora;
- przestrzeganie przez procesora zatwierdzonego kodeksu postępowania lub mechanizmu certyfikacji.

Przetwarzanie danych osobowych przez podmiot przetwarzający musi być regulowane umową lub innym instrumentem prawnym, który ma formę pisemną, w tym formę elektroniczną, i jest wiążący. Administrator i podmiot przetwarzający mogą się zdecydować na negocjowanie własnej umowy zawierającej wszystkie obowiązkowe elementy z art. 28 ust. 3 RODO bądź polegać w tym zakresie w całości lub w części na standardowych klauzulach umownych.

W odniesieniu do umowy powierzenia EROD wskazuje, że nie powinna ona jedynie powtarzać postanowień RODO, lecz zawierać bardziej szczegółowe, konkretne informacje, w jaki poziom bezpieczeństwa jest wymagany do przetwarzania danych osobowych będącego przedmiotem umowy powierzenia.

Pojęcie współadministratora danych

Kwalifikacja podmiotu jako współadministratora może wystąpić, jeżeli w przetwarzanie zaangażowany jest więcej niż jeden uczestnik. Zakwalifikowanie uczestników przetwarzania jako współadministratorów będzie miało konsekwencje przede wszystkim dla podziału obowiązków w celu zachowania zgodności z przepisami o ochronie danych osobowych, w szczególności odnoszących się do praw osób, których dane dotyczą.

Definicja z art. 4 pkt 7 RODO jest punktem wyjścia dla określenia współadministrowania. W związku z tym do rozważań dotyczących współadministrowania zastosowanie znajdują również informacje dotyczące zasad określania statusu administratora. Zgodnie z art. 26 ust. 1 zd. 1 RODO, „jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami". Innymi słowy współadministrowanie występuje w odniesieniu do konkretnych czynności przetwarzania, jeżeli różne strony określają wspólnie cele i sposoby przetwarzania.

„Wspólnie" należy interpretować jako „razem z" (together with) lub „nie samemu" (not alone). Ocena występowania współadministrowania powinna mieć charakter oceny stanu faktycznego, a nie formalnej analizy. Formalna ocena nie jest właściwa ze względu na to, że w niektórych przypadkach brak jest formalnego powołania współadministratora, określonego na przykład w przepisach prawa lub w umowie. W innych wypadkach może się natomiast zdarzyć, że formalne powołanie nie odzwierciedla faktycznych ustaleń poprzez formalne powierzenie roli administratora podmiotowi, który w rzeczywistości nie jest w stanie „określić" celów i sposobów przetwarzania.

Warto podkreślić, że nie każde przetwarzanie angażujące kilka podmiotów prowadzi do współadministrowania – powinno występować wspólne określanie celów i sposobów przetwarzania. Sytuacja wspólnego udziału w podejmowaniu zbieżnych decyzji wynika w szczególności z orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej (TSUE). Decyzje można uważać za zbieżne w odniesieniu do celów i środków, jeżeli podmioty się uzupełniają i są niezbędne w przetwarzaniu danych osobowych w taki sposób, że mają faktyczny wpływ na określanie celów i sposobów przetwarzania. Istotnym kryterium umożliwiającym ustalenie występowania zbieżnych decyzji jest to, czy przetwarzanie byłoby możliwe bez udziału obydwu stron w ten sposób, że przetwarzanie przez każdą ze stron jest nierozerwalnie związane.

To, że jedna ze stron nie ma dostępu do danych osobowych, nie jest wystarczające do wykluczenia współadministrowa-nia. Należy również podkreślić, że dany podmiot zostanie uznany za współadministratora tylko w odniesieniu do tych czynności przetwarzania, co do których wspólnie z innymi podmiotami określa cele i sposoby przetwarzania. Jeżeli jeden z podmiotów samodzielnie decyduje o celach i sposobach przetwarzania w odniesieniu do operacji przetwarzania, które poprzedzają łańcuch przetwarzania lub następują po nim, podmiot ten należy traktować jako wyłącznego administratora tej operacji poprzedzającej lub następującej. Występowanie współadministrowania nie oznacza równej odpowiedzialności różnych operatorów zaangażowanych w przetwarzanie danych osobowych. TSUE wyjaśnił, że operatorzy mogą być zaangażowani na różnych etapach przetwarzania i w różnym stopniu, co oznacza, że poziom odpowiedzialności każdego z operatorów musi być oceniany w świetle okoliczności określonej sprawy.

Wspólne określanie celów

Współadministrowanie występuje, gdy podmioty biorą udział w tych samych czynnościach przetwarzania dla wspólnie określonych celów. W przypadku gdy podmioty nie mają tego samego celu przetwarzania, współadministrowanie może występować, jeżeli cele przetwarzania są ściśle powiązane lub się uzupełniają. Taka sytuacja może zaistnieć w przypadku wspólnych korzyści wynikających z tego samego przetwarzania, jeżeli każdy z zaangażowanych podmiotów uczestniczy w określaniu celów i sposobów przetwarzania w odniesieniu do danej operacji przetwarzania.

W wyroku w sprawie Fashion ID wyjaśniono, że operator strony internetowej bierze udział przy określaniu celów przetwarzania poprzez umieszczenie wtyczki społecznościowej na swojej stronie internetowej w celu optymalizacji widoczności swoich towarów w mediach społecznościowych.

W sprawie Wirtschaftsakademie przetwarzanie danych osobowych poprzez statystyki osób odwiedzających fanpage miało na celu umożliwienie Facebookowi ulepszenia systemu reklam prezentowanych poprzez jego sieć oraz umożliwienie administratorowi fanpage'a uzyskania statystyk mających na celu zarządzanie aktywnością marketingową. Każdy z tych podmiotów miał własny interes, ale obydwie strony uczestniczą w określaniu celów przetwarzania danych osobowych osób odwiedzających fanpage.

Należy podkreślić, że występowanie wspólnych korzyści (np. gospodarczych) wynikających z przetwarzania danych osobowych nie prowadzi automatycznie do współadministrowania. Jeżeli podmiot zaangażowany w przetwarzanie danych nie osiąga własnych celów przetwarzania, ale jest opłacany za świadczone usługi, to będzie występować raczej jako podmiot przetwarzający, a nie współadministrator.

Wspólne określanie środków

Współadministrowanie wymaga również, aby przynajmniej dwa podmioty miały wpływ na środki przetwarzania. Nie oznacza to jednak, że każdy zaangażowany podmiot musi w każdym przypadku określać wszystkie sposoby przetwarzania. Różne podmioty mogą być zaangażowane na różnych etapach przetwarzania i w różnym stopniu. Może wystąpić sytuacja, w której jeden z podmiotów dostarcza środki przetwarzania i udostępnia je innym podmiotom na potrzeby czynności przetwarzania danych osobowych. Podmiot, który decyduje o wykorzystaniu danego środka przetwarzania, pozwala na przetwarzanie danych osobowych w konkretnym celu, uczestniczy również w określeniu środka przetwarzania. Taki scenariusz może się zdarzyć w przypadku platform, standardowych narzędzi lub innej infrastruktury umożliwiającej stronom przetwarzanie tych samych danych osobowych. Użycie obecnie funkcjonującego systemu nie wyklucza współadministrowania, jeżeli użytkownicy systemu decydują o przetwarzaniu danych osobowych w danym kontekście. Na przykład w wyroku w sprawie Wirtschaftsakademie TSUE uznał, że określanie przez administratora fanpage'a prowadzonego na Facebooku parametrów w postaci docelowych odbiorców oraz cele związane z zarządzaniem i promowaniem swojej działalności powinny być traktowane jako określanie sposobów przetwarzania w odniesieniu do odwiedzających fanpage. Wybór dokonany przez podmiot, polegający na wykorzystywaniu do własnych celów narzędzi lub systemu rozwijanego przez inny podmiot, umożliwiający przetwarzanie danych osobowych, prawdopodobnie będzie decyzją współadministratorów dotyczącą środków przetwarzania. Wynika to z wyroku w sprawie Fashion ID, w którym uznano, że zamieszczenie na stronie internetowej przycisku „Lubię to" udostępnionego przez Facebooka operatorom stron internetowych oznacza, że mają oni decydujący wpływ na operacje przetwarzania obejmujące zbieranie oraz przekazywanie danych osobowych osób odwiedzających stronę do Facebooka oraz wspólnie określają z Facebookiem środki przetwarzania. Należy jednak podkreślić, że korzystanie ze wspólnego systemu przetwarzania danych osobowych lub infrastruktury nie będzie we wszystkich przypadkach prowadziło do zakwalifikowania stron jako współadministratorów.

Relacje między współadministratorami

Zgodnie z art. 26 ust. 1 RODO „[w] drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z niniejszego rozporządzenia […]". Współadministratorzy muszą określić „kto co robi" (who does what) poprzez ustalenie, kto będzie wykonywał poszczególne zadania w celu zapewnienia zgodności z obowiązkami wynikającymi z RODO w odniesieniu do współadministrowania. Celem tych zasad jest zagwarantowanie, że wielu zaangażowanych uczestników przetwarzania będzie odpowiedzialnych za zapewnienie zgodności z zasadami ochrony danych osobowych, aby uniknąć sytuacji, w których ochrona danych osobowych jest obniżona lub ze względu na niejasny podział kompetencji dochodzi do luk w wykonywaniu obowiązków. Powinno być jasne, że odpowiedzialność została rozdzielona zgodnie z okolicznościami faktycznymi w celu osiągnięcia skutecznego porozumienia.

Współadministratorzy w porozumieniu powinni określić zakresy odpowiedzialności co do:

- wykonywania przez osobę, której dane dotyczą, przysługujących jej praw;
- podawania informacji, o których mowa w art. 13 i 14 RODO;
- wdrożenia podstawowych zasad ochrony danych (art. 5 RODO);
- podstaw prawnych przetwarzania (art. 6 RODO);
- środków bezpieczeństwa (art. 32 RODO);
- zgłaszania naruszenia ochrony danych organowi nadzorczemu (art. 33 RODO) oraz zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych (art. 34 RODO);
- oceny skutków dla ochrony danych (art. 34 i 36 RODO);
- wykorzystania podmiotu przetwarzającego (art. 28 RODO);
- transferu danych osobowych do państw trzecich (Rozdział V);
- organizacji kontaktu z podmiotem danych i organami nadzorczymi

Należy pamiętać, że przy podziale odpowiedzialności pomiędzy współadministratorów trzeba wziąć pod uwagę takie czynniki, jak: posiadane przez podmiot kompetencje, możliwość efektywnego zapewnienia praw podmiotów danych oraz wykonywania innych obowiązków na gruncie RODO. EROD rekomenduje dokumentowanie ww. czynników oraz wewnętrznej analizy przeprowadzonej w celu podziału obowiązków.

Taka analiza jest częścią dokumentacji zgodnie z zasadą rozliczalności. Obowiązki współadministratorów nie muszą być jednak rozdzielone jednakowo (po równo).

Mogą wystąpić sytuacje, w których nie wszystkie obowiązki zostaną rozdzielone pomiędzy współadministratorów i każdy z nich musi zapewniać zgodność z tymi samymi wymaganiami wynikającymi z RODO ze względu na naturę i kontekst przetwarzania objętego współadministrowaniem. Na przykład współadministratorzy wykorzystujący dzielone narzędzia lub systemy do przetwarzania danych osobowych muszą zapewniać zgodność z zasadą ograniczenia celu przetwarzania oraz wdrożyć odpowiednie środki, aby zapewnić bezpieczeństwo danych osobowych przetwarzanych we współdzielonym narzędziu. Ponadto każdy ze współadministratorów jest zobowiązany do prowadzenia rejestru czynności przetwarzania oraz wyznaczenia inspektora ochrony danych, jeżeli jest to wymagane na podstawie art. 37 ust. 1 RODO. Te obowiązki nie odnoszą się do wspólnego przetwarzania, lecz są właściwe dla tych podmiotów jako administratorów.

RODO nie określa wymogu co do formy uzgodnień pomiędzy współadministratorami. Jednakże EROD rekomenduje zawarcie takich ustaleń w formie wiążącego dokumentu, takiego jak umowa lub inny akt prawny, którego stronami są administratorzy. Takie działania zapewniają transparentność i rozliczalność. W przypadku niewykonywania przez współadministratorów obowiązków zgodnie z przyjętymi ustaleniami takie działania umożliwiają pociągnięcie drugiego współadministratora do odpowiedzialności. Ustalenia powinny być zawarte jasnym i prostym językiem, aby zapewnić pewność prawa oraz uniknąć potencjalnych konfliktów z pozostałymi współadministratorami, jak również z podmiotami danych oraz organami nadzorczymi.

EROD zaleca też, aby w uzgodnieniach zawrzeć także ogólne informacje o wspólnym przetwarzaniu, takie jak: przedmiot oraz cel przetwarzania, typ danych osobowych oraz kategorie podmiotów danych.

RODO zobowiązuje również współadministratorów do wykonywania następujących obowiązków względem podmiotów danych:

- uzgodnienia powinny odzwierciedlać odpowiednie role i relacje współadministratorów w stosunku do osób, których dane dotyczą;
- istota uzgodnień jest udostępniana osobie, której dane dotyczą;
- w uzgodnieniach można wyznaczyć punkt kontaktowy dla osób, których dane dotyczą;
- niezależnie od warunków uzgodnień osoby, których dane dotyczą, mogą wykonywać przysługujące im prawa w stosunku do każdego ze współadministratorów.

Przykłady z Wytycznych EROD

Administrowanie wynikające z przepisów prawa. Prawo krajowe w państwie A nakłada na władze gminne obowiązek zapewnienia obywatelom świadczeń socjalnych, takich jak miesięczne wypłaty, w zależności ich sytuacji finansowej tych osób. Aby dokonać tych płatności, władze gminne muszą zebrać i przetwarzać dane o sytuacji finansowej wnioskodawców. Chociaż prawo nie stanowi wyraźnie, że administratorem w tym zakresie są władze gminne, wynika to w sposób dorozumiany z przepisów prawa.

Kancelaria prawna jako administrator. W przypadku gdy firma zleca kancelarii prawnej reprezentowanie jej w sporze, kancelaria jest administratorem danych osobowych przetwarzanych w związku ze sprawą. W celu prawidłowej realizacji tego zadania kancelaria musi przetwarzać dane osobowe związane ze sprawą, a podstawą przetwarzania danych osobowych jest upoważnienie udzielone kancelarii do reprezentowania klienta w sądzie. Upoważnienie to nie jest jednak konkretnie ukierunkowane na przetwarzanie danych osobowych, lecz na prowadzenie sprawy. Kancelaria działa z dużym stopniem niezależności, na przykład decydując o tym, jakich informacji użyć i jak z nich korzystać w danej sprawie, a klient nie udziela kancelarii żadnych instrukcji dotyczących przetwarzania danych osobowych.

Przetwarzanie, którego kancelaria prawna dokonuje w celu wypełnienia funkcji pełnomocnika spółki, jest zatem powiązane z funkcjonalną rolą kancelarii, stąd należy ją traktować jako administratora danych przetwarzanych w tym zakresie.

Administrowanie płacami. Pracodawca A zatrudnia inną firmę do zarządzania wypłatą wynagrodzeń swoim pracownikom. Pracodawca A daje jasne instrukcje, komu zapłacić, jakie kwoty, w jakim terminie, w jakim banku, jak długo dane będą przechowywane, jakie dane należy ujawnić organowi podatkowemu itp. W takim przypadku przetwarzanie danych odbywa się w przyjętym przez firmę A celu, jakim jest wypłata wynagrodzeń jej pracownikom, a administrator listy płac nie może wykorzystywać danych do żadnych własnych celów. Sposób, w jaki administrator listy płac powinien dokonywać przetwarzania, jest w istocie jasno i ściśle określony. Niemniej administrator listy płac może decydować o pewnych szczegółowych kwestiach związanych z przetwarza-niem, takich jak: jakiego oprogramowania użyć, jak i komu udzielić dostępu do danych w ramach własnej organizacji itp. Nie zmienia to roli administratora listy płac jako **podmiotu przetwarzającego**, o ile nie będzie on przetwarzał danych w sposób sprzeczny lub wykraczający poza instrukcje wydane przez firmę A.

Księgowi. Pracodawca zatrudnia firmę księgową do przeprowadzania audytów księgowości i w związku z tym przekazuje dane o transakcjach finansowych (w tym dane osobowe) do firmy księgowej. Przetwarza ona te dane bez szczegółowych instrukcji od pracodawcy. Firma księgowa decyduje sama, zgodnie z przepisami prawa regulującymi czynności audytowe prowadzone przez firmę księgową, że zgromadzone przez nią dane będą przetwarzane wyłącznie w celu przeprowadzenia audytu pracodawcy, oraz określa, jakie dane musi posiadać, jakich kategorii osób, w jaki sposób, jak długo dane będą przechowywane i jakich środków technicznych należy użyć. W tych okolicznościach firmę księgową należy traktować jako samodzielnego **administratora** wykonującego usługi audytorskie na rzecz pracodawcy. Jednakże ocena ta może być inna w zależności od poziomu instrukcji przedstawionych przez pracodawcę i przepisów regulujących działalność księgową.

W sytuacji, gdy prawo nie przewiduje szczególnych obowiązków dla firmy księgowej i klient dostarcza szczegółowych instrukcji dotyczących przetwarzania, firma księgowa mo-głaby zostać uznana za **podmiot przetwarzający**.

Usługi hostingowe. Pracodawca A zatrudnia firmę hostingową H do przechowywania zaszyfrowanych danych na serwerach firmy H. Firma hostingowa H nie ustala, czy dane, które przechowuje, są danymi osobowymi, ani nie przetwarza danych w żaden inny sposób niż przechowywanie ich na swoich serwerach. W tym zakresie firma hostingowa H przetwarza (przechowuje) dane osobowe w imieniu pracodawcy A i jest **podmiotem przetwarzającym.** Pracodawca A musi przekazać firmie hostingowej H niezbędne instrukcje, na przykład jakie techniczne i organizacyjne środki bezpieczeństwa są wymagane, a także musi zostać zawarta umowa powierzenia przetwarzania danych zgodnie z art. 28 RODO.

Badania rynku. Firma ABC chce się dowiedzieć, jakie typy konsumentów są najbardziej zainteresowane jej produktami i zawiera umowę z usługodawcą XYZ w celu uzyskania odpowiednich informacji. Firma ABC instruuje XYZ, jakie informacje ją interesują, i podaje listę pytań, które należy zadać uczestnikom badania rynku. Firma ABC otrzymuje wyłącznie informacje statystyczne (na przykład identyfikujące trendy konsumenckie w poszczególnych regionach) od XYZ i nie ma dostępu do samych danych osobowych. Niemniej to firma ABC zadecydowała, że będzie dochodziło do przetwarzania, i odbywa się ono w określonym przez nią celu i w ramach prowadzonej przez nią działalności, a także przekazała XYZ szczegółowe instrukcje dotyczące gromadzenia informacji. W związku z tym firmę ABC należy uważać za **administratora** w odniesieniu do przetwarzania danych osobowych, które ma miejsce w celu dostarczenia żądanych przez nią informacji. XYZ może przetwarzać dane wyłącznie w celu wskazanym przez firmę ABC i zgodnie z jej szczegółowymi instrukcjami, dlatego XYZ należy traktować jako **podmiot przetwarzający. Nie jest zatem konieczne, aby administrator miał dostęp do przetwarzanych danych osobowych, aby uznać go za administratora danych.**

Usługodawca określany jako podmiot przetwarzający dane, ale działający jako administrator. Usługodawca X świadczy usługi reklamy promocyjnej i marketingu bezpośredniego różnym firmom. Firma Z zawiera z X umowę, zgodnie z którą ta ostatnia firma ma świadczyć usługi reklamowe dla klientów firmy Z i jest określana jako podmiot przetwarzający dane. Jednak firma X decyduje się na wykorzystanie bazy klientów firmy Z również do innych celów, takich jak rozwój własnej działalności gospodarczej. Decyzja o dodaniu dodatkowego celu do tego, w jakim dane osobowe zostały przekazane, zmienia firmę X w **administratora** danych dla tego zestawu operacji przetwarzania, a przetwarzanie danych w tym celu stanowi naruszenie RODO.

Ogólne wsparcie IT. Firma Z zatrudnia dostawcę usług IT do świadczenia ogólnego wsparcia w zakresie swoich systemów informatycznych, które zawierają ogromną ilość danych osobowych. Dostęp do nich nie jest głównym przedmiotem usługi wsparcia, ale nieuniknione jest, że dostawca usług IT ma systematyczny dostęp do danych osobowych podczas wykonywania usługi. Firma Z stwierdza zatem, że dostawca usług IT – będący odrębną firmą nieuchronnie zobowiązaną do przetwarzania danych osobowych (mimo że nie jest to głównym celem usługi) – ma być traktowany jako podmiot przetwarzający. W związku z tym zostaje zawarta umowa powierzenia z dostawcą usług IT.

Konsultant IT naprawiający błąd oprogramowania. Firma ABC zatrudnia specjalistę IT z innej firmy, aby naprawić błąd w oprogramowaniu używanym przez firmę. Specjalista IT nie jest zatrudniony do przetwarzania danych osobowych, a firma ABC ustaliła, że jakikolwiek dostęp do nich będzie miał charakter czysto przypadkowy i dlatego w praktyce będzie bardzo ograniczony. ABC stwierdza zatem, że specjalista IT nie jest podmiotem przetwarzającym (ani administratorem we własnym imieniu) i że spółka ABC podejmie odpowiednie środki zgodnie z art. 32 RODO, aby uniemożliwić konsultantowi IT przetwarzanie danych osobowych w nieautoryzowany sposób.

Dostawca usług chmurowych jako podmiot przetwarzający. Gmina zdecydowała się skorzystać z usług dostawcy usług chmurowych do obsługi informacji w swoich usługach szkolnych i edukacyjnych. Usługa chmurowa obejmuje zarówno usługi przesyłania wiadomości, wideo-konferencje, przechowywanie dokumentów, zarządzanie kalendarzem, przetwarzanie tekstu itp., jak i przetwarzanie danych osobowych uczniów i nauczycieli. Dostawca usług chmurowych oferuje ustandaryzowaną usługę na całym świecie. Gmina musi się jednak upewnić, że obowiązująca umowa jest zgodna z art. 28 ust. 3 RODO, a dane osobowe, których jest administratorem, są przetwarzane wyłącznie do celów gminy.

Musi ona również sprawdzić, czyjej szczegółowe instrukcje dotyczące okresów przechowywania, usuwania danych itp. są przestrzegane przez dostawcę usług chmurowych, niezależnie od tego, co jest ogólnie oferowane w ramach ustandaryzowanej usługi.

Działania marketingowe. Firmy A i B wprowadziły na rynek produkt C pod wspólną marką i chcą zorganizować wydarzenie promujące ten produkt. W tym celu decydują się na udostępnienie danych z bazy swoich klientów i potencjalnych klientów i na tej podstawie ustalają listę osób zaproszonych na wydarzenie. Uzgadniają również sposoby wysyłania zaproszeń na wydarzenie, zbierania informacji zwrotnych podczas wydarzenia i dalszych działań marketingowych. Firmy A i B można uznać za **współadministratorów** w zakresie przetwarzania danych osobowych związanych z organizacją imprezy promocyjnej, ponieważ razem decydują o wspólnie określonym celu i podstawowych środkach prze-twarzania danych w tym kontekście.

Headhunterzy. Firma X pomaga firmie Y w rekrutacji nowego personelu – dzięki swojej słynnej usłudze o wartości dodanej „global matchz". Firma X szuka odpowiednich kandydatów zarówno wśród CV otrzymanych bezpośrednio od firmy Y, jak i wśród tych, które ma już we własnej bazie danych. Taka baza danych jest tworzona i zarządzana samodzielnie przez firmę X. Mimo że formalnie firmy X i Y nie podjęły wspólnie decyzji, razem uczestniczą w przetwarzaniu w celu znalezienia odpowiednich kandydatów na podstawie zbieżnych decyzji: decyzji o utworzeniu usługi „global matchz" i zarządzaniu nią na korzyść firmy X oraz decyzji firmy Y o wzbogaceniu bazy danych o CV, które otrzymuje bezpośrednio. Decyzje takie wzajemnie się uzupełniają, są nierozłączne i niezbędne do przeprowadzenia procesu poszukiwania odpowiednich kandydatów. Dlatego w tym konkretnym przypadku firmy te należy uznać za współadministratorów takiego przetwarzania. Niemniej firma X jest wyłącznym administratorem przetwarzania niezbędnego do zarządzania swoją bazą danych, a firma Y jest wyłącznym administratorem w zakresie dalszego przetwarzania danych do własnych celów związanych z zatrudnieniem (organizacja rozmów, zawarcie umowy i zarządzanie danymi kadrowymi).

Usługi porządkowe. Firma A zawiera umowę z firmą świadczącą usługi sprzątania na sprzątanie swoich biur. Osoby sprzątające nie mają dostępu do danych osobowych ani nie przetwarzają ich w inny sposób. Chociaż mogą czasami napotkać takie dane podczas przemieszczania się po biurze, mogą wykonywać swoje zadanie bez dostępu do nich i mają umowny zakaz uzyskiwania dostępu do danych lub innego przetwarzania danych osobowych, które firma A przetwarza jako administrator. Osoby sprzątające nie są zatrudnione przez firmę A ani nie są postrzegane jako podlegające bezpośrdenio tej firmie.

Firma A jako administrator nie ma zamiaru angażować firmy sprzątającej ani jej pracowników do przetwarzania danych osobowych w swoim imieniu. W związku z tym firma świadcząca usługi sprzątania i jej pracownicy powinni być postrzegani jako strona trzecia w rozumieniu art. 4 pkt 10 RODO, a administrator musi się upewnić, że istnieją odpowiednie środki bezpieczeństwa, aby uniemożliwić tym osobom dostęp do danych, i ustanowić obowiązek zachowania poufności w sytuacji, gdyby osoby sprzątające przypadkowo natrafiły na dane osobowe.

Źródło: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en.

Dodatkowe środki ochrony w przypadku transferu danych osobowych do państwa trzeciego na podstawie standardowych klauzul umownych lub wiążących reguł korporacyjnych

adw. Xawery Konarski, Starszy Partner

W wydanym 16 lipca 2020 r. wyroku w sprawie Schrems II (C-311/18) Trybunał Sprawiedliwości Unii Europejskiej (TSUE) potwierdził, że standardowe klauzule umowne, o których mowa w art. 46 ust. 2 pkt c RODO[1], nadal stanowią – co do zasady – ważny instrument transferu danych, na podstawie którego można dokonywać transferu danych do państwa trzeciego, w tym do Stanów Zjednoczonych. Równocześnie jednak Trybunał podkreślił, że stosowanie standardowych klauzul może się okazać niewystarczającym mechanizmem transferowym. Będzie tak w szczególności wówczas, gdy dokonana przez Komisję Europejską, krajowy organ nadzorczy lub też samego eksportera danych analiza odpowiedniości ochrony w państwie trzecim da wynik negatywny. W takim wypadku eksporter danych zobowiązany jest do podjęcia „dodatkowych środków" mających na celu zapewnienie przestrzegania odpowiedniego stopnia ochrony danych w państwie trzecim (motyw 133 wyroku w sprawie Schrems II). W artykule wyjaśniamy, jakie dodatkowe środki ochrony może przedsięwziąć eksporter danych.

Wstęp

W pkt 10 dokumentu z dnia 24 lipca 2020 r. pt. Najczęstsze pytania dotyczące wyroku Trybunału Sprawiedliwości Unii Europejskiej C-311/18 (Schrems II) Europejska Rada Ochrony Danych (EROD) dokonała podziału dodatkowych zabezpieczeń na trzy rodzaje: prawne, organizacyjne oraz techniczne. Obecnie w EROD trwają prace nad stworzeniem katalogu środków tego rodzaju. Z uwagi jednak na to, że wyrok w sprawie Schrems II jest wykonalny od dnia jego wydania, eksporterzy danych już teraz muszą podejmować decyzje, czy i jakie dodatkowe zabezpieczenia stosować. Warto w związku z tym dokonać przeglądu środków tego rodzaju, których podjęcie jest rozważane w tzw. praktyce obrotu. Obecnie bowiem tylko jeden organ nadzorczy opublikował taką listę.

Przed przystąpieniem do analizy „dodatkowych środków ochrony" warto poczynić trzy uwagi o charakterze ogólnym. Po pierwsze, dodatkowe środki mają zastosowanie w sytuacji, w której dane osobowe mogą być przetwarzane poza Unią Europejską (UE) i/lub Europejskim Obszarem Gospodarczym (EOG) w państwach nieobjętych decyzjami Komisji Europejskiej o odpowiedniej ochronie danych osobowych (art. 4 RODO). Po drugie, propozycje dodatkowych zabezpieczeń znajdują zastosowanie jako uzupełnienie standardowych klauzul umownych / standardowych klauzul ochrony, o których mowa w art. 46 ust. 2 pkt c RODO, a także wiążących reguł korporacyjnych (art. 46 ust. 2 pkt b). Po trzecie, eksporterem danych w poniższym rozumieniu jest zarówno administrator, jak i podmiot przetwarzający przekazujący z terytorium Unii Europejskiej (Europejskiego Obszaru Gospodarczego) dane osobowe do państwa trzeciego (art. 44 RODO), a importerem danych jest podmiot, który dane te przetwarza w państwie trzecim.

Dodatkowe środki prawne ochrony danych osobowych

Propozycje dodatkowych środków prawnych można podzielić na dwie podstawowe grupy.

Pierwsza z nich ma na celu zwiększenie kontroli procesu transferu przez osoby, których dane są przekazywane. Chodzi w szczególności o świadomość potencjalnego ryzyka z tym związanego, określanego jeszcze przed skorzystaniem przez podmioty danych z usług oferowanych przez eksportera, a z którymi to związany jest transfer danych osobowych do państwa trzeciego. W tym kontekście eksporter danych może rozważyć dodatkowe informowanie podmiotu danych o tym, że jego dane mogą zostać objęte transferem, oraz o potencjalnym ryzyku z tym związanym. Środkiem prawnym tego rodzaju jest również wprowadzenie obowiązku eksportera danych do pozyskiwania zgody na przekazywanie danych do państwa trzeciego niezapewniającego odpowiedniego poziomu ochrony.

[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).

Druga grupa środków prawnych polega na wprowadzeniu w umowie pomiędzy eksporterem i importerem danych postanowień, mających na celu z jednej strony zapewnienie większej transparentności w zakresie przetwarzania danych przez importera, a z drugiej – jego odpowiedniego współdziałania z eksporterem danych. Do tego rodzaju postanowień należy zaliczyć klauzule, zgodnie z którymi importer nie ma dostępu do danych, o ile nie jest to niezbędne do należytego świadczenia usługi, a dostęp do nich będzie ograniczony wyłącznie do osób upoważnionych przez importera do przetwarzania danych osobowych. Zobowiąza-nie to ma dotyczyć również podwykonawców, którymi posługuje się importer. Podobny charakter ma zobowiązanie, że dostępu do danych nie mają także osoby trzecie, chyba że wynika to z przepisów prawa. W przypadku natomiast, gdy obowiązek ujawnienia danych osobom trzecim wynika z przepisów prawa obowiązujących importera danych, jest on zobowiązany do poinformowania o tym eksportera przed ujawnieniem danych osobowych, chyba że takie powiadomienie jest zabronione przez prawo. Gdy w państwie trzecim obowiązuje zakaz prawny niezwłocznego powiadomienia eksportera o ujawnieniu danych, do przekazania informacji, np. o udostępnieniu danych służbom wywiadowczym, dochodzi po upływie ustawowego lub sądowego zakazu ujawniania tej informacji.

Dodatkowe środki organizacyjne ochrony danych

Istotna część środków organizacyjnych zabezpieczenia danych związana jest z dokonaniem szacowania ryzyka ich transferu do danego państwa trzeciego / danego importera danych. Stanowi ona refleks nadrzędnej w RODO zasady risk-based approach.

W powyższym kontekście zalecić należy dokonanie klasyfikacji danych objętych transferem i dostosowanie środków ochrony do rodzajów danych, które mają być przekazane do państwa trzeciego. Na przykład za mniej ryzykowny uważa się transfer danych kontaktowych niż danych wrażliwych. W tym kontekście eksporter danych powinien mieć również zapewniony dostęp do informacji, jakie dane mogą być przetwarzane przez importera poza Unią Europejską (Europejskim Obszarem Gospodarczym) lub jakiego rodzaju usługi mogą być świadczone w państwie trzecim. Istotne jest także pozyskanie informacji, czy poza Europejskim Obszarem Gospodarczym dokonywane jest całe przetwarzanie związane z daną czynnością przetwarzania, czy też tylko jej element (np. wsparcie techniczne).

Na potrzeby dokonywania szacowania ryzyka szczególne znaczenie może mieć też pozyskiwanie od importera różnego rodzaju informacji o żądaniach dostępu do danych otrzymywanych przez importera od organów państwowych w danym państwie trzecim (np. statystyki i zakres żądań dostępu do danych otrzymywanych przez importera) pod kątem ustalenia, że dane określonego rodzaju (np. pracownicze) nie stanowią przedmiotu szczególnego zainteresowania organów z państw trzecich. Warto więc zobowiązać importera danych do przekazywania wszystkich informacji niezbędnych eksporterowi do oszacowania ryzyka transferu danych do państwa trzeciego, w którym dojdzie do przetwarzania danych przez importera oraz podwykonawców, którymi się on posługuje.

Dla oceny ryzyka przetwarzania danych przez konkretnego importera danych istotne może być podanie przez niego zasad postępowania z przekazanymi danymi. Chodzi w szczególności o stosowane (wdrożone) zasady zarządzania bezpieczeństwem informacji przez importera, np. dysponowanie certyfikatami związanymi z ochroną informacji (ISO 27001 i inne).

Wykonanie powyższego szacowania ryzyka i klasyfikacji danych, które potencjalnie mogą być transferowane, pozwala z kolei na rozważenie zastosowania kolejnego środka organizacyjnego, jakim jest ewentualna minimalizacja zakresu danych objętych transferem. W przypadku usług chmury obliczeniowej do środków tego rodzaju zaliczyć można wybór modelu chmury hybrydowej, w ramach którego w chmurze publicznej przetwarzane są dane „mniej krytyczne" dla eksportera danych.

Dodatkowe środki techniczne ochrony danych

Szczególnie istotnym środkiem technicznym zwiększającym bezpieczeństwo danych jest ich szyfrowanie, zarówno w stanie spoczynku (in rest), jak i podczas transferu (in transit). Powinno ono być wykonywane zgodnie z odpowiednimi normami ISO.

O wyborze formy szyfrowania powinny decydować wyniki dokonanej analizy szacowania ryzyka związanego z transferem. Warto w związku z tym rozważyć, czy szyfrowanie powinno odbywać się tylko za pomocą narzędzi importera danych, czy też stosować podwójne szyfrowanie, zarówno przez eksportera, jak i przez importera danych – względnie wyłącznie szyfrowanie za pomocą własnego klucza eksportera danych.

Do innych środków technicznych ochrony danych zaliczyć można również maskowanie adresów IP, wykorzystanie funkcji skrótu (funkcji haszującej) polegającej na przypisaniu określonemu ciągowi liczb w numerze innego krótkiego numeru, tak aby dane były w praktyce nieprzydatne dla podmiotu innego niż eksporter danych.

Wytyczne EROD dot. targetowania w mediach społecznościowych

r.pr. Dominika Nowak

Podczas 37. posiedzenia plenarnego, które odbyło się 2 września 2020 r., Europejska Rada Ochrony Danych (EROD) przyjęła Wytyczne 8/2020 w sprawie targetowania użytkowników mediów społecznościowych (dalej: Wytyczne), w których wyjaśnia zasady oraz dopuszczalny zakres takiego działania. Wytyczne zostały przekazane do konsultacji publicznych.

Uwagi wstępne

W związku z rozwojem mediów społecznościowych coraz więcej osób fizycznych korzysta z nich do kontaktowania się z rodziną i przyjaciółmi, do budowania relacji biznesowych lub też do rozwijania swoich zainteresowań. Na potrzeby Wytycznych EROD przez media społecznościowe rozumie platformy internetowe, które umożliwiają rozwój sieci i społeczności użytkowników i w ramach których dochodzi do dzielenia się informacjami i treściami. Usługi targetowania umożliwiają osobom fizycznym i prawnym (targeters) przekazywanie użytkownikom mediów społecznościowych wiadomości zbliżonych do ich zainteresowań. Podstawowym założeniem jest to, że im lepsze dopasowanie treści, tym wyższy współczynnik odbioru (konwersja), a tym samym skuteczniejsza kampania targetowania (zwrot z inwestycji). Targetowanie użytkowników odbywa się na podstawie różnorakich kryteriów. Mogą one być określane na podstawie danych osobowych dostarczanych aktywnie przez użytkowników, takich jak np. status związku. Kryteria mogą być również oparte na danych zaobserwowanych (observed data) oraz danych wywnioskowanych (inferred data) przez dostawcę mediów społecznościowych lub osoby trzecie, a następnie zebranych przez platformę lub innych uczestników (np. data brokerów), aby wspierać opcje targetowania reklamowego (ad-targeting).

Zakres Wytycznych

W targetowaniu w mediach społecznościowych uczestniczy wiele różnorodnych podmiotów. Na potrzeby Wytycznych podzielono te podmioty na cztery kategorie:

1. Dostawcy mediów społecznościowych (social media providers).
2. Użytkownicy (users).
3. Targetujący (targeters).
4. Inne podmioty, które mogą być zaangażowane w proces targetowania.

Istotność przyporządkowania właściwych ról i odpowiedzialności została podkreślona w dwóch orzeczeniach TSUE: w sprawie Wirtschaftsakademie i w sprawie Fashion ID[1].

Biorąc pod uwagę orzecznictwo TSUE oraz przepisy RODO dotyczące współadministrowania oraz rozliczalności, Wytyczne skupiają się na targetowaniu użytkowników w mediach społecznościowych, w szczególności na określaniu odpowiedzialności dostawców mediów społecznościowych oraz targetujących. Jeżeli występuje współadministrowanie, to Wytyczne wyjaśniają na podstawie praktycznych przykładów, jak może wyglądać podział odpowiedzialności pomiędzy dostawców mediów społecznościowych oraz targetujących.

[1] Wyrok TSUE z dnia 5 czerwca 2018 r. w sprawie C-210/16 Wirtschaftsakademie, ECI:EU:C:2018:388; wyrok TSUE z dnia 29 lipca 2019 r. w sprawie C-40/17 Fashion ID, ECLI:EU:C:2019:629.

Wytyczne składają się z następujących części:

1. Identyfikacja potencjalnych ryzyk dla praw lub wolności osób fizycznych, takich jak wykorzystywanie danych osobowych przeciwko osobom fizycznym lub poza nimi, dyskryminacja i wykluczenie, manipulacja użytkownikami, wpływanie na zachowanie użytkowników w ramach dyskursu politycznego oraz w trakcie demokratycznych wyborów.

2. Zdefiniowanie pojęć dostawców mediów społecznościowych, użytkowników, targetujących (targeters) oraz innych podmiotów, które mogą być zaangażowane w proces targetowania.

3. Analiza poszczególnych mechanizmów targetowania na podstawie danych dostarczonych aktywnie przez użytkownika do dostawcy mediów społecznościowych lub targetującego, na podstawie danych zaobserwowanych oraz danych wywnioskowanych. W ramach każdego z mechanizmów targetowania określono występujące role oraz podstawy prawne przetwarzania.

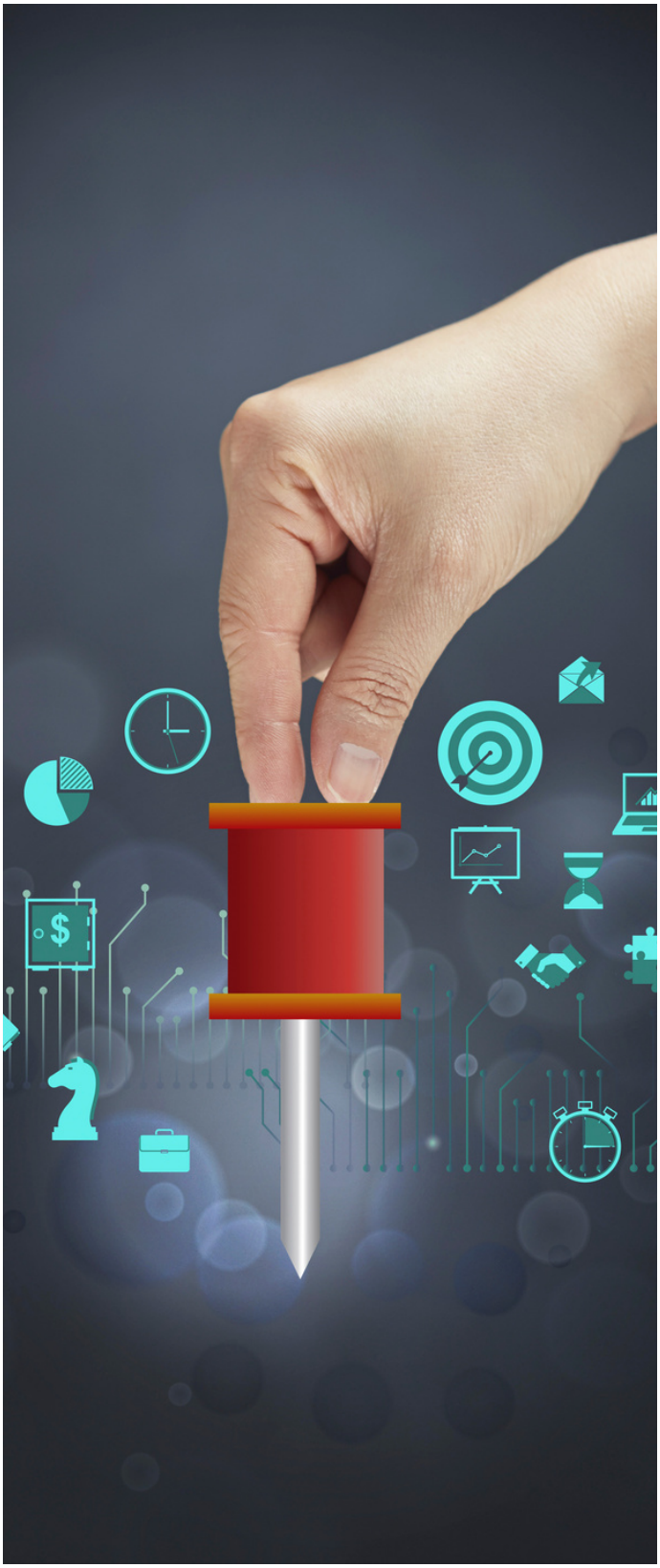
4. Analiza zasady transparentności oraz prawa dostępu w kontekście korzystania z mediów społecznościowych.

5. Kryteria przeprowadzenia oceny skutków dla ochrony danych.

6. Znaczenie występowania szczególnych kategorii danych w procesie targetowania.

7. Znaczenie występowania współadministrowania w procesie targetowania.

Europejska Rada Ochrony Danych przyjmuje uwagi do Wytycznych 8/2020 w sprawie targetowania użytkowników mediów społecznościowych do 19 października 2020 r.



Źródło:
https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-082020-targeting-social-media-users_en.

Wytyczne irlandzkiego organu nadzorczego dotyczące niechcianych lub utraconych danych

Mateusz Kupiec

Częstym problemem z zakresu ochrony danych osobowych, z jakim muszą się mierzyć administratorzy danych, jest sytuacja, gdy otrzymują oni dane osobowe, których nie planowali przetwarzać. W trakcie wykonywania codziennych czynności w organizacji może również dojść do przypadkowej utraty przez administratora kontroli nad przetwarzanymi informacjami dotyczącymi osób fizycznych. Irlandzki organ nadzorczy – Komisarz ds. ochrony danych – niedawno opublikował wytyczne dotyczące wskazanych problemów. Przedstawiamy najważniejsze ustalenia organu.

Wytyczne dla organizacji, które przypadkowo otrzymały dane osobowe

Irlandzki Komisarz ds. ochrony danych (dalej także: Komisarz lub DPC) zauważa, że w związku ze wzrostem ilości informacji, jakie są codziennie wytwarzane, coraz bardziej prawdopodobne jest przypadkowe uzyskanie przez różne podmioty dostępu do danych dotyczących osób fizycznych. Organ przypomina, że nawet w takiej sytuacji konkretny podmiot przetwarza dane osobowe w rozumieniu RODO i jako ich administrator musi działać zgodnie z przepisami rozporządzenia.

Podmiotom, które otrzymały niechciane dane osobowe, Komisarz zaleca:

- w przypadku otrzymania niechcianych danych osobowych poprzez wiadomość e-mail udzielenie niezwłocznej odpowiedzi na taką wiadomość oraz trwałe usunięcie załączników (bez otwierania ich);
- w przypadku otrzymania błędnie zaadresowanego listu albo przesyłki dokonanie identyfikacji nadawcy poprzez np. oznaczenia na kopercie;
- w przypadku otrzymania informacji, które mają zostać odzyskane przez właściwego administratora, przechowywanie ich w bezpiecznym miejscu;
- kontakt z organem nadzorczym w przypadku braku możliwości identyfikacji podmiotu, od którego konkretny administrator otrzymał niechciane dane.

Wytyczne dla administratorów, którzy utracą kontrolę nad danymi osobowymi na rzecz strony trzeciej

Zgodnie z art. 4 pkt 10 RODO „strona trzecia" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe. DPC zauważa, że nie wszystkie podmioty, które uzyskały dostęp do utraconych danych osobowych, będą chętne do współpracy w przypadku prośby administratora o zwrot lub usunięcie tych informacji. Niemniej nawet wtedy administrator danych osobowych nie zostaje zwolniony z obowiązków wynikających z RODO.

[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; dalej: RODO).

Zdaniem Komisarza ds. ochrony danych administrator, który utracił kontrolę nad danymi, poza zgłoszeniem naruszenia powinien także:

- poinformować stronę trzecią, która weszła w posiadanie danych osobowych, że przetwarza je ona bez podstawy prawnej, co stanowi naruszenie praw podmiotów danych;
- skonsultować się ze swoimi doradcami prawnymi co do środków zaradczych, z których może skorzystać;
- rozważyć zawiadomienie Policji.

Komentarz

Wytyczne irlandzkiego organu nadzorczego stanowią cenne wskazówki dla tych administratorów danych osobowych, którzy otrzymali przypadkowo niechciane dane osobowe lub utracili kontrolę nad przetwarzanymi informacjami.

Stanowiska Komisarza warto uzupełnić o uwagę, że RODO nie przewiduje instytucji „nielegalnego" administratora danych osobowych. Oznacza to, że administrator przetwarzający dane osobowe bez podstawy prawnej narusza wprawdzie przepisy RODO, ale nadal przysługują mu uprawnienia władcze w stosunku do posiadanych informacji, co wynika wprost z definicji „administratora danych" zawartej w art. 4 pkt 7 RODO. Tym samym jest on zobowiązany do podjęcia niezbędnych kroków w celu przywrócenia stanu zgodnego z prawem. W takiej sytuacji wytyczne Komisarza mogą być pomocne.

Źródło:
www.dataprotection.ie/sites/default/files/uploads/2020-08/Guidance%20for%20Organisations%20Accidentally%20in%20Receipt%20of%20Personal%20Data.pdf;
www.dataprotection.ie/sites/default/files/uploads/2020-08/Guidance%20for%20Data%20Controllers%20who%20Lose%20Control%20of%20data%20to%20a%20Third%20Party.pdf

Odpowiednie środki techniczne i organizacyjne – dobre praktyki bawarskiego organu nadzorczego

Mateusz Kupiec

Bawarski organ nadzorczy (Bayerisches Landesamt für Datenschutzaufsicht; dalej: „bawarski organ nadzorczy" lub „BayLfD") opublikował 13 października 2020 r. listę środków technicznych i organizacyjnych, które administratorzy danych osobowych mogą zastosować, aby zapewnić odpowiedni poziom bezpieczeństwa procesu przetwarzania danych osobowych.

Organ wskazuje, że opracowane przez niego zestawienie nie jest wyczerpujące, a jego celem jest w szczególności pomoc małym i średnim przedsiębiorstwom w spełnieniu wymogów RODO. Wytyczne BayLfD składają się z 18 punktów i dotyczą praktycznych aspektów zarządzania bezpieczeństwem w organizacji. Poniżej przedstawiamy wybrane wskazówki organu.

1. Autoryzacja

W ocenie organu reglamentacja dostępu do zasobów informatycznych i przetwarzanych danych osobowych pozytywnie wpływa na bezpieczeństwo przechowywanych informacji w organizacji. BayLfD zaleca w szczególności, aby administratorzy:

- wprowadzili automatyczną blokadę dostępu w wypadku zbyt wielu nieudanych prób logowania z powodu wpisania błędnego hasła – blokada może mieć charakter czasowy (np. 1 godzina, 6 godzin, 24 godziny) albo całkowity (w celu odblokowania systemu konieczny jest kontakt z działem IT);
- instruowali zatrudnionych, że nie mogą zapisywać haseł na karteczkach ani na tablicach z przypinkami;
- rejestrowali liczbę nieudanych prób logowania użytkownika, który w końcu pomyślnie się zalogował, w celu rozpoznania ataków lub prób ataków;
- zakazali przechowywania haseł w przeglądarce bez ochrony hasłem głównym;
- w miarę możliwości wdrożyli automatyczną politykę stosowania silnych haseł w systemach z identyfikatorami użytkowników;
- unikali stosowania haseł grupowych w organizacji.

2. Business Continuity

W celu zapewnienia ciągłości działania (przetwarzania) BayLfD rekomenduje:

- regularne sprawdzanie, czy codziennie wykonywany jest co najmniej jeden backup przetwarzanych danych osobowych;
- zrezygnowanie ze stosowania makropoleceń w dokumentach tworzonych za pomocą programów z pakietu Office w codziennych operacjach w celu ochrony przed atakami typu ransomware;
- opracowanie pisemnych zasad tworzenia kopii zapasowych;
- zapobieganie automatycznemu uruchamianiu się pobranych programów;
- przygotowanie (również w formie pisemnej) i regularny przegląd planu awaryjnego dla zapewnienia ciągłości działania – plan ten powinien określać, które systemy mają być naprawiane i w jakiej kolejności oraz z którymi osobami (zewnętrznymi) lub dostawcami usług można się konsultować w sytuacji awaryjnej.

3. Sieć

Jednym ze skutków pandemii SARS-CoV-2 jest znaczny wzrost cyberataków. W celu ograniczenia ich skuteczności BayLfD sugeruje administratorom danych, aby:

- stosowali systemy wykrywania włamań (IDS) lub systemy zapobiegania włamaniom (IPS);
- korzystali z serwera proxy, przez który muszą przejść wszystkie połączenia HTTP(S);
- umożliwiali osobom spoza organizacji jedynie dostęp do sieci WLAN przeznaczonej dla gości, tj. bez dostępu do sieci wewnętrznej;
- wprowadzili protokołowanie na poziomie firewalla w celu wykrycia i analizy nieautoryzowanego dostępu pomiędzy sieciami;
- blokowali niebezpieczne załączniki do poczty elektronicznej (np. zawierające rozszerzenia .exe, .doc, .cmd).

4. Protokołowanie

Odpowiednie dokumentowanie zdarzeń w systemie informatycznym pozwala zidentyfikować naruszenia bezpieczeństwa. Zdaniem bawarskiego organu nadzorczego administratorzy powinni więc:

- przeprowadzać regularną ocenę plików dziennika (logów) w celu wykrycia nietypowych wpisów – najlepiej: heurystyka automatyczna;
- przechowywać logi na oddzielnym serwerze logów;
- zsynchronizować zegary używanych systemów przetwarzania informacji (komputerów osobistych itp.) z odpowiednimi źródłami czasu, aby umożliwić ukierunkowaną analizę w wypadku zdarzeń związanych z bezpieczeństwem.

5. Bezpieczeństwo fizyczne infrastruktury

BayLfD zauważa, że systemy informatyczne i przechowywane w nich dane osobowe powinny być chronione nie tylko przed nieuprawnionym dostępem, lecz także przed zagrożeniami związanymi z np. klęskami żywiołowymi. W tym celu organ zaleca:

- wprowadzenie jasnych zasad postępowania z osobami spoza organizacji (np. wymóg eskorty gości, wydawanie identyfikatorów odwiedzającym);
- korzystanie z systemów alarmowych;
- stosowanie automatycznych systemów gaśniczych w serwerowniach (np. gaszenie gazem CO2) z uwzględnieniem przepisów bezpieczeństwa i higieny pracy;
- zakup sprzętu do zapewnienia zasilania systemów serwerowych, szczególnie w wypadku krótkotrwałych awarii lub wahań napięcia.

6. Obsługa techniczna

W ocenie BayLfD korzystanie z usług zewnętrznej obsługi technicznej, w szczególności w celu utrzymania infrastruktury informatycznej, musi być właściwie monitorowane i dokumentowane. W celu przeciwdziałania incydentom bezpieczeństwa organ rekomenduje:

- zobowiązanie podmiotu, z którego usług korzysta administrator, do zachowania poufności lub nakazanie podpisania odpowiedniego oświadczenia pracownikowi tego podmiotu;
- określenie zasad przekazywania sprzętu IT zewnętrznej obsłudze technicznej, producentowi urządzenia (np. w celu naprawy);
- wyznaczenie pracownika wewnętrznego, który będzie nadzorował i dokumentował działania zewnętrznej obsługi technicznej w organizacji administratora.

Link do całości opracowania BayLfD (wyłącznie w języku niemieckim):
https://www.lda.bayern.de/media/checkliste/baylda_checkliste_tom.pdf.

Age appropriate design code – nowy standard ICO dotyczący ochrony prywatności dzieci przez dostawców usług informacyjnych

Mateusz Kupiec

2 września 2020 r. wszedł w życie Age appropriate design code (Kodeks projektowania stosownie do wieku) – zbiór 15 standardów opracowanych przez biuro brytyjskiego organu nadzorczego (ICO), mających na celu zagwarantowanie lepszej ochrony prywatności dzieci w Internecie. Chociaż terytorialny zakres stosowania Kodeksu obejmuje wyłącznie Wielką Brytanię, to zawarte w nim standardy mają na tyle uniwersalny charakter, że będą przydatne dla każdego administratora danych osobowych, który przetwarza dane osobowe dzieci. Przedstawiamy wybrane elementy Kodeksu.

Transparentność

Autorzy Kodeksu zwracają szczególną uwagę na zagadnienie przejrzystości informacji dotyczących przetwarzania danych osobowych, których adresatami są dzieci. Zdaniem autorów dostawcy treści internetowych powinni zwracać uwagę na przedział wiekowy osób niepełnoletnich oraz potrzeby danej grupy wiekowej. Podejście „one-size-fits-all" nie uwzględnia faktu, że dzieci mają różne potrzeby na różnych etapach rozwoju. W związku z tym w przypadku młodszych dzieci, znajdujących się na wcześniejszych etapach rozwoju poznawczego, konieczne może być dostarczenie mniej szczegółowych informacji o przetwarzaniu danych i poleganie w większym stopniu na zaangażowaniu rodziców. W zależności od wieku dziecka ICO zaleca więc stosowanie różnych form prezentacji klauzul informacyjnych. Na przykład zdaniem organu dzieci od 10 roku życia powinny być w stanie samodzielnie wybrać, w jakim formacie (pisemnym, audio lub wideo) chcą zobaczyć prezentowane klauzule informacyjne, a dzieciom od 6 do 9 roku życia należy też wyjaśniać podstawy działania serwisu.

Warto w tym miejscu zauważyć, że zalecenia organu przedstawione w Kodeksie stanowią przydatne uzupełnienie fragmentów Wytycznych w sprawie przejrzystości na podstawie rozporządzenia 2016/679 (WP 260) Grupy Roboczej Art. 29, które dotyczą czytelnej komunikacji z dziećmi jako podmiotami danych.

Techniki „popychania" (nudge techniques)

Techniki „popychania" mają na celu zachęcenie użytkowników do podjęcia takiej decyzji, jaka preferowana jest przez projektanta danego serwisu lub aplikacji. W sieci istnieje ryzyko, że takie techniki mogą potencjalnie być stosowane wobec dzieci w celu nakłonienia ich do przekazania danych osobowych. Zdaniem autorów Kodeksu takie techniki powinny być wykorzystywane wyłącznie w celu zwiększenia dobra dzieci, a nie nakłaniania ich do podejmowania decyzji, które miałyby zły wpływ na ochronę ich prywatności. W związku z tym nie należy m.in. używać takich technik nakłaniania, które mogą prowadzić dzieci do kłamstw na temat ich wieku, na przykład poprzez definiowanie z góry wyłącznie starszego przedziału wiekowego i nieumożliwianie wyboru prawdziwego wieku.

[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).

Inteligentne zabawki i urządzenia

W Kodeksie ICO podejmuje również problem inteligentnych, połączonych z Internetem zabawek, urządzeń, które przetwarzają dane osobowe dzieci. Organ zaleca podmiotom oferującym takie przedmioty m.in.:

- Informowanie w momencie sprzedaży oraz przed konfiguracją urządzenia o tym, że produkt przetwarza dane osobowe. Zarówno opakowanie produktu fizycznego, jak i ulotka lub instrukcja obsługi (papierowa lub cyfrowa) powinny zawierać wyraźną informację (np. ikonę), że produkt jest „połączony" i przetwarza dane osobowe użytkowników.
- Udostępnienie opcji zakładania profilu użytkownika dla osób, które regularnie posługują się urządzeniem, aby ułatwić korzystanie z niego osobom dorosłym lub dostosować usługi do wieku konkretnego dziecka.
- Umożliwienie potencjalnym użytkownikom inteligentnej zabawki lub połączonego urządzenia zapoznania się z informacjami o ich prywatności, z warunkami użytkowania i z innymi istotnymi danymi bez konieczności wcześniejszego zakupu i konfiguracji urządzenia, aby te osoby mogły podjąć świadomą decyzję o nabyciu takiego produktu.

Na problem zagrożeń dla prywatności dzieci, jaki niosą za sobą inteligentne zabawki, zwrócił uwagę także Prezes UODO w stanowisku z czerwca 2020 r., które zawiera porady dotyczące bezpiecznego korzystania z takich urządzeń.

Link do Kodeksu: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/.

Link do stanowiska Prezesa UODO: https://uodo.gov.pl/pl/138/1548.

Komentarz

W dobie powszechnego dostępu do Internetu ochrona prywatności najmłodszych powinna być czynnikiem branym pod uwagę przez każdy podmiot oferujący treści online. Jak wskazują wyniki badania EU Kids Online 2020, Internet stał się nieodłączną częścią codzienności dzieci i młodzieży w państwach UE. Wraz ze wzrostem aktywności oraz obecności najmłodszych w sieci rośnie ilość wytwarzanych przez nich danych osobowych w środowisku online. Dzieci zalicza się do kategorii wrażliwych podmiotów danych, których autonomia informacyjna powinna być chroniona w szczególny sposób.

Źródło: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/.

Ochrona danych osobowych przetwarzanych w systemach sztucznej inteligencji

adw. Katarzyna Syska

Brytyjski organ nadzorczy (Information Commissioner's Office; ICO) wydał wytyczne dotyczące zastosowania przepisów o ochronie danych osobowych do przetwarzania danych w systemach wykorzystujących sztuczną inteligencję (systemy AI). Poniżej przedstawiamy wybrane kwestie odnoszące się do stosowania podstawowych zasad przetwarzania danych w systemach AI, na które ICO zwrócił uwagę

Zapewnianie zgodności z prawem przetwarzania danych w systemach AI

ICO dostrzega, że w każdej sytuacji przetwarzania danych w ramach systemu AI konieczne jest ustalenie podstawy prawnej przetwarzania. Organ podkreślił, że dotyczy to także etapu szkolenia systemu AI.

Co istotne podstawa przetwarzania danych w odniesieniu do etapu szkolenia lub testowania systemu AI może być różna od tej stosowanej na etapie jego wdrożenia i wykorzystywania. Należy bowiem zauważyć, że w tych przypadkach inne będą cele przetwarzania danych. W związku z tym konieczne jest zidentyfikowanie celów przetwarzania i jego podstaw odnośnie do poszczególnych czynności przetwarzania danych w systemie AI.

ICO podaje w tym kontekście przykład systemu AI służącego do rozpoznawania twarzy. System taki jest szkolony w ogólnym celu, jakim jest rozpoznawanie twarzy (tj. identyfikacja osób fizycznych). Jednakże może mieć on być wykorzystywany w bardzo różnych celach, począwszy od zapobiegania przestępczości, poprzez uwierzytelnianie, a skończywszy na oznaczaniu osób na zdjęciach w sieci społecznościowej. W zależności od konkretnego celu prztwarzania danych (w tym związanego ze szkoleniem systemu AI), podstawa ich przetwarzania może być różna. ICO rekomenduje także udokumentowanie podstaw prawnych przetwarzania danych.

Stosowanie zasady minimalizacji do systemów AI

Brytyjski organ zwraca uwagę na potencjalny konflikt między zasadą minimalizacji danych, która wymaga przetwarzania jak najmniejszej ilości danych, a możliwością rozwijania i stosowania systemów AI, jakie co do zasady wymagają dużej ilości danych

W tym kontekście brytyjski organ zwraca uwagę, że zgodnie z zasadą minimalizacji dane osobowe powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do osiągnięcia celu przetwarzania. ICO podkreśla, że określenie, co jest w danej sytuacji adekwatne, stosowne i ograniczone zależy od okoliczności. Kluczowe jest zatem sprecyzowanie, jaki zakres danych jest rzeczywiście potrzebny do tego, aby osiągnąć konkretny cel – np. przeprowadzić szkolenie systemu AI. Jednocześnie ICO zaleca stosowanie różnych technik minimalizacji danych.

Stosowanie zasady prawidłowości do systemów AI

Brytyjski organ podnosi też kwestię konieczności zapewnienia poprawności danych w odniesieniu do danych tworzonych lub wnioskowanych przez system AI (np. prognozy co do tego, czy ktoś spłaci pożyczkę, rekomendacji treści, którymi dana osoba może być zainteresowana, klasyfikacji wiadomości e-mail jako spamu).

W tym kontekście ICO zwraca uwagę na dokładność statystyczną w systemach AI, czyli to, jak często system odgaduje poprawną odpowiedź, mierzoną w odniesieniu do poprawnie oznaczonych danych testowych.

ICO wskazuje, że co prawda zasada prawidłowości ma zastosowanie do danych tworzonych przez system AI, ale nie oznacza to jednak, że system AI musi być w 100% statystycznie dokładny, aby był zgodny z tą zasadą. Istotne w tym kontekście jest to, żeby dane tworzone przez system AI były oznaczane jako statystyczne przypuszczenia lub przewidywania dotyczące czegoś, tworzone przez system AI, a nie faktyczne informacje o osobie. ICO zwraca także uwagę na konieczność wprowadzenia odpowiednich matematycznych lub statystycznych procedur profilowania, co wynika z motywu 71 RODO.

Ponadto w przypadku korzystania z systemu AI do wyciągania wniosków (tworzenia prognoz czy rekomendacji) na temat ludzi, należy upewnić się, że system jest wystarczająco dokładny statystycznie w odniesieniu do konkretnych celów. Jest to także związane z zasadą rzetelności i uczciwości przetwarzania danych

Stosowanie zasady rzetelności do systemów AI

Zgodnie z wytycznymi ICO rzetelność (uczciwość) przetwarzania w kontekście systemów AI oznacza, że należy wykorzystywać dane w sposób, którego ludzie mogą się racjonalnie spodziewać. Nie powinno się natomiast posługiwać danymi tak, aby wywierać nieuzasadniony niekorzystny wpływ na osoby, których dane dotyczą.

ICO zwraca szczególną uwagę na kwestię potencjalnej dyskryminacji w związku z korzystaniem z systemów AI. Przetwarzanie danych w systemach AI, które prowadziłoby do dyskryminacji ze względu na płeć, rasę, wiek, stan zdrowia, wyznanie, niepełnosprawność, orientację seksualną lub inne cechy, byłoby niezgodne z zasadą rzetelności. ICO rekomenduje zatem stosowanie różnych technik zapobiegających dyskryminacji przez systemy AI oraz testowanie systemów pod tym kątem.

35 mln euro kary dla H&M za zbieranie szczegółowych danych dotyczących życia prywatnego pracowników

adw. Katarzyna Syska

Hamburski organ ochrony danych osobowych nałożył administracyjną karę pieniężną w wysokości 35 258 707,95 euro na H&M Hennes & Mauritz Online Shop A.B. & Co. KG. W centrum usług H&M w Norymberdze przez kilka lat zbierano szczegółowe informacje o życiu prywatnym pracowników, co hamburski organ uznał za bardzo poważne naruszenie przepisów o ochronie danych osobowych. Organ ocenił taką wysokość kary jako skuteczną i proporcjonalną – ma ona powstrzymywać administratorów danych przed podobnymi naruszeniami przepisów.

Jakie dane o pracownikach zbierano?

Po nieobecnościach pracowników, takich jak urlopy i zwolnienia lekarskie, przełożeni przeprowadzali z tymi osobami rozmowy z okazji powrotu do pracy. W wielu przypadkach zbierano wówczas informacje dotyczące doświadczeń urlopowych pracowników, lecz także objawów chorób i diagnoz. Niektórzy przełożeni zadawali pytania również na temat spraw rodzinnych i przekonań religijnych osób zatrudnionych. Część tych danych była utrwalana i przechowywana w systemie informatycznym. Informacje były zbierane co najmniej od 2014 r. Dostęp do nich miało ok. 50 menedżerów w całej spółce. Dane służyły m.in. do oceny wyników pracy pracowników, do utworzenia ich szczegółowego profilu, a także do podejmowania decyzji dotyczących zatrudnienia tych osób.

Jak organ dowiedział się o zbieraniu danych?

W październiku 2019 r. dane stały się dostępne na kilka godzin dla wszystkich osób w firmie z powodu błędnej konfiguracji systemu. Organ ochrony danych dowiedział się o tym z doniesień prasowych. Natychmiast nakazał „zamrożenie" zawartości dysku sieciowego, na którym przechowywane były powyższe dane pracowników, a następnie zażądał przekazania tych danych. Praktykę zbierania szczegółowych informacji o pracownikach potwierdzono też w drodze prze-słuchań świadków.

Jakie działania podjął pracodawca?

H&M wypłaciło poszkodowanym pracownikom odszkodowania. Ponadto wprowadzono nowe środki mające na celu lepszą ochronę prawa do prywatności pracowników, w tym powoła-no koordynatora ds. ochrony danych osobowych oraz wdrożono procedurę postępowania z żądaniami dostępu do danych.

Źródło: https://edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_pl.

ICO nałożył na British Airways 20 mln funtów za naruszenie art. 32 RODO

dr Iga Małobęcka-Szwast

W dniu 16 października 2020 r. brytyjski organ nadzorczy (ICO) nałożył na British Airways administracyjną karę pieniężną w wysokości 20 mln funtów za naruszenie ochrony danych osobowych, które dotknęło ponad 400 tys. klientów, i niedopełnienie obowiązków związanych z zapewnieniem odpowiedniego bezpieczeństwa danych osobowych (art. 5 ust. 1 lit. f i art. 32 RODO[1]). Jest to jak dotąd najwyższa administracyjna kara pieniężna nałożona przez ICO.

Na czym polegało naruszenie?

ICO stwierdził, że British Airways nie przetwarzało danych osobowych swoich klientów w sposób zapewniający odpowiednie bezpieczeństwo, zgodnie z art. 5 ust. 1 lit. f i art. 32 RODO.

Do naruszenia ochrony danych doszło między 22 czerwca a 5 września 2018 r., kiedy hakerzy uzyskali dostęp do systemów IT i sieci British Airways. Hakerzy przekierowywali dane karty płatniczej klienta ze strony British Airways do oszukańczej witryny (proces określany jako skimming). Przedsiębiorstwo zostało poinformowane o naruszeniu przez osobę trzecią i powiadomiło ICO w dniu 6 września 2018 r. Ogółem naruszenie dotyczyło około 430 tys. podmiotów danych – klientów i pracowników British Airways.

W wyniku ataku hakerzy uzyskali dostęp do danych osobowych klientów i pracowników, takich jak: imię i nazwisko, adres i dane karty płatniczej (w tym kod CVV), a także dane logowania pracowników British Airways i konta administratora.

Niepowodzenie w zapobieganiu atakowi

W ocenie ICO British Airways mogło zastosować wiele środków, aby złagodzić efekt lub zapobiec ryzyku uzyskania dostępu do swojej sieci przez hakerów. Do środków tych należą m.in.:

- ograniczenie dostępu do aplikacji, danych i narzędzi tylko do tych, które są wymagane do pełnienia roli użytkownika;
- przeprowadzenie rygorystycznych testów w formie symulacji cyberataku na systemy przedsiębiorstwa;
- ochrona kont pracowników i osób trzecich za pomocą uwierzytelniania wieloskładnikowego.

Według ICO żaden z tych środków nie wiązałby się z nadmiernymi kosztami ani barierami technicznymi dla British Airways.

Jednocześnie ICO zauważył, że British Airways dokonało znacznych ulepszeń w zakresie bezpieczeństwa IT od czasu ataku.

Ponadto ICO stwierdził, że chociaż naruszenie nie dotyczyło szczególnych kategorii danych, to dane finansowe, które wyciekły, należy uznać za wrażliwe.

[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).

Brak świadomości ataku

ICO zaznaczył, że British Airways nie wykryło ataku z 22 czerwca 2018 r., ale zostało zaalarmowane przez stronę trzecią ponad dwa miesiące później – 5 września 2018 r. Nie jest jasne, czy i kiedy British Airways samodzielnie zidentyfikowałoby atak. Uznano to za poważne naruszenie ze względu na liczbę dotkniętych nim osób oraz potencjalne znaczące skutki finansowe dla osób, których dane dotyczą.

Wysokość kary

Choć kara w wysokości 20 mln funtów jest jak dotąd najwyższą karą nałożoną przez ICO, jest ona znacznie mniejsza niż przewidywano. W lipcu 2019 r. ICO po-informował o zamiarze nałożenia kary pieniężnej w wysokości 183 mln funtów. Została ona jednak obniżona ze względu na działania zaradcze podjęte przez British Airways oraz ekonomiczne skutki pandemii COVID-19.

Przy obliczaniu grzywny ICO wziął pod uwagę oświadczenia British Airways w odpowiedzi na pierwotne zawiadomienie o zamiarze nałożenia kary oraz dodatkowe informacje techniczne, które przekazało przedsiębiorstwo, jak również czynniki wymienione w art. 83 ust. 2 RODO, w tym m.in. wagę i czas trwania naruszenia, liczbę osób, których dane dotyczą, oraz szkody, jakie poniosły, a także kroki podjęte przez British Airways w celu złagodzenia skutków incydentu dla tych osób.

Okoliczności łagodzące obejmowały fakt, że British Airways nie odniosło żadnych korzyści finansowych z naruszenia, niezwłocznie powiadomiło ICO o naruszeniu po powzięciu o nim wiadomości, nie miało wcześniejszych podobnych naruszeń i zaoferowało odszkodowanie osobom fizycznym za straty finansowe poniesione w wyniku kradzieży danych ich kart. ICO stwierdził, że British Airways w pełni współpraco-wało podczas dochodzenia, i zwrócił uwagę na ulepszenia, które zostały wprowadzone w bezpieczeństwie IT British Airways od czasu naruszenia.

ICO obniżył pierwotnie zapowiadaną wysokość kary do 24 mln funtów, aby odzwierciedlić działania zaradcze podjęte przez British Airways, i obniżył karę o kolejne 4 mln funtów, aby odzwierciedlić ekonomiczne konsekwencje pandemii COVID-19.

Źródło: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/

ZESPÓŁ RODO

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

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

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

Dominika Nowak
Radca prawny, Senior Associate
dominika.nowak@traple.pl

dr Iga Małobęcka-Szwast LL.M.
Senior Associate
iga.malobecka@traple.pl

Mateusz Kupiec
Trainee
mateusz.kupiec@traple.pl

Redaktor newslettera:
dr Iga Małobęcka-Szwast

Pytania prosimy kierować na adres:
rodo@traple.pl