NR 2 - LIPIEC 2020

NEWSLETTER RODO

Temat numeru -

Zasady monitoringu wizyjnego w świetle decyzji organów nadzorczych w UE

Tematy artykułów:

- Transfer danych osobowych do państwa trzeciego (wyrok Schrems II)
- Obowiązek informacyjny wobec członków zarządu osób prawnych
- Odpowiedzialność administratora za pracowników
- Wykorzystanie dronów a ochrona danych osobowych
- Naruszenia dotyczące marketingu bezpośredniego

Traple Konarski Podrecki & Wspólnicy

TKP

ZASADY MONITORINGU WIZYJNEGO W ŚWIETLE DECYZJI ORGANÓW NADZORCZYCH W UE

Katarzyna Syska, Grzegorz Sibiga

Organy nadzorcze w państwach Unii Europejskiej nałożyły już kilkanaście kar pieniężnych za niezgodne z prawem przetwarzanie danych w związku z prowadzeniem monitoringu wizyjnego. Poniżej przedstawiamy przegląd decyzji organów nadzorczych dotyczących monitoringu oraz płynące z tych decyzji wnioski.

Zbieranie zbyt wielu danych w drodze monitoringu

Jednym z najczęstszych typów naruszeń jest zbieranie w drodze monitoringu danych osobowych, które nie są niezbędne do osiągnięcia zamierzonego celu. Chodzi zatem o naruszenie zasady minimalizacji danych. W praktyce różne sytuacje mogą doprowadzić do takiego naruszenia.

Jedną z nich jest **zbyt duży zasięg kamer monitorujących**. Organy nadzorcze zwracają szczególną uwagę, aby monitoring wizyjny nie obejmował przestrzeni publicznej ani terenu należącego do podmiotów innych niż administrator.

Na przykład austriacki organ nadzorczy nałożył karę na zakład bukmacherski, który zasięgiem monitoringu objął także duży obszar przestrzeni publicznej przed wejściem do zakładu (decyzja z 12 września 2018 r.). Był to obszar ulicy, a na obrazach widoczni byli przechodnie oraz pojazdy i ich tablice rejestracyjne. Organ uznał, że doszło w związku tym do naruszenia zasad określonych w art. 5 RODO[1]. Podobną decyzję wydał hiszpański organ nadzorczy wobec hotelu, który zasięgiem monitoringu wizyjnego objął obszar publiczny w otoczeniu hotelu. Organ uznał, że doszło do naruszenia zasady minimalizacji danych (decyzja z 26 lutego 2020 r.).

Proporcjonalność stosowania monitoringu

Były też przypadki, w których **organy zakwestionowały proporcjonalność stosowania monitoringu wizyjnego** z innych względów. Francuski organ nadzorczy nałożył karę na biuro tłumaczeń, które objęło stałym monitoringiem wizyjnym kilku swoich pracowników. Kamera była zainstalowana w biurze, które nie było dostępne dla osób z zewnątrz, i była skierowana na stanowiska pracy tych pracowników. Monitoring wizyjny miał na celu zapewnienie bezpieczeństwa osób i mienia. Jednakże organ doszedł do wniosku, że w tym przypadku zbieranie danych w drodze stałego monitoringu pracowników w ich miejscu pracy było nieproporcjonalne w stosunku do celu przetwarzania (decyzja z 13 czerwca 2019 r.).

Natomiast szwedzki organ nadzorczy w decyzji dotyczącej wspólnoty mieszkaniowej stwierdził, że stosowanie monitoringu wizyjnego wymaga regularnej oceny, czy jego stosowanie jest wciąż konieczne do osiągnięcia celów przetwarzania. Jedna z kamer umieszczona była przy wejściu do budynku, a celem tego było przeciwdziałanie wandalizmowi, gdyż takie incydenty zdarzyły się dwa lata wcześniej. Organ stwierdził, że w niniejszym przypadku nie wykazano, aby stosowanie monitoringu było niezbędne (decyzja z 15 czerwca 2020 r.).

Nagrywanie dźwięku łącznie z obrazem

Innym ciekawym przykładem jest **nagrywanie dźwięku łącznie z obrazem**. W takiej sytuacji dochodzi do zbierania informacji o tym, co mówią osoby widoczne na nagraniach. Taka okoliczność miała miejsce w przypadku wspomnianej wyżej szwedzkiej wspólnoty mieszkaniowej – jedna z kamer umieszczonych w budynku mieszkalnym (w części wspólnej) nagrywała także dźwięk. Szwedzki organ nadzorczy uznał to za istotne naruszenie prywatności oraz stwierdził, że w danym przypadku okoliczności sprawy nie uzasadniają takiej ingerencji (decyzja z 15 czerwca 2020 r.).

[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).

Innym przykładem na nagrywanie fonii jest sprawa Taksi Helsinki – firmy taksówkarskiej w Helsinkach, która zainstalowała w swoich pojazdach kamery rejestrujące obraz i dźwięk. Fiński organ nadzorczy stwierdził, że przetwarzanie danych w zakresie dźwięku nie było zgodne z zasadą minimalizacji danych (decyzja z 26 maja 2020 r.).

Monitoring służący do rozpoznawania twarzy

Z kolei pierwsza kara pieniężna nałożona przez szwedzki organ nadzorczy dotyczyła stosowanego w szkole **systemu monitoringu, który służył także do rozpoznawania twarzy** uczniów. Miał on na celu sprawdzanie ich obecności na lekcjach. W związku z tym, że system służył do rozpoznawania twarzy uczniów, dochodziło do zbierania danych biometrycznych. Szwedzki organ nadzorczy stwierdził, że do sprawdzania obecności w szkole nie jest konieczne przetwarzanie szczególnych kategorii danych (danych biometrycznych) ani stosowanie systemu służącego do rozpoznawania twarzy. Organ uznał, że jest to istotne naruszenie praw uczniów oraz że przetwarzanie takich danych jest nieproporcjonalne w stosunku do celów (decyzja z 20 sierpnia 2019 r.).

Brak odpowiedniego poinformowania o monitoringu wizyjnym

Unijne organy nadzorcze w kilku przypadkach stwierdziły, że osoby, których dane były zbierane za pośrednictwem systemu monitoringu wizyjnego, nie były w ogóle albo w wystarczający sposób o tym poinformowane. W przypadku szwedzkiej wspólnoty mieszkaniowej mieszkańcy nie byli informowani o administratorze danych, o tym, gdzie mogą uzyskać więcej informacji, ani o tym, że dźwięk jest nagrywany, co szwedzki organ uznał za szczególnie ciężkie naruszenie. W decyzji dotyczącej biura tłumaczeń francuski organ stwierdził, że pracownicy nie było poinformowani o przetwarzaniu ich danych osobowych, co stanowiło naruszenie art. 12 i 13 RODO. W przypadku Taksi Helsinki informacje przekazywane klientom o przetwarzaniu ich danych były niekompletne – brak było m.in. informacji o prawie do wniesienia skargi do organu nadzorczego. Natomiast austriacki organ nadzorczy w decyzji dotyczącej zakładu bukmacherskiego zwrócił także uwagę na brak oznaczeń wskazujących na to, że obszar jest monitorowany.

Brak przeprowadzenia oceny skutków dla ochrony danych

Organy nadzorcze zwracały również uwagę na brak przeprowadzenia oceny skutków dla ochrony danych. Był to m.in. przypadek szwedzkiej szkoły, w której stosowano monitoring do rozpoznawania twarzy uczniów, a także kazus helsińskiej firmy taksówkarskiej.

Nieodpowiednia podstawa prawna lub zakwestionowanie podstawy prawnej

W kilku przypadkach organy nadzorcze miały zastrzeżenia co do podstawy prawnej przetwarzania danych. W sprawie szwedzkiej szkoły stosującej system rozpoznawania twarzy podstawą prawną przetwarzania danych biometrycznych była zgoda opiekunów prawnych uczniów. Szwedzki organ uznał tę podstawę za nieodpowiednią z uwagi na brak równowagi między administratorem danych a uczniami. Austriacki organ nadzorczy – w sprawie dotyczącej zakładu bukmacherskiego – stwierdził naruszenie art. 6 ust. 1 lit. f RODO, ponieważ uznał, że osoby objęte monitoringiem (przechodnie, osoby w samochodach) nie mogły się rozsądnie spodziewać, że ich dane będą zbierane w ten sposób. Organ uznał zatem, że uzasadniony interes administratora nie jest w tym przypadku nadrzędny nad prawami, wolnościami ani interesami osób, których dane dotyczą. Natomiast w sprawie helsińskich taksówek administrator nie był w stanie wykazać, że przetwarzał dane zgodnie z art. 5 ust. 1 lit. a RODO (zasada zgodności z prawem) oraz art. 6 ust. 1 lit. f RODO (prawnie uzasadniony interes), zatem organ nadzorczy stwierdził naruszenie zasady rozliczalności.

Brak realizacji żądania dostępu do danych

Pierwsza z kar nałożonych przez węgierski organ nadzorczy dotyczyła braku realizacji żądania dostępu do danych, czyli nieprzekazania osobie, której dane dotyczą, kopii nagrania z jej danymi osobowymi. Osoba ta poprosiła administratora o kopię nagrania, aby przedstawić je jako dowód w postępowaniu sądowym. Administrator nie spełnił żądania, ponieważ stwierdził, że nagranie nie stanowiłoby odpowiedniego dowodu, bo wynikało z niego tylko, że ta osoba była w danym miejscu danego dnia (nie był nagrywany dźwięk). Następnie administrator usunął nagranie. W swojej decyzji węgierski organ zwrócił uwagę na to, że administrator nie może wymagać jakiegokolwiek uzasadnienia wniosku o dostęp do danych (decyzja z 18 grudnia 2018 r.).

OCHRONA DANYCH OSOBOWYCH W CZASACH PANDEMII COVID-19

Stanowisko EROD w sprawie ograniczeń praw podmiotów danych w związku ze stanem wyjątkowym w państwach członkowskich

Iga Małobęcka-Szwast

Dnia 2 czerwca 2020 r., podczas 30. posiedzenia plenarnego Europejska Rada Ochrony Danych (EROD) przyjęła oświadczenie dotyczące ograniczeń praw osób, których dane dotyczą, w związku z wprowadzeniem stanu wyjątkowego w państwach członkowskich. Oświadczenie dostarcza cennych wskazówek co do interpretacji art. 23 RODO.

Pomimo stanu wyjątkowego RODO wciąż obowiązuje

EROD podkreśla, że nawet w tych wyjątkowych czasach państwa członkowskie powinny przestrzegać zasad ochrony danych osobowych przy wdrażaniu środków nadzwyczajnych, przyczyniając się w ten sposób do poszanowania nadrzędnych wartości, takich jak demokracja, praworządność i prawa podstawowe, na których opiera się Unia Europejska.

EROD zwraca uwagę, że RODO nadal ma zastosowanie i nie uniemożliwia dokonywania niezbędnych do walki z pandemią COVID-19 operacji przetwarzania danych. Takie przetwarzanie powinno odbywać się w zgodzie z podstawowymi prawami i wolnościami osób, których dane dotyczą.

Zasady ograniczania praw osób, których dane dotyczą

W swoim oświadczeniu EROD wskazuje na główne zasady dotyczące ograniczeń praw osób, których dane dotyczą (art. 23 RODO), w związku z wprowadzeniem stanu wyjątkowego w państwach członkowskich.

W ocenie EROD:

- Ograniczenia, które są tak ogólne czy rozległe lub w takim stopniu ingerują w prawa osób, których dane dotyczą, iż naruszają istotę danego prawa, nie mogą być uznane za uzasadnione.
- Pod pewnymi warunkami art. 23 RODO pozwala krajowym prawodawcom ograniczyć za pomocą aktu prawnego zakres obowiązków administratorów i podmiotów przetwarzających oraz praw osób, których dane dotyczą, jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności zdrowiu publicznemu.

- Prawa osób, których dane dotyczą, stanowią rdzeń podstawowego prawa do ochrony danych, a art. 23 RODO należy interpretować w ten sposób, że stosowanie tych praw jest ogólną zasadą. Ponieważ ograniczenia stanowią wyjątki od tej zasady, należy je stosować tylko w szczególnych okolicznościach.
- Ograniczenia muszą być przewidziane przepisami prawa, a prawo ustanawiające te ograniczenia powinno być wystarczająco jasne, aby umożliwiało zrozumienie, w jakich warunkach administratorzy są uprawnieni do ich stosowania.
- Ograniczenia muszą być przewidywalne dla osób, które są nimi objęte. EROD podkreśla, że nałożone na czas nieokreślony ograniczenia, które obowiązują z mocą wsteczną lub są obwarowane nieprecyzyjnymi warunkami, nie spełniają kryterium przewidywalności.
- Samo wystąpienie pandemii lub jakiejkolwiek innej sytuacji nadzwyczajnej nie jest wystarczającym powodem do wprowadzenia jakiegokolwiek ograniczenia praw osób, których dane dotyczą. To raczej ograniczenia

muszą wyraźnie przyczyniać się do ochrony ważnego celu leżącego w ogólnym interesie publicznym UE lub państwa członkowskiego.

- Stan wyjątkowy przyjęty w związku z pandemią jest warunkiem prawnym, który może uzasadniać ograniczenia praw osób, których dane dotyczą, z zastrzeżeniem, że ograniczenia te mogą mieć zastosowanie tylko w takim zakresie, w jakim jest to absolutnie niezbędne i proporcjonalne w celu ochrony zdrowia publicznego. Z tego względu wprowadzane ograniczenia muszą mieć ściśle oznaczony zakres i czas obowiązywania (w szczególności nie mogą obowiązywać dłużej niż stan wyjątkowy).
- Przyjęte w związku z wprowadzeniem stanu wyjątkowego ograniczenia zawieszające lub odraczające stosowanie praw osób, których dane dotyczą, oraz obowiązków spoczywających na administratorach danych i podmiotach przetwarzających bez żadnych wyraźnych ograniczeń czasowych byłyby de facto równoznaczne z całkowitym zawieszeniem tych praw. Stałoby to w sprzeczności z warunkiem wprowadzenia ograniczeń, zgodnie z którym takie ograniczenia nie mogą naruszać istoty podstawowych praw i wolności.

EROD zwraca jednocześnie uwagę, że w przypadku takich ograniczeń muszą znaleźć zastosowanie gwarancje przewidziane w art. 23 ust. 2 RODO – przepis ten precyzuje minimalny zakres informacji, które powinny znaleźć się w akcie prawnym wprowadzającym ograniczenia.

EROD zapowiada również wydanie w najbliższym czasie wytycznych dotyczących wdrożenia art. 23 RODO, który umożliwia państwom członkowskich wprowadzanie ograniczeń obowiązków i praw przewidzianych w RODO (art. 12–22, art. 34 oraz art. 5 RODO) na zasadach określonych w tym przepisie.

Źródło: https://edpb.europa.eu/our-work-tools/our-documents/autre/statement-restrictions-data-subject-rights-connection-state_en.

ORZECZNICTWO SĄDÓW KRAJOWYCH ORAZ WYTYCZNE I STANOWISKA ORGANÓW NADZORCZYCH

Transfer danych osobowych do państwa trzeciego - znaczenie wyroku w sprawie Schrems II

Xawery Konarski

W dniu 16 lipca 2020 r. Trybunał Sprawiedliwości Unii Europejskiej (TSUE) wydał wyrok w sprawie Schrems II (C-311/18). W artykule omawiamy najważniejsze ustalenia TSUE i wpływ wyroku na transfery danych osobowych do państw trzecich (w tym do USA).

Wyrok w sprawie Schrems I i stwierdzenie nieważności decyzji Komisji Europejskiej w sprawie tzw. Bezpiecznej Przystani

Sprawa ta została zainicjowana 25 czerwca 2013 r. skargą Maximiliana Schremsa, użytkownika Facebooka, wniesioną – z racji miejsca przetwarzania przez Facebook danych osobowych na terytorium Unii Europejskiej – do irlandzkiego organu ds. ochrony danych.

Maximilian Schrems zażądał w szczególności, aby jego dane osobowe nie były przekazywane przez Facebook Ireland na serwery Facebook Inc., zlokalizowane w Stanach Zjednoczonych, z uwagi na niespełnienie wymogu adekwatności ochrony danych osobowych w tym państwie. Skarga ta została oddalona przez organ irlandzki, który stwierdził, że ochrona taka jest zapewniona przez porozumienie UE – USA, ustanawiające tzw. Safe Harbour („Bezpieczna Przystań"). Ten mechanizm transferu danych, jako spełniający adekwatność ochrony, został potwierdzony decyzją Komisji Europejskiej nr 2000/520.

W wyniku procedury odwoławczej i skierowanego przez sąd irlandzki pytania prejudycjalnego do TSUE, Trybunał w wyroku z dnia 6 października 2015 r. w sprawie Schrems I stwierdził nieważność decyzji Komisji nr 2000/520 (C-362-14). W konsekwencji tego wyroku, sąd irlandzki uchylił decyzję organu irlandzkiego, a M. Schrems został wezwany do przeformułowania swojej skargi. Podtrzymał on w niej żądanie zakazania transferu danych do Stanów Zjednoczonych, kwestionując możliwość jego dokonania na innych, niż „Bezpieczna Przystań", mechanizmach transferowych. W ramach prowadzonego postępowania sąd irlandzki ponownie zwrócił się do TSUE z pytaniem prejudycjalnym, w którego wyniku doszło do wydania przez Trybunał wyroku z dnia 16 lipca 2020 r. (Schrems II).

Wyrok w sprawie Schrems II – najważniejsze ustalenia TSUE

Orzeczenie w sprawie Schrems II dotyczy oceny dopuszczalności transferów danych osobowych do Stanów Zjednoczonych, wykonywanych na podstawie dwóch mechanizmów określonych w RODO:

- Po pierwsze – tzw. Tarczy Prywatności, a więc porozumienia pomiędzy UE i USA, zastępującego „Bezpieczną Przystań". Zgodnie z decyzją Komisji Europejskiej nr 2016/1250 transfer danych do podmiotów dobrowolnie przyjmujących zasady ochrony danych osobowych zapisanych w Tarczy Prywatności był traktowany jako spełniający wymóg adekwatności ochrony w rozumieniu art. 45 ust. 1 RODO (poprzednio art. 25 ust. 6 dyrektywy 95/46/WE).
- Po drugie – standardowych klauzul umownych, zawartych w załączniku do decyzji Komisji Europejskiej nr 2010/87. Ten mechanizm transferowy jest z kolei wskazany jako podstawa przekazywania danych osobowych do państwa trzeciego w art. 46 ust. 2 lit. c RODO (poprzednio art. 26 ust. 2 dyrektywy 95/46/WE).

W wyroku z dnia 16 lipca 2020 r. TSUE stwierdził nieważność decyzji 2016/1250 w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA. Jak wynika z uzasadnienia orzeczenia, zadecydowały o tym ograniczenia ochrony danych osobowych, które wynikają z wewnętrznego prawa Stanów Zjednoczonych dotyczącego dostępu i wykorzystywania przez organy amerykańskie (np. NSA, FBI) danych osobowych przekazywanych z Unii Europejskiej. Dane te były wykorzystywane w ramach programów wywiadowczych PRISM i UPSTREAM.

Zdaniem Trybunału, regulacje te nie są zgodne z prawem ochrony danych osobowych Unii Europejskiej, ponieważ nie realizują wymogu proporcjonalności (art. 52 ust. 2 Karty Praw Podstawowych Unii Europejskiej, KPP). Nie zawierają one bowiem jasnych i precyzyjnych zasad regulujących zakres stosowania ustanowionych ograniczeń praw podmiotów danych osobowych, w szczególności nie wskazują zakresu tego ograniczenia, a także w jakich okolicznościach i na jakich warunkach można przetwarzać dane w celach wywiadowczych. Nie jest więc spełniony warunek ograniczenia ingerencji w prawo do prywatności i ochrony danych do sytuacji absolutnie niezbędnych.

Istotne jest również to, że zainteresowanym osobom (podmiotom danych) z Unii Europejskiej nie przyznano odpowiednich uprawnień w zakresie możliwości zaskarżenia do sądu decyzji amerykańskich służb wywiadowczych (art. 47 KPP).

Co istotne, **w wyroku stwierdzającym nieważność decyzji Komisji Europejskiej nr 2016/1250 dotyczącej Tarczy Prywatności nie określono okresu przejściowego (pkt 202 uzasadnienia wyroku). Oznacza to, że od 16 lipca 2020 r. transfery danych do USA dokonywane na tej podstawie są nieskuteczne**, ze wszystkim z tego wynikającymi konsekwencjami (np. możliwością nałożenia administracyjnej kary pieniężnej, o której mowa w art. 83 ust. 5 lit. c RODO).

Dokonując z kolei oceny decyzji Komisji Europejskiej nr 2010/87 w sprawie standardowych klauzul umownych, Trybunał potwierdził jej ważność. Nadal więc stanowią one ważny instrument transferu danych, na podstawie którego można dokonywać transferu danych do państwa trzeciego, w tym do Stanów Zjednoczonych.

Równocześnie jednak Trybunał podkreślił, że decyzja ta ustanawia obowiązek, by podmiot przekazujący dane (eksporter danych) i podmiot odbierający (importer danych) sprawdzili uprzednio, czy wymagany prawem UE stopień ochrony danych jest zapewniony w danym państwie trzecim. Decyzja ta zobowiązuje także importera danych do poinformowania eksportera danych z UE o ewentualnej niemożności zastosowania się do standardowych klauzul ochrony, w którym to przypadku do tego ostatniego należy zawieszenie przekazywania danych lub rozwiązanie umowy zawartej z importerem danych. Należy również pamiętać, że w takim przypadku właściwy krajowy organ nadzorczy może również skorzystać z własnych uprawnień (np. zakazać albo zawiesić przekazywanie danych) w stosunku do podmiotu będącego eksporterem danych z UE. Podstawą prawną takich decyzji jest art. 58 ust. 2 lit. f) oraz art. 58 ust. 2 lit. j RODO.

Praktyczne znaczenie wyroku w sprawie Schrems II

Podsumowując znaczenie wyroku w sprawie Schrems II, niewątpliwie wprowadziło ono element większego ryzyka prawnego w przypadku transferów danych do Stanów Zjednoczonych. Od dnia wydania wyroku nie można już bowiem bazować na decyzji Komisji Europejskiej stwierdzającej adekwatność ochrony w przypadku podmiotów samocertyfikujących się w ramach Tarczy Prywatności – tak już to bowiem zaznaczono wyżej, w wyroku z dnia 16 lipca 2020 r. TSUE nie określił okresu przejściowego.

Mimo że decyzja Komisji zatwierdzająca standardowe klauzule umowne pozostaje w mocy, to w wyroku wyraźnie podkreślono, że zawarcie umowy uwzględniającej te klauzule, nie czyni transferu - ”samo przez się” – dopuszczalnym. Należy bowiem również **dokonać uprzedniej oceny, czy importer danych jest w stanie spełnić warunki ochrony określone standardowymi klauzulami zatwierdzonymi przez Komisję Europejską**, w szczególności czy nie uniemożliwia mu tego wewnętrzne prawo obowiązujące w danym państwie trzecim. W przypadku transferów do Stanów Zjednoczonych, wykonywanych na podstawie tego mechanizmu transferowego, aktualne pozostaje pytanie, czy argumenty, które zadecydowały o unieważnieniu decyzji o Tarczy Prywatności nie powinny być brane pod uwagę przy ocenie dopuszczalności transferu na podstawie standardowych klauzul. W wyroku wyraźnie również zobowiązano unijne organy nadzorcze do wydawania decyzji o zakazie przekazywania danych w przypadku uznania, że warunki określone w standardowych klauzulach umownych nie są lub nie mogą być przestrzegane w danym państwie trzecim. Należy w związku z tym podkreślić, że powyższe wymogi dodatkowych działań w przypadku korzystania ze standardowych klauzul umownych dotyczą wszystkich transferów do państwa trzeciego (albo organizacji międzynarodowej), a więc nie tylko przekazywania danych osobowych do Stanów Zjednoczonych.

Spełnianie obowiązku informacyjnego wobec członków zarządu osób prawnych – stanowisko Prezesa UODO

Katarzyna Syska

W odpowiedzi na pytanie dotyczące konieczności spełniania obowiązku informacyjnego wobec członków zarządu osób prawnych Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO) uznał ich dane za dane osobowe w rozumieniu RODO i stwierdził, że zachodzi obowiązek spełnienia wobec tych osób obowiązku informacyjnego.

Na stronie internetowej Prezesa UODO opublikowana została odpowiedź na pytanie: „Co z obowiązkiem informacyjnym wobec członków zarządu osób prawnych?". Pytanie dotyczyło sytuacji, w której dane osobowe członków zarządu osoby prawnej lub innych osób uprawnionych do składania oświadczeń w imieniu określonego podmiotu znajdują się w treści dokumentacji dotyczącej postępowań administracyjnych.

Dane członków organów, pełnomocników, pracowników osób prawnych są danymi osobowymi

W pierwszej kolejności Prezes UODO zajął się tym, czy dane osób będących członkami organów osoby prawnej powinny być uznane za dane osobowe i czy podlegają one ochronie zgodnie z RODO[1].

W tym kontekście organ przywołał motyw 14 RODO, w którym wyjaśniono, że RODO nie dotyczy przetwarzania danych osobowych dotyczących osób prawnych, w szczególności przedsiębiorstw będących osobami prawnymi, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej. Prezes UODO odwołał się też do definicji danych osobowych.

W związku z powyższym Prezes UODO stwierdził, że „RODO chroni dane osobowe możliwych do zidentyfikowania osób fizycznych i wyklucza spod tej ochrony dane dotyczące osób prawnych".

Jeśli chodzi o osoby fizyczne będące członkami organów osób prawnych, Prezes UODO wskazał, że osoby te są zidentyfikowane (w myśl definicji danych osobowych). **W związku z tym ich dane są danymi osobowymi, a nie danymi osoby prawnej (w rozumieniu motywu 14 RODO).**

To samo dotyczy danych pełnomocników osób prawnych, a także danych pracowników, którzy są osobami kontaktowymi osoby prawnej, o ile osoby te są możliwe do zidentyfikowania.

Na co powołał się Prezes UODO?

Organ powołał się na odpowiedź Komisji Europejskiej na pisemne pytanie jednego z europosłów dotyczące m.in. motywu 14 RODO. Z odpowiedzi tej wynika, że RODO nie dotyczy danych kontaktowych osoby prawnej, np. adresu e-mail takiego jak ikeacontact@ikea.com. Natomiast dane osobowe pracowników osoby prawnej, w tym ich profesjonalne adresy e-mail, są objęte zakresem RODO (np. johnsmith@ikea.sk).

Ponadto przywołano wyrok Trybunału Sprawiedliwości UE w sprawie Manni. W wyroku tym Trybunał stwierdził, że dane osób fizycznych znajdujące się w rejestrach handlowych stanowią dane osobowe i że „okoliczność, iż informacje te wpisują się w ramy działalności zawodowej, nie oznacza, że nie można ich scharakteryzować jako dane osobowe".

Na marginesie warto przypomnieć, że Komisja Europejska zajęła takie samo stanowisko w swoich odpowiedziach dotyczących stosowania RODO. Komisja wskazała, że „RODO ma zastosowanie do wszystkich danych osobowych dotyczących osób fizycznych w związku z ich działalnością zawodową, między innymi do danych pracowników zatrudnionych w przedsiębiorstwie/organizacji, służbowych adresów e-mail typu »imię.nazwisko@firma.eu« lub numerów telefonów służbowych".

Konieczność spełniania obowiązku informacyjnego

Prezes UODO stwierdził, że skoro dane osób takich jak członkowie organów, pełnomocnicy, pracownicy, którzy są osobami kontaktowymi osoby prawnej, stanowią dane osobowe, to konieczne jest spełnienie wobec nich obowiązku informacyjnego, chyba że zachodzi przesłanka wyłączająca ten obowiązek.
Organ nie odniósł się jednak do tego, czy którakolwiek z przesłanek wyłączających obowiązek informacyjny mogłaby mieć w tym przypadku zastosowanie.

[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).

Odpowiedzialność administratora za pracowników - wyrok Sądu Najwyższego Zjednoczonego Królestwa

Iga Małobęcka-Szwast

Sąd Najwyższy Zjednoczonego Królestwa orzekł, że WM Morrisons Supermarkets plc (pracodawca) nie ponosi odpowiedzialności za działania nieuczciwego pracownika, który ujawnił dane osobowe 98 988 współpracowników. Sąd stwierdził jednak, że brytyjska ustawa o ochronie danych z 1998 r. (DPA 1998) nie wyklucza istnienia takiej odpowiedzialności zastępczej[1] w innym stanie faktycznym.

Stan faktyczny

Morrisons zapewnił pracownikowi dostęp do danych płacowych innych pracowników, aby mógł on przekazać te informacje zewnętrznemu audytorowi. Dane obejmowały dane osobowe pracowników, takie jak imię i nazwisko, adres, wynagrodzenie, dane rachunku bankowego i numery ubezpieczenia społecznego. Po dostarczeniu wymaganych informacji zewnętrznemu audytorowi pracownik, który miał pretensje do pracodawcy z powodu wcześniejszych działań dyscyplinarnych przeciwko niemu, opublikował na ogólnodostępnej stronie internetowej plik zawierający ww. dane pracowników Morrisons.

W następstwie naruszenia pracownicy Morissons, których dane wyciekły, wszczęli postępowanie bezpośrednio przeciwko Morrisons, zarzucając, że jest on odpowiedzialny zastępczo za czyny swojego pracownika. Roszczenia pracowników dotyczyły naruszenia ustawowych obowiązków wynikających z DPA 1998, w szczególności niewłaściwego wykorzystania informacji prywatnych i naruszenia poufności.

Wyrok Sądu Najwyższego

Sąd Najwyższy stwierdził, że w niniejszej sprawie Morrisons nie może być uznany za odpowiedzialnego za czyny swojego pracownika. Sąd Najwyższy zastosował ogólną zasadę odpowiedzialności zastępczej, zgodnie z którą aby pracodawcy ponosili odpowiedzialność zastępczą, bezprawne działania pracowników muszą być ściśle związane z ich obowiązkami zawodowymi i zadaniami, do których zostali upoważnieni przez pracodawcę.

W tym przypadku Sąd Najwyższy stwierdził, że publikowanie danych osobowych w Internecie nie było zadaniem, do którego pracownik był upoważniony, a zatem nie wchodziło w zakres jego „kompetencji i działalności". Sąd Najwyższy zauważył, że sam fakt, że zatrudnienie pracownika dało mu możliwość popełnienia czynu niezgodnego z prawem, nie jest wystarczający, aby uzasadnić nałożenie na pracodawcę odpowiedzialności zastępczej za taki czyn. W niniejszej sprawie Sąd uznał, że Morrisons (pracodawca) nie ponosi odpowiedzialności za naruszenie ochrony danych osobowych przez swojego pracownika, które miało na celu wyrządzić szkodę pracodawcy. Podkreślił, że motywacja pracownika i fakt, że nie działał on w interesie swojego pracodawcy, ale z powodów czysto osobistych, były ważnymi czynnikami przy ocenie sprawy.

Jednocześnie Sąd Najwyższy podkreślił, że brytyjska ustawa o ochronie danych z 1998 r. nie wyklucza istnienia takiej odpowiedzialności zastępczej w innym stanie faktycznym.

Odniesienie do polskiego systemu prawnego

Choć niniejsza sprawa powstała na gruncie systemu prawnego innego państwa członkowskiego, odpowiedzialność pracodawcy za zaniedbania i naruszenia przepisów o ochronie danych osobowych przez pracowników jest również szeroko dyskutowana na gruncie RODO i ma znaczenie dla polskiego systemu prawnego.

RODO wprost nie przewiduje odpowiedzialności pracowników za naruszenie przepisów RODO – odpowiedzialność tę ponoszą jedynie administrator i podmiot przetwarzający. Nie oznacza to jednak, że pracownicy nie ponoszą żadnej odpowiedzialności za swoje zaniedbania i naruszenia w zakresie ochrony danych osobowych. Takie zaniedbania i naruszenia mogą bowiem skutkować odpowiedzialnością dyscyplinarną, odszkodowawczą (względem pracodawcy) lub karną pracowników (art. 107 UODO[2]).

Źródło: Sprawa WM Morrison Supermarkets plc (Appellant) przeciwko Various Claimants (Respondents), [2020] UKSC 12, https://www.supremecourt.uk/cases/docs/uksc-2018-0213-press-summary.pdf.

[1] Sąd Najwyższy orzekał w tym przypadku o istnieniu „vicarious liability", czyli odpowiedzialności zastępczej (odpowiedzialności za czyny innych osób), która jest koncepcją wywodzącą się z angielskiego prawa dotyczącego czynów niedozwolonych. Zakłada ona ścisłą odpowiedzialność pracodawców za czyny niedozwolone, których dopuszczają się ich pracownicy.

[2] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

TSUE rozstrzygnie, czy organizacje konsumenckie mają legitymację do wnoszenia powództw za naruszenie RODO

Iga Małobęcka-Szwast

Decyzją z dnia 28 maja 2020 r. Federalny Trybunał Sprawiedliwości (BGH) zawiesił postępowanie wszczęte przez Niemiecką Federację Organizacji Konsumenckich (VZBV) przeciwko spółce Facebook Ireland Limited (Facebook) i skierował pytanie prejudycjalne do Trybunału Sprawiedliwości Unii Europejskiej (TSUE). BGH zmierza do ustalenia, czy VZBV jest uprawniona do wszczęcia postępowania cywilnego przeciwko podmiotowi dopuszczającemu się naruszenia RODO, niezależnie od naruszenia praw konkretnych osób, których dane dotyczą, oraz bez upoważnienia osoby, której dane dotyczą.

Stan faktyczny sprawy

Sprawa sięga 2014 r. (tj. przed wejściem w życie RODO[1]), kiedy to niemiecka Federacja Organizacji Konsumenckich (VZBV) wniosła pozew przeciwko spółce Facebook Ireland Limited (Facebook), zarzucając spółce naruszenie prawa ochrony danych osobowych (poprzednio obowiązującej federalnej ustawy o ochronie danych i dyrektywy 95/46/WE).

VZBV twierdzi, że klauzula informacyjna dotycząca przetwarzania danych osobowych w App Center (centrum aplikacji) na platformie internetowej Facebook, wyświetlana użytkownikom przed wyrażeniem zgody na ujawnienie ich danych osobowych podmiotom trzecim, jest niezgodna z wymogami prawnymi wynikającymi z prawa ochrony danych osobowych.

W szczególności w ocenie VZBV informacje przedstawione przez Facebook są niewystarczające, ponieważ zakres i cel przetwarzania danych są niejasne dla użytkowników. Zgoda użytkowników nie jest w pełni świadoma, a w konsekwencji również nie jest skuteczna. Takie działanie Facebooka VZBV ocenia jako nieuczciwą praktykę handlową w rozumieniu niemieckiej ustawy o przeciwdziałaniu nieuczciwym praktykom rynkowym (Gesetz gegen den unlauteren Wettbewerb, UWG). Nieuczciwy charakter tej praktyki upatruje w naruszeniu wymagań prawnych dotyczących uzyskania skutecznej zgody użytkownika na przetwarzanie jego danych osobowych. Jednocześnie powód oparł swoją legitymację do wniesienia pozwu na przepisach krajowych, tj. § 8 ust. 3 pkt 3 w zw. z § 3 i 3a UWG oraz § 3 ust. 1 pkt 1 w zw. z § 2 ust. 1 i ust. 2 pkt. 11 UKlaG.

Do argumentacji VZBV przychylił się zarówno berliński sąd okręgowy, jak i sąd apelacyjny orzekający w drugiej instancji.

Postępowanie przed BGH

Sprawa trafiła do I Senatu Cywilnego BGH, odpowiedzialnego m.in. za prawo konkurencji. Musi on rozstrzygnąć, czy naruszenie przez operatora sieci społecznościowej prawa ochrony danych osobowych w związku z informowaniem użytkowników tej sieci o zakresie i celu gromadzenia oraz wykorzystywania ich danych uzasadnia roszczenia o zaniechanie naruszenia i czy mogą być one dochodzone przez organizacje konsumenckie w drodze postępowania przed sądami cywilnymi.

Co ciekawe, BGH już raz zawiesił postępowanie w tej sprawie w oczekiwaniu na wyrok TSUE w sprawie Fashion ID (sprawa C-40/17). TSUE w wyroku z dnia 29 lipca 2019 r. potwierdził legitymację do występowania organizacji konsumenckiej (VZBV) przeciwko podmiotowi dopuszczającemu się naruszenia, jednak wyłącznie na gruncie poprzednio obowiązującej dyrektywy 95/46/WE. BGH uznał, że wyrok ten nie pozwala na podobną konkluzję na gruncie RODO, w szczególności że zagadnienie legitymacji organizacji konsumenckiej do wszczynania postępowania cywilnego przeciwko podmiotowi dopuszczającemu się naruszenia RODO jest kwestionowane w orzecznictwie i literaturze.

[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] Organizacja zrzeszająca stowarzyszenia ochrony konsumentów niemieckich krajów związkowych.

Niejasne brzmienie art. 80 RODO

Zgodnie z art. 80 RODO osoba, której dane dotyczą, ma prawo umocować organizację, która spełnia określone wymogi (nie ma charakteru zarobkowego, została należycie ustanowiona zgodnie z prawem krajowym, ma cele statutowe leżące w interesie publicznym i działa w dziedzinie ochrony praw i wolności osób, których dane dotyczą, w związku z ochroną ich danych osobowych), do wniesienia w imieniu tej osoby skargi, wykonywania w jej imieniu praw, o których mowa w art. 77[3], 78[4] i 79[5] RODO, oraz żądania w jej imieniu odszkodowania, o którym mowa w art. 82 RODO, jeżeli przewiduje to prawo państwa członkowskiego.

W ocenie BGH istnieją dwie sprzeczne interpretacje tego przepisu. Z jednej strony można argumentować, że prawo wszczęcia postępowania cywilnego przysługuje wyłącznie wtedy, gdy spełnione są wszystkie wymogi art. 80 RODO. Zdaniem BGH przepisy UWG i UKlaG, na które powołuje się VZBV, nie spełniają tych wymogów. Z drugiej strony przepis ten jest niejednoznaczny, dlatego organizacje konsumenckie powinny mieć możliwość wszczęcia postępowania cywilnego dotyczącego naruszeń RODO, niezależnie od naruszenia konkretnych praw poszczególnych osób, których dane dotyczą, i nawet bez upoważnienia osoby, której dane dotyczą.

Pytanie prejudycjalne

Z tego względu BGH zwrócił się do TSUE z pytaniem prejudycjalnym, które zmierza do ustalenia, czy przepisy rozdziału VIII, w szczególności art. 80 ust. 1 i 2 oraz art. 84 ust. 1 RODO, są sprzeczne z przepisami krajowymi, które z jednej strony przyznają konkurentom, a z drugiej strony stowarzyszeniom, instytucjom i izbom upoważnionym na mocy prawa krajowego (tj. UWG w zw. z UKlaG), uprawnienie do podjęcia kroków prawnych przed sądami cywilnymi za naruszenie przepisów o RODO przeciwko sprawcy naruszenia, niezależnie od naruszenia konkretnych praw poszczególnych osób, których dane dotyczą, i bez upoważnienia osoby, której dane dotyczą.

Praktyczne znaczenie i odniesienie do polskiego systemu prawnego

Zagadnienie legitymacji organizacji konsumenckich do wszczynania postępowań cywilnych na mocy RODO ma ogromne znaczenie praktyczne. Jeżeli TSUE (a w konsekwencji BGH) potwierdzi legitymację organizacji konsumenckich do wszczynania postępowania cywilnego za naruszenie przepisów o RODO przeciwko sprawcy naruszenia, abstrakcyjne naruszenia RODO mogłyby być dochodzone w sądzie przez organizacje konsumenckie (oraz inne organizacje pozarządowe spełniające wymogi art. 80 RODO), w oderwaniu od konkretnego naruszenia praw osoby, której dane dotyczą, i bez otrzymania od niej stosownego upoważnienia.

Warto zwrócić uwagę, że zagadnienie to ma istotne znaczenie również dla polskiego systemu prawnego. Ani Kodeks postępowania cywilnego, ani Kodeks postępowania administracyjnego, ani ustawa o ochronie danych osobowych[6] nie przewidują bowiem udziału organizacji społecznych w postępowaniu administracyjnym i sądowym w formie przewidzianej w art. 80 RODO. Polski prawodawca nie zdecydował się na uregulowanie tej kwestii w prawie krajowym. Nie jest zatem jasne, na jakich zasadach miałby się odbywać udział takich organizacji w ww. postępowaniach w wykonaniu art. 80 RODO.

Źródło: Decyzja BGH z dnia 28 maja 2020 r. (sygn. I ZR 186/17)
https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020066.html.

[3] Prawo do wniesienia skargi do organu nadzorczego.
[4] Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu.
[5] Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu.
[6] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

Wykorzystanie dronów a ochrona danych osobowych

Grzegorz Sibiga, Mateusz Kupiec

Urząd Ochrony Danych Osobowych (UODO) zajął się problematyką ochrony danych osobowych w związku z wykorzystywaniem dronów. W Unii Europejskiej obszar ten jest przedmiotem zainteresowania również innych organów i podmiotów.

Konferencja w UODO i przewodnik

W dniu 8 lipca 2020 r. UODO zorganizował Ogólnopolską Konferencję Naukową „Drony a prywatność". W jej trakcie pracownicy UODO oraz innych urzędów administracji publicznej, przedstawiciele środowiska naukowego i praktycy przedstawili m.in. problematykę naruszenia prywatności za pomocą dronów, zakresu zastosowania RODO[1] do działań z wykorzystaniem dronów oraz sposobu wykonania w tych działaniach określonych obowiązków zawartych w RODO, a także praktycznych aspektów wykorzystania dronów (np. do kontroli pracowników czy wspierania zadań straży gminnej). Ze strony kancelarii w konferencji uczestniczył dr hab. Grzegorz Sibiga z wystąpieniem „Działania z wykorzystaniem dronów a podstawowe zasady przetwarzania danych osobowych (art. 5 RODO)".

Po konferencji UODO planuje opracowanie poradnika o tematyce dotyczącej dronów w kontekście ochrony danych osobowych.

Działania innych organów i podmiotów

Zagadnienie prawidłowego wykorzystania dronów w kontekście RODO staje się również przedmiotem zainteresowania innych organów nadzorczych i podmiotów zajmujących się branżą bezzałogowych statków powietrznych. Do organów, które wypowiedziały się dotychczas na ten temat, należą:

- **Hiszpańska Agencja Ochrony Danych (AEPD);**
- **Information Commissioner's Office (ICO);**
- **Norweski Urząd Ochrony Danych (Datatilsynet).**

Problemem tym zajęła się również nieistniejąca już **Grupa Robocza Art. 29** (obecnie: Europejska Rada Ochrony Danych, EROD) **w opinii 01/2015** w sprawie kwestii ochrony danych i prywatności dotyczących wykorzystania dronów. Istotne znaczenie dla prawidłowego korzystania z dronów przez podmioty komercyjne w świetle regulacji o ochronie danych osobowych mają także **wytyczne opracowane w ramach kampanii informacyjnej Drones.eu**, która współfinansowana jest przez Komisję Europejską w ramach programu COSME. Poniżej omówimy krótko powyższe stanowiska i zalecenia.

Hiszpańska Agencja Ochrony Danych (AEPD)

Dnia 30 maja 2019 r. AEPD wydała broszurę „Drony i Ochrona Danych", w której dokonuje rozróżnienia operacji przy użyciu dronów na:

1. Operacje, których istotą jest przetwarzanie danych osobowych, np. monitoring.
2. Operacje, które nie wymagają przetwarzania danych osobowych, np. badania topograficzne. Operacje te są następnie dzielone na te, podczas których:

- nie ma ryzyka przypadkowego przetwarzania danych osobowych;
- istnieje ryzyko przypadkowego przetwarzania danych osobowych.

AEPD przedstawia również zalecenia odnośnie do urzeczywistnienia zasad ochrony danych osobowych podczas ich przetwarzania przy użyciu dronów. Szczególny nacisk położono na zasadę minimalizacji i ograniczenie ryzyka przypadkowego przetwarzania danych osobowych.

[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).

ICO

Brytyjski organ nadzorczy na swojej stronie internetowej opublikował zestaw ogólnych wskazówek dotyczących tego, w jaki sposób chronić prywatność innych podczas korzystania z dronów. Szczegółowe wytyczne odnośnie do problemu ochrony danych osobowych i bezzałogowych samolotów powietrznych można znaleźć w Kodeksie dobrych praktyk w sprawie CCTV (CCTV Code of Practice). Kodeks ten został opublikowany wprawdzie w stanie prawnym sprzed rozpoczęcia stosowania RODO, ale jego część dotycząca problematyki dronów nadal może być przydatna dla podmiotów wykorzystujących takie urządzenia.

Datatilsynet

Norweski organ nadzorczy również zabrał głos w sprawie problemu dronów i gwarancji dla osób, których dane osobowe są przetwarzane za pomocą tych urządzeń. Opublikowany przez niego przewodnik zawiera porady dla władzy publicznej i podmiotów prywatnych odnośnie do korzystania z bezzałogowych statków powietrznych.

Grupa Robocza Art. 29

Chociaż ustalenia Grupy Roboczej Art. 29 dotyczyły nieobowiązującej już dyrektywy 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, to zachowują one aktualność na gruncie RODO. W dokumencie tym Grupa Robocza przedstawia m.in.:

- analizę prawną zagadnienia dronów i ochrony danych osobowych;
- zalecenia dla producentów i operatorów dronów;
- zalecenia dla decydentów w zakresie ochrony danych osobowych;
- zalecenia dla organów ścigania.

Dronerules.eu

W ramach tej kampanii informacyjnej opublikowano kodeks postępowania w zakresie ochrony prywatności oraz poradnik dla producentów dronów dotyczący *privacy-by-design*. Chociaż dokumenty te nie mają wiążącej mocy prawnej, to zawierają cenne wskazówki dla podmiotów z branży samolotów bezzałogowych w zakresie ochrony danych osobowych, np. w przedmiocie realizacji zasady rozliczalności. Na stronie Dronerules.eu opublikowano również przykładowy wzór oceny skutków dla ochrony danych (DPIA) oraz listę kontrolną (checklist) z zakresu ochrony danych osobowych, którą personel operatora dronów powinien wypełnić przed rozpoczęciem lotu.

EROD publikuje nowy rejestr zawierający decyzje podjęte w ramach mechanizmu kompleksowej współpracy (one-stop-shop)

Iga Małobęcka-Szwast

Europejska Rada Ochrony Danych (EROD) opublikowała na swojej stronie internetowej nowy rejestr, zawierający decyzje podjęte przez krajowe organy nadzorcze w ramach mechanizmu kompleksowej współpracy (one-stop-shop). Aktualnie rejestr zawiera 110 decyzji przyjętych w ramach mechanizmu one-stop-shop, które mogą stanowić cenną wskazówkę dla podmiotów przetwarzających dane w różnych państwach członkowskich UE.

Mechanizm one-stop-shop

Na gruncie przepisów RODO organy nadzorcze mają obowiązek współpracy w sprawach o charakterze transgranicznym w celu zapewnienia spójnego stosowania RODO w ramach tzw. mechanizmu kompleksowej współpracy (one-stop-shop). Mechanizm ten, uregulowany w art. 60 RODO, przewiduje, iż wiodący organ nadzorczy odpowiada za przygotowanie projektów decyzji i współpracuje z organami nadzorczymi, których sprawa dotyczy, w celu osiągnięcia porozumienia.

Zgodnie z art. 60 RODO wiodący organ nadzorczy i organy nadzorcze, których sprawa dotyczy, wymieniają się wszelkimi stosownymi informacjami. Wiodący organ nadzorczy może w dowolnym momencie zwrócić się do innych organów nadzorczych, których sprawa dotyczy, o wzajemną pomoc i może realizować z nimi wspólne operacje, w szczególności w celu przeprowadzenia postępowania lub monitorowania wdrażania środka dotyczącego administratora lub podmiotu przetwarzającego posiadającego jednostkę organizacyjną w innym państwie członkowskim. Wiodący organ nadzorczy przekazuje innym organom, których sprawa dotyczy, stosowne informacje dotyczące danej sprawy i przedkłada im projekt decyzji w celu uzyskania ich opinii i należytego uwzględnienia ich uwag. Jeżeli inny organ nadzorczy, którego sprawa dotyczy, nie zgłosi sprzeciwu wobec projektu decyzji, uznaje się, że wiodący organ nadzorczy i organy nadzorcze, których sprawa dotyczy, porozumiały się w sprawie projektu decyzji i są nią związane. W razie przyjęcia decyzji wiodący organ nadzorczy doręcza ją odpowiednio głównej lub pojedynczej jednostce organizacyjnej administratora lub podmiotu przetwarzającego oraz informuje o decyzji inne organy nadzorcze, których sprawa dotyczy, oraz EROD, dołączając streszczenie stanu faktycznego i powodów decyzji.

Rejestr decyzji podjętych w ramach mechanizmu kompleksowej współpracy

Jak informuje EROD, do początku czerwca 2020 roku wiodące organy nadzorcze przyjęły 110 ostatecznych decyzji na podstawie mechanizmu one-stop-shop. Rejestr obejmuje dostęp do decyzji oraz ich streszczeń w języku angielskim przygotowanych przez sekretariat EROD. Stanowi on szczególnie wartościowe narzędzie dla praktyków ochrony danych, jak również dla podmiotów przetwarzających i administratorów prowadzących działania związane z przetwarzaniem danych w różnych krajach UE, którzy uzyskają dostęp do informacji o tym, jak w rzeczywistości wygląda współpraca organów nadzorczych w celu egzekwowania stosowania przepisów RODO.

Z opublikowanych w rejestrze decyzji wynika, że większość stwierdzonych naruszeń dotyczy wykonywania praw osób, których dane dotyczą, takich jak prawo dostępu (art. 15 RODO), prawo do usunięcia danych (art. 17 RODO) czy prawo do sprzeciwu (art. 21 RODO). Decyzje odnoszą się także m.in. do przetwarzania danych osobowych bez podstawy prawnej (art. 6 RODO) bądź z naruszeniem zasady przejrzystości (art. 12 RODO), do obowiązku informacyjnego (art. 13–14 RODO) czy też do obowiązku zapewnienia odpowiednich zabezpieczeń (art. 32 RODO).

Rejestr zawierający decyzje podjęte w ramach mechanizmu kompleksowej współpracy dostępny jest pod adresem: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en.

Źródło: https://edpb.europa.eu/news/news/2020/edpb-publishes-new-register-containing-one-stop-shop-decisions_en.

Komisja Europejska opublikowała raport z oceny RODO po dwóch latach stosowania

Mateusz Kupiec

W dniu 24 czerwca 2020 r. Komisja Europejska wydała długo wyczekiwany komunikat do Parlamentu Europejskiego i Rady „Ochrona danych jako filar wzmacniania pozycji obywateli oraz podejścia UE do transformacji cyfrowej – dwa lata stosowania ogólnego rozporządzenia o ochronie danych". Przedstawiamy najważniejsze uwagi i ustalenia KE po pierwszych dwóch latach stosowania RODO.

W ogólnym rozrachunku RODO okazało się sukcesem...

Zdaniem autorów raportu ostatnie dwa lata funkcjonowania RODO należy ocenić pozytywnie. Podkreślają oni, że wdrożenie RODO przede wszystkim:

- przyczyniło się do wzrostu świadomości prawnej Europejczyków odnośnie do ochrony danych osobowych, co potwierdzają opublikowane w czerwcu tego roku wyniki ankiety przeprowadzonej przez Agencję Praw Podstawowych Unii Europejskiej;
- umożliwiło osobom, których dane dotyczą, skuteczne dochodzenie swoich praw i zagwarantowało swobodny przepływ danych osobowych w UE;
- stało się wzorem do naśladowania dla powstających modeli ochrony danych osobowych na całym świecie (np. w Kenii, Japonii, amerykańskim stanie Kalifornia);

- sprawiło, że przedsiębiorstwa mają teraz tylko jeden zestaw zasad dotyczących ochrony danych, których muszą przestrzegać;
- spowodowało, że przedsiębiorstwa coraz częściej postrzegają dostosowanie organizacji do przepisów o ochronie danych osobowych jako element dający im przewagę konkurencyjną;
- dało krajowym organom nadzorczym odpowiednie narzędzia do egzekwowania przestrzegania przepisów RODO, np. kary administracyjne;
- okazało się elastyczne w zakresie wspierania rozwiązań cyfrowych w nieprzewidzianych okolicznościach, takich jak kryzys wywołany pandemią COVID-19.

...ale wciąż istnieje szereg obszarów wymagających poprawy

Niezależnie od powyższych osiągnięć Komisja zauważa, że:

- chętne korzystanie przez państwa członkowskie z możliwości wprowadzania wyjątków od zasad RODO w niektórych obszarach utrudnia harmonizację zasad ochrony danych osobowych w UE oraz prowadzenie działalności transgranicznej w zakresie nowych technologii i cyberbezpieczeństwa. KE wskazuje przykładowo na niejednakowe uregulowanie wieku, od którego dzieci mogą samodzielnie wyrażać zgodę na przetwarzanie ich danych osobowych w ramach korzystania z usług społeczeństwa informacyjnego (np. w Polsce granica ta wynosi 16 lat, podczas gdy w Belgii – 13 lat).
- odrębności prawne występują również w obszarze krajowych warunków dopuszczalności przetwarzania szczególnej kategorii danych osobowych (danych wrażliwych) oraz uregulowań dotyczących relacji między prawem do swobody wypowiedzi a prawem do ochrony danych osobowych;
- spełnienie obowiązków wynikających z RODO okazuje się szczególnie uciążliwe dla małych i średnich przedsiębiorstw. Podmiotom tym często bowiem brakuje odpowiedniego know-how oraz zasobów finansowych, aby prowadzić działalność w pełnej zgodności z RODO;
- organy nadzorcze nie wykorzystały jeszcze w pełni wszystkich przysługujących im uprawnień, np. w zakresie prowadzenia wspólnych dochodzeń;
- w sprawach transgranicznych potrzebne są bardziej zharmonizowane i skuteczne ustalenia między organami nadzorczymi. Brak personelu i zasobów po stronie niektórych z tych podmiotów jest postrzegany jako przyczyna, dla której nie udało się dotąd nawiązać ściślejszej współpracy między organami;
- istnieje potrzeba uaktualniania i dostosowywania standardowych klauzul umownych do zmieniających się realiów;
- brakuje spójnego podejścia ze strony krajowych organów nadzorczych do takich problemów jak stosowanie przesłanki prawnie uzasadnionego interesu czy pliki cookies;
- dochodzenie niektórych praw wynikających z RODO przez osoby, których dane dotyczą, jest wciąż utrudnione. Odnośnie do prawa do przenoszenia danych osobowych podkreślono, że jego skuteczność jest w zasadzie ograniczona do kilku sektorów. Nadal też nie określono precyzyjnie, jak należy rozumieć pojęcie formatu nadającego się do odczytu maszynowego.

Przyszłość RODO

Następny raport dotyczący stosowania RODO ma zostać opracowany w roku 2024. Do tego czasu w celu zapewnienia prawidłowego i skutecznego stosowania RODO Komisja między innymi:

- ukończy ocenę istniejących decyzji stwierdzających odpowiedni stopień ochrony danych osobowych w państwach trzecich;
- wzywa państwa członkowskie do przydzielania organom nadzorczym wystarczających środków do wykonywania ich zadań;
- zaleca państwom członkowskim, by rozważyły ograniczenie wprowadzania przepisów, które mogą powodować znaczące odrębności prawne i zagrażać swobodnemu przepływowi danych w UE;
- wskazuje, że może zaproponować zmiany w RODO mające na celu ujednolicenie wieku, od którego dzieci mogą samodzielnie wyrażać zgodę na przetwarzanie ich danych osobowych w ramach korzystania z usług społeczeństwa informacyjnego;
- wzywa krajowe organy nadzorcze i Europejską Radę Ochrony Danych (EROD) do wydawania jasnych i możliwych do zastosowania wytycznych związanych z ochroną danych osobowych.

Komentarz

Komunikat Komisji Europejskiej potwierdza, że w trakcie ostatnich dwóch lat stosowania RODO nastąpił intensywny wzrost poziomu ochrony i bezpieczeństwa danych osobowych w wielu branżach i sektorach. Jednostki w końcu otrzymały możliwość świadomego podejmowania decyzji dotyczących sposobu wykorzystania ich danych przez podmioty trzecie. Warto też zauważyć, że kolejnym wyzwaniem dla spójności stosowania RODO w państwach UE będzie interpretowanie przepisów rozporządzenia przez krajowe sądy. Pozytywnie należy odnieść się do postulatu KE w przedmiocie zwiększenia wsparcia państw członkowskich dla organów nadzorczych. Zapewnienie im odpowiednich zasobów może przyczynić się do wzrostu efektywności wykonywania przez nie swoich kompetencji, w tym w szczególności do skrócenia czasu rozpatrywania spraw.

Naruszenia ochrony danych osobowych dotyczące marketingu bezpośredniego

Dominika Nowak

W okresie od maja do lipca 2020 r. organy nadzorcze państw członkowskich nałożyły dwie administracyjne kary pieniężne w związku z naruszeniem ochrony danych osobowych w obszarze marketingu bezpośredniego. Przedstawiamy ich zestawienie i krótki komentarz.

Finlandia

Opis decyzji: Dnia 18 maja 2020 r. fiński organ nadzorczy nałożył na czołowego operatora pocztowego (Posti Oy) karę pieniężną w wysokości 100 000 euro. Naruszenie obejmowało 161 000 klientów w 2019 r.

Naruszenie to dotyczyło m.in. udzielania niewystarczających informacji osobom, których dane dotyczą, na temat uprawnień przysługujących im na gruncie RODO[1].

Osoby fizyczne złożyły zawiadomienie do organu nadzorczego, ponieważ otrzymywały komunikaty i marketing bezpośredni od różnych firm po tym, jak powiadomiły Posti Oy o zmianie adresu. W trakcie postępowania ujawniono, że Posti Oy nie poinformował osób, których dane dotyczą, o ich prawach, w tym o prawie do sprzeciwu wobec ujawniania danych, w szczególności w związku z powiadomieniami o zmianie adresu.

W ocenie organu operator pocztowy powinien wyraźnie poinformować swoich klientów o ich prawie do sprzeciwu wobec przetwarzania ich danych osobowych. Posti Oy przekazało takie informacje jedynie osobom, które oprócz powiadomienia o zmianie adresu zakupiły także dodatkowe usługi.

Więcej informacji:
https://edpb.europa.eu/news/national-news/2020/finnish-dpa-imposed-three-administrative-fines-data-protection-violations_en

Belgia

Opis decyzji: Belgijski organ nadzorczy nałożył administracyjną karę pieniężną w wysokości 1000 euro na stowarzyszenie za naruszenie art. 6 ust. 1, art. 17 ust. 1 lit. c i d oraz art. 21 ust. 3 i 4 RODO.

Organ nadzorczy zakwestionował następującą praktykę. Stowarzyszenie na podstawie prawnie uzasadnionego interesu (art. 6 ust. 1 lit. f RODO) wysyłało komunikaty marketingowe do byłych darczyńców w celu pozyskania środków. Administracyjna kara pieniężna została nałożona w następstwie skargi wniesionej do belgijskiego organu nadzorczego przez byłego darczyńcę. Stowarzyszenie nie zastosowało się do wniosku o usunięcie danych osobowych skierowanego na podstawie art. 17 ust. 1 RODO oraz sprzeciwu wniesionego zgodnie z art. 21 ust. 2 RODO. Ponadto uznano, że stowarzyszenie nie mogło skutecznie powołać się na prawnie uzasadniony interes jako podstawę przetwarzania, ponieważ nie spełniało ono kumulatywnych warunków nałożonych przez orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej, w szczególności wyroku w sprawie Rigas (C-13/16). W tym orzeczeniu określono trzy kumulatywne przesłanki legalności przetwarzania danych osobowych: po pierwsze, realizację uzasadnionych interesów przez administratora danych lub osoby trzecie, którym dane są ujawniane, po drugie, konieczność przetwarzania danych osobowych dla potrzeb wynikających z uzasadnionych interesów oraz po trzecie, przesłankę, aby prawa i wolności osoby objętej ochroną danych nie miały w danej sprawie pierwszeństwa nad uzasadnionym interesem administratora lub osoby trzeciej. Jest to tzw. test równowagi.

[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 szczególności organ nadzorczy miał wątpliwości, czy osoba, której dane dotyczą, mogłaby zasadnie oczekiwać, że jej dane będą przetwarzane do celów marketingu bezpośredniego wiele lat po zebraniu tych danych. Ponadto nie ułatwiono podmiotom danych w wystarczający sposób prawa do wniesienia sprzeciwu.

Więcej informacji:
https://edpb.europa.eu/news/national-news/2020/belgian-dpa-imposed-fine-1000-eur-association-sent-direct-marketing-messages_en.

Komentarz

Z powyższych decyzji wynikają następujące wnioski dla podmiotów prowadzących działalność marketingową:

- Niezwykle istotne dla administratora jest wyraźne poinformowanie podmiotu danych o prawie do wniesienia sprzeciwu wobec przetwarzania danych osobowych (art. 21 ust. 4 RODO).
- Administrator powinien przeprowadzić tzw. test równowagi, jeżeli prowadzi marketing bezpośredni na podstawie prawnie uzasadnionego interesu.
- Osoba, której dane dotyczą, nie może zasadnie oczekiwać, że dostanie komunikat marketingowy, jeżeli ostatni kontakt ze strony administratora nastąpił wiele lat temu. Jednym z czynników świadczących o występowaniu prawnie uzasadnionego interesu jest upływ czasu od ostatniego kontaktu z podmiotem danych.

NR 2 - LIPIEC 2020

ARTYKUŁY I PUBLIKACJE

#czasopisma

„Przepisy uzupełniające o ochronie danych osobowych” - artykuł autorstwa **dr. hab. Grzegorza Sibiga** na temat przepisów ustaw znowelizowanych ustawą z 21.02.2019 r. dotyczących przetwarzania i ochrony danych osobowych w sektorze publicznym, który ukazał się w kwietniowym numerze czasopisma „IT w administracji” (nr 4/2020).

„Decyzje Prezesa UODO wiążą sądom ręce” – wywiad z **dr. hab. Grzegorzem Sibiga**, w którym przedstawia on swoją ocenę przepisów procesowych z polskiej ustawy o ochronie danych osobowych dotyczących m.in. związania sądu decyzją Prezesa UODO i relacji między postępowaniem administracyjnym a postępowaniem sądowym (art. 95-97 ustawy o ochronie danych osobowych). Wywiad ukazał się w Dzienniku Gazecie Prawnej z dnia 7 lipca 2020 r.

NADCHODZĄCE WYDARZENIA

#webinar

Zasady monitoringu wizyjnego w świetle decyzji i stanowisk organów nadzorczych w UE

Plan webinarium

Podczas webinarium przedstawimy przegląd kar nakładanych przez unijne organy nadzorcze w związku z prowadzeniem monitoringu wizyjnego. Wnioski płynące z tych decyzji mają kluczowe znaczenie dla prawidłowego i zgodnego z prawem wdrożenia systemów monitoringu wizyjnego zarówno w Polsce, jak i w innych krajach Unii Europejskiej. Omówimy także kluczowe elementy wytycznych dotyczących monitoringu wizyjnego. W szczególności skupimy się na następujących sprawach:

1. Kary nakładane przez organy unijne nadzorcze w związku prowadzeniem monitoringu oraz podstawy nałożenia kar

- Przegląd nałożonych kar pieniężnych i ich wysokość
- Jak zapewnić legalność przetwarzania danych w ramach monitoringu wizyjnego?
- Jak oceniać zakres danych zbieranych w drodze monitoringu?
- O czym należy informować w związku z prowadzeniem monitoringu wizyjnego?
- Czy konieczne jest przeprowadzenie DPIA?

2. Zasady monitoringu w świetle wytycznych EROD, Prezesa UODO oraz orzeczeń sądów

- Co wynika z wytycznych EROD nr 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo?
- Jakie są wskazówki Prezes UODO dotyczące monitoringu wizyjnego?

3. Praktyczne problemy dotyczące stosowania monitoringu (w szczególności monitoringu wizyjnego)

Prelegenci: Zespół RODO Traple Konarski Podrecki i Wspólnicy

Rejestracja >>

ZESPÓŁ RODO

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

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

Katarzyna Syska
Adwokat
katarzyna.syska@traple.pl

Dominika Nowak
Radca prawny
dominika.nowak@traple.pl

dr Iga Małobęcka-Szwast LL.M.
Starszy prawnik
iga.malobecka@traple.pl

Mateusz Kupiec
Stażysta
mateusz.kupiec@traple.pl

Pytania prosimy kierować na adres:
rodo@traple.pl