NR 2 - MARZEC-KWIECIEŃ 2022

NEWSLETTER RODO

W numerze m.in.:

- Administracyjna kara pieniężna została po raz pierwszy nałożona w jednym postępowaniu na administratora i podmiot przetwarzający
- Decyzja organu belgijskiego w sprawie mechanizmu (TCF 2.0)
- RODO i chmura – wytyczne Datatilsynet
- Wytyczne DSK ws. marketingu bezpośredniego
- Były pracownik nie jest zaufanym odbiorcą danych – wnioski z decyzji Prezesa UODO

Traple Konarski Podrecki & Wspólnicy

TKP

Administracyjna kara pieniężna została po raz pierwszy nałożona w jednym postępowaniu na administratora i podmiot przetwarzający

Dominika Nowak

Stan faktyczny

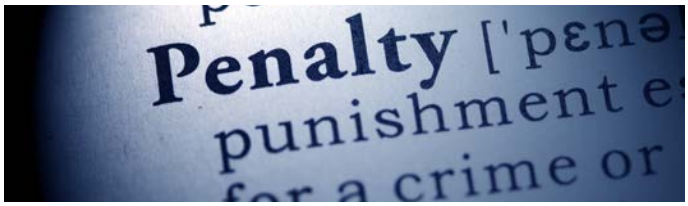
W kwietniu 2020 r. firma Fortum Marketing and Sales SA (dalej: „Fortum" lub „Administrator") zgłosiła Prezesowi UODO naruszenie ochrony danych osobowych. Zgodnie ze zgłoszeniem doszło do skopiowania danych klientów Administratora w związku z wprowadzeniem zmiany w środowisku teleinformatycznym w ramach systemu służącego do cyfrowej archiwizacji dokumentów. W zakresie tego systemu Fortum współpracował z PIKA sp. z o.o. (dalej: „PIKA" lub „podmiot przetwarzający").

W kwietniu 2020 r. Fortum zgłosił Prezesowi UODO naruszenie ochrony danych osobowych. W zgłoszeniu wskazano, że doszło do skopiowania danych klientów Fortum. To zdarzenie miało związek z wprowadzeniem zmiany w środowisku teleinformatycznym dla ww. usługi w celu poprawienia wydajności działania całego repozytorium. Naruszenie dotyczyło nowej bazy danych, zawierającej takie informacje o klientach Fortum, jak: imię i nazwisko, adres zamieszkania lub pobytu, numer PESEL, rodzaj, seria i numer dokumentu tożsamości, adres e-mail, numer telefonu, numer i adres punktu poboru oraz dane dotyczące umowy (np. data i numer umowy, rodzaj paliwa, numer licznika). Wskazano, że naruszenie dotyczy 137 314 osób.

Najpierw, w kwietniu, Prezes UODO wszczął postępowanie administracyjne z urzędu wobec Fortum. W odpowiedzi na zawiadomienie firma wyjaśniła, że wprowadzone zmiany i sposób ich wprowadzenia nie zostały z nią skonsultowane przez PIKA. Fortum współpracuje z PIKA na podstawie umowy przechowywania (archiwum dokumentów) wraz z usługami towarzyszącymi zawartej w 2016 r. oraz umowy powierzenia przetwarzania z maja 2018 r. W piśmie z czerwca 2018 r., w odpowiedzi na pytania organu, Administrator wyjaśnił, że przed zawarciem umowy powierzenia przetwarzania nie przeprowadził dodatkowej weryfikacji podmiotu przetwarzającego, ponieważ Fortum od wielu lat współpracuje z PIKA – jest to lider na rynku usług archiwizacji i digitalizacji. Wcześniej nie dochodziło do incydentów bezpieczeństwa. Fortum przyznał, że nie realizował względem PIKA prawa kontroli z art. 28 ust. 3 lit. h RODO[1]. W maju 2020 r., czyli po stwierdzeniu naruszenia, Administrator wysłał do podmiotu przetwarzającego ankietę, stanowiącą pierwszy element procesu weryfikacji.

W wyjaśnieniach z czerwca 2020 r. Fortum wskazał, że PIKA, wdrażając zmianę, nie zastosowała się do przyjętych procedur i nie przedstawiła Administratorowi koncepcji zmian ani projektów funkcjonalnych lub technicznych.

Następnie, w piśmie z lipca 2020 r., Prezes UODO zawiadomił PIKA o uznaniu jej za stronę prowadzonego postępowania administracyjnego. Składając wyjaśnienia, PIKA wskazała, że nie konsultowała z Administratorem wdrożenia zmian w oprogramowaniu. Fortum zgłosił problem w działaniu oprogramowania. PIKA zidentyfikowała przyczynę i rozpoczęła rozwiązywanie problemu bez konsultacji z Fortum.



Rozstrzygnięcie i argumenty Prezesa UODO

W decyzji z 19 stycznia 2022 r. Prezes UODO:

- stwierdził naruszenie przez Fortum art. 5 ust. 1 lit. f, art. 24 ust. 1, art. 25 ust. 1, art. 28 ust. 1 oraz art. 32 ust. 1 i 2 RODO, tj. niewdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych, skutkujące naruszeniem ich poufności, oraz brak weryfikacji podmiotu przetwarzającego, czy zapewnia on wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą, i nałożył za naruszenie ww. przepisów administracyjną karę pieniężną w wysokości 4 911 732 zł;

[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).

- stwierdził naruszenie przez PIKA art. 32 ust. 1 i 2 oraz art. 32 ust. 1 i 2 w związku z art. 28 ust. 3 lit. c i f RODO, tj. niewdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych, w tym zapewnienie ich poufności, i nałożył na PIKA administracyjną karę pieniężną w wysokości 250 135 zł.

Organ wskazał, że:

- nie ustanowiono odpowiednich zabezpieczeń bazy danych, w której przetwarzane są dane osobowe, co doprowadziło do nieuprawnionego dostępu (wprowadzenie takich zabezpieczeń jest jednym z wzorcowych elementów bezpieczeństwa na podstawie normy ISO 27001:2017-06);
- nie dokonano pseudonimizacji danych osobowych w nowo powstałej bazie, co w połączeniu z brakiem innych skutecznych zabezpieczeń doprowadziło do wystąpienia naruszenia ochrony danych;
- polityki stosowane przez PIKA nie zawierały szczegółowych postanowień odnośnie do sposobu dokonywania zmian w systemach informatycznych służących do przetwarzania danych osobowych;
- ewidencjonowanie przez PIKA prac dla klientów w wewnętrznym systemie nie jest wystarczające do zapewnienia bezpieczeństwa danych osobowych, gdyż poszczególne etapy prac nie są dostatecznie udokumentowane;
- PIKA działała wbrew umowie powierzenia przetwarzania zawartej z Fortum, ponieważ nie została wdrożona pseudonimizacja;
- PIKA nie zachowała należytej staranności, zasilając rzeczywistymi danymi osobowymi nowo utworzoną bazę danych;
- Fortum nie prowadził nadzoru nad tym, jak faktycznie przebiega wdrożenie zmian w usłudze;
- Fortum, jako administrator, nie jest zwolniony z realizacji obowiązków związanych z zapewnieniem bezpieczeństwa danych osobowych ze względu na korzystanie z usług podmiotu przetwarzającego;
- Fortum nie przeprowadzał u podmiotu przetwarzającego audytów, w tym inspekcji na podstawie art. 28 ust. 3 lit. h RODO, podczas gdy jest to jeden z istotniejszych środków bezpieczeństwa – to uprawnienie jest powiązane z obowiązkiem nałożonym na administratora z art. 28 ust. 1 RODO, czyli wyborem odpowiedniego podmiotu przetwarzającego.

Prezes UODO uznał, że ani Administrator, ani podmiot przetwarzający nie wdrożyli odpowiednich środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych, co stanowi naruszenie art. 32 RODO.

Ponadto Prezes UODO uznał, że długotrwała współpraca stron, która nie jest poparta okresowym, systematycznym przeprowadzaniem audytów bądź inspekcji, nie gwarantuje, że procesor w sposób prawidłowy wykona zadania wymagane przepisami oraz wynikające z umowy powierzenia przetwarzania. Dotychczasowa współpraca może stanowić wyłącznie punkt wyjścia do wykonywania weryfikacji podmiotu przetwarzającego. Zawarcie umowy powierzenia przetwarzania bez przeprowadzenia odpowiedniej weryfikacji nie jest wystarczające do spełnienia przez administratora obowiązków z art. 28 ust. 1 RODO.

Komentarz

W niniejszej sprawie Prezes UODO po raz pierwszy nałożył w jednym postępowaniu administracyjnym karę pieniężną jednocześnie na administratora i podmiot przetwarzający. Decyzja ta jest przełomowa ze względu na to, że pokazuje, jak istotne jest wykonywanie przez administratora obowiązku z art. 28 ust. 1 RODO, czyli weryfikowanie podmiotu przetwarzającego przed zawarciem umowy powierzenia przetwarzania.

Ponadto organ nadzorczy uznał, że obowiązek podmiotu przetwarzającego z art. 28 ust. 3 lit. h RODO, czyli udostępnienie administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków z art. 28 RODO oraz umożliwianie administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzania audytów, w tym inspekcji, powinien być – zdaniem organu – skorelowany z faktycznym przeprowadzeniem przez administratora takich audytów. Innymi słowy, korzystanie z usług outsourcingu nie zwalnia administratora z nadzoru nad takim podmiotem przetwarzającym, w tym ze sprawdzania, czy realizuje on zawartą umowę powierzenia przetwarzania. W praktyce oznacza to, że każdy administrator, który korzysta z usług outsourcingu, powinien zweryfikować, czy przeprowadził sprawdzenie procesora przed zawarciem umowy, w trybie art. 28 ust. 3 RODO, oraz powinien zaplanować przeprowadzanie audytów u procesora zgodnie z art. 28 ust. 3 lit. h RODO.

Decyzja belgijskiego organu ds. ochrony danych osobowych w sprawie TCF 2.0 – znaczenie dla rynku reklamy cyfrowej

Xawery Konarski

Istota TCF w ekosystemie reklamy cyfrowej

W dniu 2 lutego 2022 r. Belgijski Urząd Ochrony Danych (APD) wydał decyzję w sprawie narzędzia *Transparency & Consent Framework* (TCF), zarządzanego przez IAB Europe. Jest ona wynikiem prowadzonego przez belgijski urząd postępowania mającego na celu zbadanie zgodności funkcjonowania TCF z przepisami ochrony danych osobowych.

TCF to narzędzie, z którym spotykamy się na co dzień przeglądając strony internetowe. W uproszczeniu jest to system wyskakujących okienek (*pop-up*), które pojawiają się po wejściu na większość witryn w sieci. Za ich pomocą przekazywane są użytkownikom informacje wymagane przez RODO, po to by mogli oni udzielić świadomej zgody na przetwarzanie danych osobowych przy użyciu *cookies*, w tym na wyświetlanie spersonalizowanych reklam.

Dla całego ekosystemu reklamowego TCF, uruchomiony w kwietniu 2018 r., ma olbrzymie znaczenie. Stworzone w *open source* rozwiązanie ma na celu zapewnienie spełnienia wymogów RODO i przepisów o e-Prywatności w związku ze stosowaniem przez firmy z branży reklamowej plików cookies. W ramach TCF, IAB Europe stworzyła wspólny system klasyfikacji wszystkich możliwych czynności oraz celów przetwarzania danych, istotnych z punktu widzenia reklamy internetowej. Dzięki temu zapewniono standaryzację sposobów w jaki strony internetowe zabiegają o zgodę użytkownika na przetwarzanie danych przez te strony oraz przez strony trzecie, rejestrowania informacji o wyborach dokonywanych przez użytkowników oraz przekazywania tych informacji podmiotom trzecim. Mechanizm TCF zapewnia internautom możliwość określenia ich preferencji co do celów, na które ich dane mają być przetwarzane (np. analityka, reklama), jak i podmiotów, które mogą te dane wykorzystywać. Preferencje te są zapisywane w TCF i udostępniane podmiotom uczestniczącym w łańcuchu reklamy internetowej (np. wydawcy, platformy reklamy programatycznej).

Znaczenie prawne i zaskarżenie decyzji APD przez IAB Europe

Belgijski organ ds. ochrony danych osobowych zakwestionował spełnienie przez TCF niektórych wymogów RODO, takich jak na przykład odpowiedni sposób i zakres poinformowania internautów o przetwarzaniu ich danych osobowych. Wydana przez APD decyzja została w dniu 4 marca 2022 r. zaskarżona przez IAB Europe do sądu belgijskiego. Niezależnie od zaskarżenia decyzji, IAB Europe powołało Task Force analizujący uwagi belgijskiego urzędu. IAB Europe złożyło również wniosek o wstrzymanie wykonalności decyzji do czasu ostatecznego rozstrzygnięcia sprawy.

IAB Europe nie zgadza się ze stanowiskiem belgijskiego organu nadzorczego, że organizacja ta jest administratorem informacji o preferencjach użytkowników, a co za tym idzie odpowiada między innymi za podstawę prawną przetwarzania tych informacji. IAB Europe jest bowiem tylko organizatorem systemu TCF, a informacje te we własnym zakresie wykorzystują podmioty z łańcucha reklamy internetowej (np. wydawcy, czy dostawcy platform SSP, DSP oraz DMP). IAB Europe jedynie więc dostarcza rozwiązanie, same decyzje o wykorzystaniu danych zapisanych w TCF podejmują natomiast podmioty korzystające z tego rozwiązania. Podkreślono również, że IAB Europe jako twórca TCF w żaden sposób nie determinuję, jakie konkretne działania związane z przetwarzaniem danych osobowych podejmują podmioty korzystające z narzędzia. To wyłącznie użytkownicy TCF decydują, do którego z celów skatalogowanych w TCF należy zaliczyć działania związane z przetwarzaniem danych, a następnie wykorzystują ten system klasyfikacji do przekazywania informacji innym osobom i podmiotom. TCF nie „nakazuje" więc ani nie uruchamia operacji przetwarzania danych. Decyzje dotyczące określenia celów i środków przetwarzania danych osobowych podejmowane są wyłącznie przez użytkowników TCF, bez udziału IAB Europe, które również nie ma dostępu do przechowywanych

danych o wyborach podjętych przez podmioty danych (np. zgoda na przetwarzanie na cele reklamowe).

Na marginesie skargi IAB Europe należy podkreślić, że sam mechanizm TCF jako narzędzie służące do informowania i określeni podstawy przetwarzania danych, nie został jednak zakwestionowany. To samo dotyczy stosowania pop-up do przekazania informacji użytkownikom. Decyzja belgijskiego organu wiąże również tylko i wyłącznie IAB Europe, a nie podmioty będące uczestnikami TCF, ponieważ nie są one stronami postępowania. Zakwestionowanie mechanizmu TCF przez któryś z krajowych organów ochrony danych wymaga zainicjowania oddzielnego postępowania. Z wstępnych informacji uzyskanych w innych państwach wynika jednak, że organy do spraw ochrony danych osobowych zamierzają poczekać na ostateczne rozstrzygnięcie sprawy przez belgijski sąd. Warto również zaznaczyć, że inaczej niż w Belgii, w Polsce w sprawach instalowania cookies właściwy jest nie Prezes Urzędu Ochrony Danych Osobowych, lecz Prezes Urzędu Komunikacji Elektronicznej.

Wpływ decyzji APD na rynek reklamy internetowej

Niezależnie od ostatecznego rozstrzygnięcia w sprawie decyzji APD z pewnością cały postępowanie będzie miał istotny wpływ na sposób funkcjonowania reklamy internetowej. IAB Europe zapewnia przy tym, że będzie ściśle współpracować z APD i innymi organami ochrony danych w celu implementacji wszystkich niezbędnych wytycznych i mechanizmów monitorowania, aby zapewnić ciągłą użyteczność TCF na rynku. W związku z tym IAB Europe złożył do APD tzw. plan naprawczy, do którego został zobowiązany w decyzji z dnia 2 lutego 2022 r. Plan ten, po jego zatwierdzeniu przez organ, ma być wdrożony w ciągu następnych 6 miesięcy. Jedną z najważniejszych propozycji IAB Europe jest rezygnacja z prawnie uzasadnionego interesu jako podstawy prawnej przetwarzania danych.

Kompetencje Prezesa UODO w kontekście wyroku NSA z dnia 10 lutego 2022 r., sygn. akt III OSK 5028/21

Bartłomiej Żeromski

W lutym br. przed Naczelnym Sądem Administracyjnym (NSA) zawisła sprawa dotycząca tego, czy Prezes Urzędu Ochrony Danych Osobowych (UODO) ma kompetencje do rozstrzygania spraw, których przedmiotem są nieprawidłowości w procesie przetwarzania danych osobowych, zaistniałych przed rozpoczęciem stosowania RODO oraz przed wejściem w życie Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r., poz. 1781; dalej: „ustawa z 2018 r.").

Stan faktyczny

W maju 2020 r. do polskiego organu nadzorczego wpłynęła skarga pracownicy jednego z sądów rejonowych. Kwestionowane zdarzenie miało polegać na udostępnieniu w styczniu 2018 r. pisma zawierającego dane osobowe skarżącej pracownikom tego sądu. Pismo, które skarżąca skierowała do zespołu ds. przeciwdziałania mobbingowi, zostało załączone do zarządzenia wewnętrznego i przekazane pracownikom sądu.

Prezes UODO w czerwcu 2020 r. wydał postanowienie, mocą którego odmówił wszczęcia postępowania w sprawie, wskazując, że kwestionowane zdarzenie zaistniało w czasie obowiązywania Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922; dalej: „ustawa z 1997 r.").

W wydanym rozstrzygnięciu organ wskazał, że jednym z zadań Prezesa UODO jest prowadzenie postępowań w sprawie stosowania RODO[1] (art. 57 ust. 1 lit. h RODO). Natomiast zgodnie z przepisami przejściowymi zawartymi w obecnie obowiązującej ustawie o ochronie danych osobowych (art. 160 ust. 2 ustawy z 2018 r.) Prezes UODO prowadzi sprawy wszczęte i niezakończone przed wejściem w życie ustawy z 2018 r. na podstawie ustawy z 1997 r. Jednocześnie brak przepisu, który umożliwia prowadzenie postępowania przez ten organ, gdy zdarzenie miało miejsce przed wejściem w życie ustawy z 2018 r., a żądanie wszczęcia postępowania w sprawie zostało złożone po tym terminie.

Wojewódzki Sąd Administracyjny w Warszawie (WSA) w wyroku z dnia 12 grudnia 2020 r., sygn. akt II SA/Wa 1389/20, podzielił powyższe stanowisko, a następnie Naczelny Sąd Administracyjny wyrokiem z dnia 10 lutego 2022 r. w sprawie III OSK 5028/21 oddalił skargę kasacyjną od wyroku WSA. NSA w uzasadnieniu wyroku podniósł, że przepisy ustawy z 1997 r. zachowały swoją moc w zakresie objętym tzw. dyrektywą policyjną do 6 lutego 2019 r., co oznacza, że w pozostałych sprawach nie mają one zastosowania.

Konsekwencje

Orzeczenia wydane w tej sprawie dotyczą wyłącznie sytuacji, w których zdarzenie mające podlegać ocenie się zakończyło. Oznacza to, że jeżeli doszło do jednorazowego udostępnienia danych i proces ten nie jest kontynuowany, to organ nie ma podstaw prawnych do badania legalności tego zdarzenia. Ustawa z 1997 r. została uchylona, a możliwość jej stosowania dotyczy obecnie wyłącznie spraw, które zostały wszczęte na gruncie tej ustawy i nie zostały do tej pory ostatecznie zakończone.

[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).

Powyższe nie dotyczy sytuacji, w których kwestionowany proces przetwarzania zaczął się przed rozpoczęciem stosowania RODO i był kontynuowany po jego rozpoczęciu. Przykładowo jeżeli w przedmiotowej sprawie pismo skarżącej zostałoby opublikowane na stronie BIP sądu w okresie od stycznia 2018 r. do czerwca 2018 r., to taki proces podlegałby ocenie organu, nawet gdyby żądanie wszczęcia postępowania zostało złożone do organu w maju 2020 r.

Stanowisko to pośrednio wskazuje też, że organ nie może stosować uprawnień o charakterze sankcyjnym, tj. kary pieniężnej lub upomnienia, do uchybień w procesie przetwarzania danych zaistniałych przed 25 maja 2018 r., jeżeli wszczął postępowanie w sprawie przetwarzania danych po tej dacie. Jeżeli organ wyda rozstrzygnięcie w przedmiocie kary pieniężnej, wskazując, że w ramach jej miarkowania wziął pod uwagę czas trwania naruszenia, które rozpoczęło się przed 25 maja 2018 r., to jest to podstawa do zaskarżenia rozstrzygnięcia.

Jednocześnie podnieść należy, że stanowisko zarówno organu, jak i sądów administracyjnych w tej sprawie zasługuje na aprobatę. Brak jest przepisu umożliwiającego ocenę zgodności postępowania administratora przez Prezesa UODO z przepisami ustawy z 1997 r., chyba że w warunkach art. 160 ust. 2 ustawy z 2018 r. Ustawa z 1997 r. została uchylona i brak jest organu, który mógłby badać prawidłowość stosowania przepisów w niej zawartych.

W kontekście powyższego powstaje jednak pytanie, czy organ, oceniając proces przetwarzania danych, który rozpoczął się przed 25 maja 2018 r. i jest obecnie kontynuowany, może ocenić okoliczności, które zdarzyły się pod rządami poprzednio obowiązujących przepisów. Sama legalność pozyskania danych determinuje przecież możliwość dalszego ich przetwa-rzania. Jeżeli więc organ nie mógłby dokonać oceny pozyskania danych, nawet jeśli doszło do niego przed wejściem w życie ustawy z 2018 r., to w konsekwencji nie mógłby też dokonać prawidłowej oceny w sprawie.

Prowadzenie każdego postępowania administracyjnego przed organem musi zmierzać do wydania decyzji administracyjnej pozostającej w kompetencji tego organu. Skoro niezależnie od stanu faktycznego brak jest możliwości zastosowania art. 58 ust. 2 RODO do zdarzeń zakończonych przed 25 maja 2018 r., to organ nie może prowadzić postępowania w sprawie, bo każde takie postępowanie musiałoby się zakończyć umorzeniem. Jednocześnie ocena legalności pozyskania danych jest niezbędnym elementem oceny stanu faktycznego w sprawie, dlatego zasadne wydaje się, żeby organ mógł ocenić legalność pozyskania danych zgodnie z przepisami obowiązującymi w chwili pozyskania danych. W konsekwencji organ wyda decyzję odnoszącą się do trwającego już po 25 maja 2018 r. procesu przetwarzania danych, biorąc pod uwagę całą historię procesu ich przetwarzania, w tym m.in. wykonanie obowiązków informacyjnych czy wpływ cofnięcia zgody na przetwarzanie danych przed 25 maja 2018 r.

Wytyczne BayLfD ws. korzystania z faksu

Mateusz Kupiec

Faks to wciąż popularny środek do przesyłania dokumentów przez podmioty publiczne oraz prywatne. Faksy są wykorzystywane do komunikacji wewnętrznej oraz zewnętrznej, a nierzadko przekazywane za ich pomocą dokumenty zawierają dane osobowe. W jednym z poprzednich numerów naszego newslettera przedstawialiśmy komunikat heskiego organu nadzorczego z zakresu ochrony danych osobowych, który stwierdził, że korzystanie z faksu na potrzeby przetwarzania danych osobowych może co do zasady skutkować naruszeniem przepisów RODO[1].

W ostatnim czasie bawarski organ nadzorczy (Bayerischen Landesbeauftragten für den Datenschutz, BayLfD) opublikował wytyczne dla podmiotów z sektora publicznego dotyczące ochrony danych osobowych w związku z korzystaniem z faksu. Wskazówki organu mogą być przydatne dla podmiotów decydujących się na dalsze przesyłanie dokumentów za pomocą faksu.

Wytyczne BayLfD

Bawarski organ nadzorczy z zakresu danych osobowych stwierdza, że przesyłanie danych osobowych faksem wiąże się z różnymi zagrożeniami dla prywatności osób, których dane dotyczą. Organ w szczególności wskazuje na ryzyko naruszenia ochrony danych osobowych spowodowane błędną wysyłką faksu zarówno w przypadku wprowadzenia nieprawidłowego numeru połączenia, np. poprzez jego błędne wpisanie, jak i przez używanie nieaktualnego lub nieprawidłowo zapisanego numeru telefonu. BayLfD zwraca uwagę, że konieczność wybrania prefiksu lub kombinacji cyfr dla faksów wewnętrznych lub zewnętrznych również może spowodować nieprawidłowe doręczenie dokumentu, jeśli numer połączenia jest poprawny, ale błędnie wprowadzono – lub o nim zapomniano – prefiks niezbędny do wysyłania faksów wewnętrznych lub zewnętrznych (np. „0", które należy wybrać przed numerem zewnętrznym w przypadku centrali abonenckich). Ponadto może się zdarzyć, że adresat został wskazany, ale z organizacji administratora wysłano niewłaściwy list.

W celu przeciwdziałania takiemu ryzyku pracownicy powinni być zobowiązani przez administratora do zachowania szczególnej ostrożności przy wysyłaniu faksów, np. w instrukcji służbowej. Dodatkowo administrator powinien wprowadzić następujące środki techniczne i organizacyjne gwarantujące bezpieczeństwo przetwarzanych danych:

- dwukrotne sprawdzenie numeru faksu po jego wprowadzeniu, w miarę możliwości z zastosowaniem zasady czterech par oczu;
- w przypadku pierwszego kontaktu lub braku kontaktu od dłuższego czasu należy uzyskać potwierdzenie, że numer faksu jest (nadal) poprawny;
- zapisywanie często używanych numerów faksów w urządzeniu faksowym lub w oddzielnie przechowywanej książce adresowej.

Ponadto w ocenie organu na potrzeby realizacji zasady rozliczalności z art. 5 ust. 2 RODO w związku z korzystaniem faksu administratorzy powinni sporządzić m.in.:

- dokumentację dotyczącą lokalizacji faksów używanych w organizacji, w tym uwzględnić informacje o środkach zapobiegających nieuprawnionemu dostępowi;
- instrukcję dotyczącą korzystania z faksu jako środka komunikacji;
- odrębną, scentralizowaną dokumentację faksów wysyłanych w trybie pilnym, z powodów wysokiego ryzyka.
- analizę ryzyka związanego z wysyłaniem faksów o poufnej treści.

Wytyczne

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

Wytyczne EROD w sprawie prawa dostępu do danych

Bartłomiej Żeromski

11 marca 2022 r. zakończył się etap publicznych konsultacji wytycznych Europejskiej Rady Ochrony Danych (EROD) 01/2022 w sprawie prawa dostępu do danych. Wytyczne są obszernym dokumentem, dlatego pokrótce zostaną omówione wyłącznie niektóre kwestie w nich poruszone.

EROD postuluje, by prawo dostępu do danych zapewniało możliwość pozyskania informacji o przetwarzanych danych osobowych w sposób łatwy, przejrzysty oraz efektywny. Ma to umożliwić weryfikację zarówno legalności przetwarzania danych osobowych przez administratora, jak i ich prawidłowości, co ułatwi wykonywanie innych praw osoby, której dane dotyczą. Prawo dostępu do danych należy przy tym odróżnić od realizacji innych, podobnych praw. Przenosząc wytyczne w tym zakresie na grunt krajowy, jako przykład można wskazać prawo dostępu do dokumentacji medycznej i jej kopii. Co istotne, EROD zdaje się traktować prawo dostępu do danych jako prawo, z którego osoba niejako domyślnie korzysta, zwracając się o informacje o sobie, chyba że wskaże wprost, że składa żądanie na innej podstawie prawnej niż art. 15 RODO[1].

EROD w wytycznych zwraca uwagę również na to, że rolą administratora nie jest dokonywanie analizy, czy sposób realizacji prawa osoby, której dane dotyczą, pozwoli jej na weryfikację legalności przetwarzania danych albo na wykonanie następczo innych praw, które jej przysługują.

W wytycznych podkreślono, że administrator powinien zapewnić, by komunikacja z nim była łatwa i przyjazna dla egzekwującego swoje uprawnienie. Dopuszczalne jest tworzenie odpowiednich kanałów komunikacji w tym celu, jednak administrator nie może wymagać, by osoba, której dane dotyczą, kierowała do niego swoje żądania wyłącznie tym kanałem. Istotne jest jednocześnie potwierdzenie tożsamości osoby, która zgłasza żądanie wykonania prawa dostępu, tak by nie mieć wątpliwości, że jest ona osobą, za którą się podaje. Jeżeli administrator nie jest co do tego przekonany, powinien zwrócić się o podanie dodatkowych informacji, które umożliwią zidentyfikowanie osoby. Należy jednak pamiętać, że zakres żądanych informacji powinien być proporcjonalny do danych już przetwarzanych przez administratora. Potwierdzenie tożsamości nie powinno prowadzić do gromadzenia przez administratora nadmiarowych danych osobowych.

Według EROD prawo dostępu do danych dotyczy wszystkich danych osobowych wnioskodawcy, które są przetwarzane przez administratora – również tych poddanych pseudonimizacji – a pojęcie danych osobowych należy rozumieć szeroko. Jednym z elementów, który wzbudził kontrowersje w ramach publicznych konsultacji wytycznych, to wskazanie przez EROD, że zakresem prawa dostępu do danych mogą być objęte także dane osobowe innej osoby. Jako przykład podano przechowywaną przez usługodawcę historię komunikacji zawierającą wychodzące i przychodzące wiadomości.

Zgodnie z wytycznymi prawo dostępu do danych może być realizowane na wiele różnych sposobów, w zależności od ilości danych osobowych czy skomplikowania procesu przetwarzania. EROD informuje, że jeżeli w żądaniu nie wskazano inaczej, prawo dostępu do danych dotyczy wszystkich danych osobowych zgromadzonych w zasobach administratora. Administrator jest jednak uprawniony do zwrócenia się o sprecyzowanie żądania, jeżeli ilość przechowywanych przez niego danych dotyczących wnioskującego jest znaczna. Ponadto jeżeli dane osobowe przetwarzane przez administratora są w formie kodowej lub w postaci innego rodzaju „surowych danych", administrator ma obowiązek zapewnić wyjaśnienie przekazywanych informacji w taki sposób, by były zrozumiałe dla wnioskodawcy. Przejrzystość w komunikacji z osobą, której dane dotyczą, jest widocznie akcentowana w wytycznych. Jako jedno z rozwiązań w sytuacji, gdy administrator przetwarza dużą ilość danych, wskazano możliwość zastosowania podejścia warstwowego, które ułatwi osobie zrozumienie przekazywanych jej danych i informacji. Administrator musi być w stanie wykazać, że podejście warstwowe do wykonania prawa dostępu do danych stanowi wartość dodaną dla osoby. Niemniej osoba ta może domagać się zrezygnowania z podejścia warstwowego w stosunku do niej.

[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).

Kopia danych oraz informacje o danych osobowych powinny być przekazane na stałym nośniku, przez co rozumieć należy formę elektroniczną (m.in. hiperłącze), dzięki czemu osoba może pobrać informacje lub kopię danych. Europejska Rada Ochrony Danych wskazuje, że dopuszczalne jest również przekazanie kopii danych osobowych w formie transkrypcji lub zestawienia, jeżeli nie spowoduje to zmiany treści ani zawartości danych. Jednocześnie administrator nie powinien usuwać danych po uzyskaniu wniosku o dostęp do danych, a przed ich realizacją. W wytycznych podkreślono, że administrator powinien zapewnić obsługę żądania osoby w taki sposób, że nawet jeżeli przed upływem terminu na wykonanie prawa dostępu do danych upływa termin retencji danych, to w pierwszej kolejności należy zrealizować wniosek, a następnie usunąć dane osobowe. Dotyczy to także administratorów, którzy przetwarzają dane osobowe wyłącznie przez krótki czas.

W wytycznych odniesiono się też do wyjątków od wykonywania prawa dostępu do danych. Zgodnie z art. 15 ust. 4 RODO prawo do uzyskania kopii danych nie może niekorzystnie wpływać na prawa i wolności innych osób. EROD podnosi, że wyjątek ten należy jednak ujmować wąsko. Nie umożliwia on zupełnej odmowy realizacji prawa osoby, której dane dotyczą, ale może skutkować nieprzekazaniem części kopii przetwarzanych danych osobowych. Ponadto administrator jest uprawniony do niewykonania prawa dostępu do danych w przypadku, gdy żądanie byłoby nadmierne lub ewidentnie nieuzasadnione, albo do pobrania rozsądnej opłaty, uwzględniającej administracyjne koszty udzielenia informacji, prowadzenie komunikacji lub podjęcie żądanych działań (art. 12 ust. 5 RODO). W wytycznych opowiedziano się za wąskim rozumieniem tych wyjątków, jednak przy ich omawianiu EROD podniosła, że administrator nie może dowolnie wybrać, czy odmówi wykonania uprawnienia, czy też pobierze rozsądną opłatę w przypadku żądania o charakterze nadmiernym. EROD wymaga od administratora dokonania adekwatnej decyzji – w zależności od okoliczności sprawy – w zakresie wyboru pomiędzy tymi środkami. Jest to o tyle kontrowersyjne, że z RODO nie wynika tego rodzaju ograniczenie wyboru. Wątpliwe są również podstawy, na których organ krajowy mógłby zakwestionować wybór administratora w tym zakresie. Zgodnie z art. 12 ust. 5 RODO to administrator dokonuje wyboru, w jaki sposób powinien zareagować w przypadku, gdy żądanie jest ewidentnie nieuzasadnione lub nadmierne.

W ramach konsultacji publicznych ponad 70 podmiotów zgłosiło uwagi do przedstawionych wytycznych, z których część dotyczy mniej lub bardziej kontrowersyjnych propozycji EROD. Możliwe więc, że treść samych wytycznych ulegnie jeszcze zmianie. Pomimo że wytyczne EROD nie są prawem, to już teraz stanowią cenną wskazówkę co do stosowania RODO dla administratorów i osób, których dane dotyczą.

Wytyczne

Były pracownik nie jest zaufanym odbiorcą danych – wnioski z decyzji Prezesa UODO z dnia 19 stycznia 2022 r. w sprawie Santander Bank Polska SA

Patrycja Szurmak

22 lutego 2022 r. Prezes Urzędu Ochrony Danych Osobowych (dalej: „Prezes UODO") opublikował decyzję z dnia 19 stycznia 2022 r. nakładającą na Santander Bank Polska SA (dalej: „Santander" lub „Bank") administracyjną karę finansową w wysokości 545 000 zł za naruszenie **art. 34 ust. 1 RODO[1], tj. niezawiadomienie bez zbędnej zwłoki o naruszeniu ochrony danych osobowych osób, których dane dotyczą**.

Santander w ramach analizy naruszenia ochrony danych stwierdził, że nie wystąpiło wysokie ryzyko naruszenia praw lub wolności osób fizycznych, i nie dokonał zawiadomienia tych osób zgodnie z art. 34 RODO. Prezes UODO w czasie postępowania wyjaśniającego ocenił, że naruszenie wiązało się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, z tego też względu konieczne jest zawiadomienie osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych, zgodnie z obowiązkiem wyrażonym w art. 34 w związku z art. 12 RODO.

W decyzji Prezes UODO wskazuje, że fakt braku precyzyjnego określenia kręgu pracowników, których naruszenie dotyczy, nie stanowi przeszkody dla realizacji obowiązku **wynikającego z art. 34**, oraz analizuje, jak należy interpretować „**zaufanego odbiorcę danych**".

Okoliczności naruszenia

Santander zawiadomił UODO o naruszeniu ochrony danych osobowych w związku z dostępem do profilu płatnika na Platformie Usług Elektronicznych ZUS (PUE ZUS) byłego pracownika Banku. Były pracownik mógł przeglądać dane osobowe innych pracowników znajdujących się na profilu płatnika Banku. Santander, zgłaszając naruszenie ochrony danych osobowych w rozumieniu art. 33 RODO, poinformował o naruszeniu ochrony danych 10 500 osób. Były pracownik mógł przeglądać takie dane pracowników Banku, jak: imiona, nazwiska, numery PESEL, adresy zamieszkania lub pobytu oraz informacje o zwolnieniach lekarskich stanowiące dane dotyczące zdrowia. W toku postępowania ustalono, że pracownik po zakończeniu pracy korzystał z przysługujących mu uprawnień i pięciokrotnie logował się do platformy. Nie ustalono dokładnie, jakich osób dane przetwarzał były pracownik ani w jakim zakresie.

Santander w ramach analizy zdarzenia oraz szacowania ryzyka naruszenia praw lub wolności osób fizycznych uznał, że zaistniałe naruszenie ochrony danych osobowych, polegające na posiadaniu przez pracownika Banku po ustaniu stosunku pracy nieuprawnionego dostępu do danych pracowniczych przetwarzanych na Platformie Usług Elektronicznych ZUS w zakresie: imion i nazwisk, adresów zamieszkania lub pobytu, numerów PESEL, a ponadto informacji o zwolnieniach lekarskich, tj. danych dotyczących zdrowia, **powoduje niskie ryzyko naruszenia praw lub wolności osób fizycznych, skutkujące brakiem konieczności zawiadomienia osób, których dotyczy naruszenie**.

Santander przedstawił swoją analizę oceny naruszenia pod kątem naruszenia praw lub wolności osób fizycznych oraz wskazał argumenty, na podstawie których podjął taką decyzję. Bank podał m.in., że byłego pracownika, który miał dostęp do danych osobowych na platformie PUE ZUS, można uznać za odbiorcę „zaufanego". Bank zaufał odbiorcy z uwagi na złożone przez pracownika w trakcie zatrudnienia w Banku oświadczenia, „że ten nie podejmie żadnych dalszych działań w kwestii tych danych". Zdaniem Banku za okoliczność przemawiającą za prawidłowością dokonanej oceny ryzyka przemawia fakt, że była pracownica Banku samodzielnie zgłosiła administratorowi nieuprawniony dostęp do platformy PUE ZUS.

[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).

Ustalenia UODO

Prezes UODO po przeprowadzonym postępowaniu administracyjnym stwierdził, że w analizowanej sprawie doszło do naruszenia ochrony danych osobowych w rozumieniu art. 4 pkt 12 RODO. UODO również podtrzymał swoje stanowisko i uznał, że przedmiotowe naruszenie poufności danych zawartych na platformie PUE ZUS przez byłego pracownika Banku powoduje wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Prezes UODO w swoich ustaleniach odniósł się do kwestii, jak należy rozumieć zaufanego odbiorcę w ramach oceny ryzyka naruszenia praw lub wolności osób fizycznych.

Zaufany odbiorca danych – Grupa Robocza art. 29

Termin „zaufany odbiorca danych" pojawia się w kontekście oceny ryzyka naruszenia praw lub wolności osób fizycznych. Grupa Robocza art. 29 (obecnie Europejska Rada Ochrony Danych – EROD) w wytycznych dotyczących zgłaszania naruszeń ochrony danych zgodnie z RODO[2] wyjaśnia, jak można przeprowadzić „test", czy w danym przypadku mamy do czynienia z takim nieuprawnionym, ale „zaufanym odbiorcą". EROD podaje, że administrator może ufać odbiorcy na tyle, aby móc racjonalnie oczekiwać, że strona ta nie odczyta omyłkowo wysłanych danych lub nie uzyska do nich wglądu oraz że wypełni polecenie ich odesłania. Nawet jeżeli uzyskano wgląd do danych, administrator nadal może mieć zaufanie do odbiorcy, że nie podejmie on żadnych dalszych działań w kwestii tych danych oraz że niezwłocznie zwróci dane do administratora i będzie współpracować przy ich odzyskaniu.

Analiza, czy w danym przypadku dane zostały ujawnione zaufanemu odbiorcy, jest ważnym czynnikiem przy ocenie wagi konsekwencji naruszenia konkretnych danych osobowych.

EROD podkreśla, że zaufany odbiorca może spowodować, iż skutki naruszenia nie będą poważne, co z kolei może wyeliminować prawdopodobieństwo wystąpienia ryzyka dla osób fizycznych, w wyniku czego nie będzie już potrzeby powiadomienia organu nadzorczego lub osób fizycznych, na które to naruszenie wywiera wpływ[3].

EROD w wytycznych 1/2021 jako przykład zaufanego odbiorcy podaje agenta ubezpieczeniowego, który działając jako podmiot przetwarzający, otrzymał wiadomość e-mail z danymi nie swoich klientów i poinformował o tym niezwłocznie administratora oraz zobowiązał się do usunięcia błędnie przekazanej wiadomości.

Zaufany odbiorca danych – Prezes UODO

Prezes UODO w decyzji wskazuje, że kluczowym czynnikiem, na podstawie którego można uznać danego odbiorcę za zaufanego, **są stosunki, w jakich pozostają podmioty**.

Pojęcie zaufanego odbiorcy na gruncie decyzji w sprawie Santander

Prezes UODO w swojej decyzji precyzuje, że były pracownik nie może być postrzegany przez organizację jako zaufany odbiorca. Były pracownik, który nie jest już upoważniony do przetwarzania danych ze względu na rozwiązanie stosunku pracy, nie jest godny zaufania. Zdaniem Prezesa UODO, aby można mówić o zaufanym odbiorcy, między podmiotami musi istnieć pewna więź prawna lub faktyczna, która pozwala na ocenę stopnia zaufania stron. Według Prezesa UODO między Bankiem a byłym pracownikiem nie występuje więź ani prawna, ani biznesowa. Prezes UODO wskazuje, że nie można ponad wszelką wątpliwość uznać, iż były pracownik zachowa się w odpowiedni sposób.

Pojęcie zaufanego odbiorcy na gruncie innych decyzji Prezesa UODO

Czy komentowana decyzja w zakresie wykładni zaufanego odbiorcy jest przełomowa? Nie, ale warto zapoznać się z argumentacją Prezesa UODO dotyczącą tego, jak polski organ nadzorczy rozumie pojęcie zaufanego odbiorcy. Przykładowo można wskazać, że w decyzji DKN.5131.5.2020 Prezes UODO za zaufanego odbiorcę danych uznał kontrahenta, z którym współpracuje administrator, a w decyzji DKN.5131.5.2020 jako zaufanego odbiorcę podał niewłaściwy dział organizacji (podobnie jak EROD w swoich wytycznych).

Polski organ nadzorczy w decyzji DKN.5130.3114.2020 wskazał, że domownik nie jest „z automatu" zaufanym odbiorcą danych. Aby mieć pewność, że dany domownik jest zaufanym odbiorcą, należy każdorazowo badać relację łączącą takiego nieuprawnionego odbiorcę z docelowym odbiorcą.

Wnioski z decyzji w sprawie Santander

Na kanwie decyzji w sprawie Santander można odnotować dwa ważne wnioski:

- były pracownik nie jest zaufanym odbiorcą danych;
- brak precyzyjnego określenia osób, których naruszenie dotyczy, nie stanowi przeszkody dla realizacji obowiązku **wynikającego z art. 34. W przypadku gdy administrator nie wie, czyje dane zostały naruszone, należy przyjąć szeroki katalog i poinformować wszystkich potencjalnych „poszkodowanych"**.

Pełna treść

[2] Zob. https://www.uodo.gov.pl/pl/10/12 (dostęp: 15.03.2022).
[3] Również w tym wypadku wszystko będzie zależało od konkretnej sytuacji i każdy przypadek należy rozważać indywidualnie.

Nowe wytyczne DSK ws. marketingu bezpośredniego i przepisów o ochronie danych osobowych

Mateusz Kupiec

Marketing bezpośredni to zbiorowe określenie działań skierowanych bezpośrednio do odbiorcy, mających na celu nakłonienie go do nabycia towarów lub usług oferowanych przez reklamodawcę. Przykładem takich działań może być wysyłanie drogą elektroniczną lub tradycyjną pocztą komunikatów o promocjach, wyświetlanie reklam behawioralnych konkretnej osobie na podstawie jej profilu. Marketing bezpośredni związany jest z przetwarzaniem danych osobowych, a w szczególności danych kontaktowych osób fizycznych.

Znaczna część administratorów ma problemy z prawidłowym spełnieniem wymogów wynikających z RODO[1] w związku z prowadzeniem działań marketingowych wobec podmiotów danych. Świadczą o tym wysokie kary nakładane przez organy krajowe w poszczególnych państwach członkowskich UE za naruszenia przepisów rozporządzenia przez administratorów w trakcie prowadzonych przez nich kampanii marketingowych[2].

Wytyczne Datenschutzkonferenz

18 lutego 2022 r. Konferencja Niezależnych Organów Ochrony Danych Federacji i Krajów Związkowych (zgromadzenie wszystkich organów nadzorczych z zakresu ochrony danych osobowych w Niemczech, dalej: „Datenschutzkonferenz" lub „DSK") opublikowała aktualizację swoich wytycznych z 2018 r. ws. marketingu bezpośredniego i przepisów o ochronie danych osobowych. Dokument ten zawiera wiele istotnych wskazówek dla administratorów danych, którzy prowadzą działania marketingowe na podstawie przetwarzania danych osobowych:

- Reklamodawcy muszą być w stanie udowodnić, że adres e-mail wykorzystywany do celów reklamowych jest aktualnym adresem istniejącego klienta.
- Ustalając okres przechowywania danych po ustaniu relacji biznesowej z podmiotem danych, należy wziąć pod uwagę upływ czasu od ostatniego aktywnego kontaktu i charakter relacji biznesowej. Ponowne wykorzystywanie danych osobowych w celu wysyłania osobie fizycznej treści marketingowych po długiej przerwie reklamowej może być uzasadnione m.in. w przypadku długoletniej bazy klientów.
- W przypadku gdy to podmiot danych wysyła pierwszą wiadomość elektroniczną, przeznaczona dla niego klauzula informacyjna powinna być umieszczona pod linkiem przesłanym w automatycznym potwierdzeniu otrzymania wiadomości. Taki link ma pozwolić podmiotowi danych na łatwe uzyskanie dostępu do informacji z art. 13 RODO.
- W sytuacji tworzenia profilu osoby fizycznej w celach marketingowych co do zasady nadrzędne będą prawa i wolności podmiotu danych w stosunku do prawnie uzasadnionego interesu administratora, co wyklucza przesłankę prawnie uzasadnionego interesu jako podstawy prawnej takiego przetwarzania danych.
- Gdy rozpoczęto już konkretne działania marketingowe w postaci analogowej (np. wysyłka newslettera pocztą tradycyjną), a dane kontaktowe podmiotu danych są już przetwarzane technicznie, realizacja przez administratora otrzymanego w międzyczasie sprzeciwu z art. 21 może okazać się właściwie niemożliwa. W takich przypadkach reklamodawcy powinni w indywidualnej odpowiedzi na zgłoszony sprzeciw poinformować podmiot danych, że jego wniosek został uwzględniony, ale przez krótki, dokładnie wskazany okres może otrzymywać on jeszcze wiadomości reklamowe.
- Podmiot danych może odwołać udzieloną zgodę w dowolnej formie. Administrator danych musi jednak być w stanie określić, czy osoba wycofująca zgodę jest tą samą osobą, która w pierwszej kolejności zgodziła się na przetwarzanie danych. Przykładowo w przypadku oświadczenia o odwołaniu zgody złożonego za pośrednictwem internetowego formularza kontaktowego może być wymagane potwierdzenie „wycofania zgody" przez osobę fizyczną, np. poprzez kliknięcie linku otrzymanego na adres e-mail znajdujący się w bazie administratora. W przypadku oświadczenia złożonego za pomocą wiadomości e-mail wysłanej z adresu poczty elektronicznej służącego podmiotowi danych do stałych kontaktów z administratorem taka dodatkowa weryfikacja tożsamości wycofującego zgodę nie jest wymagana.

Wytyczne

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

[2] Na przykład administracyjna kara pieniężna w wysokości 8500 euro nałożona przez fiński organ nadzorczy w lutym 2021 r. na wydawcę magazynu, który kontaktował się za pomocą tzw. robocalss z podmiotami danych bez ich zgody, https://edpb.europa.eu/news/national-news/2021/finnish-sa-fine-company-carrying-out-direct-marketing-robocalls-without_en (dostęp: 8.03.2022). W 2020 r. belgijski organ nadzorczy ukarał administratora danych administracyjną karą pieniężną w wysokości 10 000 euro w związku z wysłaniem wiadomości marketingowej do niezamierzonego adresata, https://edpb.europa.eu/news/national-news/2020/belgian-dpa-fines-controller-sending-direct-marketing-message-wrong-person_sk (dostęp 8.03.2022).

Dark patterns w świetle Wytycznych EROD nr 03/2022 ws. dark patterns w interfejsach platform mediów społecznościowych

Mateusz Kupiec

Dark patterns to sposób projektowania interfejsów użytkownika na stronach internetowych czy platformach w taki sposób, aby korzystające z nich osoby podejmowały działania, których inaczej by nie podjęły. Często podawanym przykładem takich praktyk jest wyróżnienie graficzne opcji, którą właściciel interfejsu chciałby, aby użytkownik wybrał. Stosowanie *dark patterns* wzbudza kontrowersje, ponieważ w ten sposób ograniczana jest autonomia osób korzystających z usług społeczeństwa informacyjnego.

W odniesieniu do prawa ochrony danych osobowych podnosi się, że stosowanie *dark patterns* przez administratorów może naruszać zasadę przejrzystości przetwarzania (art. 5 ust. 1 lit. a RODO[1]) oraz negatywnie wpływać na ocenę dobrowolności zgody podmiotu danych wyrażonej za pomocą interfejsu opartego na *dark patterns*. W ostatnim czasie zagadnienie *dark patterns* w kontekście przepisów RODO wzbudziło ogromne zainteresowanie ze względu na wysyłanie przez organizację NOYB administratorom, których cookie banery uznano za manipulujące zachowaniem użytkowników, zautomatyzowanych projektów skarg do organów nadzorczych w związku z naruszeniem przepisów rozporządzenia.

Dostrzegając zagrożenia, jakie niesie za sobą stosowanie *dark patterns*, Europejska Rada Ochrony Danych (EROD) opublikowała Wytyczne 03/2022 ws. *dark patterns* w interfejsach platform mediów społecznościowych (dalej: „Wytyczne"). W dokumencie tym EROD zawarła praktyczne zalecenia dla projektantów i użytkowników platform mediów społecznościowych w zakresie tego, jak oceniać i unikać *dark patterns*.

W dalszej części tekstu przedstawię wybrane ustalenia EROD poczynione w Wytycznych.

Wybrane zalecenia EROD:

- EROD podaje wiele przykładów stosowania szerokiego wachlarza technik manipulacyjnych przez dostawców platform. Wskazuje jednak, ze stosowanie *dark patterns* nie oznacza tylko naruszenia przepisów o ochronie danych, lecz także naruszenie przepisów dotyczących praw konsumentów.
- Dostawcy mediów społecznościowych muszą przestrzegać zasad określonych w art. 5 RODO. Zasada przejrzystości przetwarzania ma szczególnie doniosłe znaczenie na etapie zakładania konta na platformie mediów społecznościowych. W zależności od swojej roli w obrocie danymi osobowymi administratorzy platform mediów społecznościowych powinni przekazywać użytkownikom informacje podczas rejestracji w sposób skuteczny i zwięzły, a także wyraźnie odróżniać je od innych informacji, niezwiązanych z ochroną danych.
- EROD wskazuje, że interfejs użytkownika i jego sposób poruszania się po tym interfejsie można wykorzystać jako narzędzie dokumentacji realizacji przepisów RODO. Ponadto w ocenie organu jakościowe i ilościowe badania z udziałem użytkowników sieci mogą być wykorzystywane również do wspierania wykazywania spełnienia zasady rozliczalności.
- Zdaniem EROD, gdy użytkownicy platform społecznościowych są nakłaniani przez ich twórców do szybkiego podawania swoich danych, np. podczas rejestracji, zostają pozbawieni możliwości podjęcia świadomej decyzji o przekazaniu informacji o sobie samych. Język stosowany przez platformy mediów społecznościowych może zachęcać użytkowników do podawania większej ilości danych, niż jest to wymagane.
- EROD zaleca, aby w przypadku, gdy usługi społeczeństwa informacyjnego są oferowane i skierowane do mieszkańców różnych państw członkowskich, informacje o ochronie danych były dostępne w zrozumiałych dla nich językach. Ważne jest, aby użytkownicy mieli możliwość samodzielnego wyboru języka, w którym chcą otrzymać informacje o przetwarzaniu ich danych.

[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).

Dark patterns a gwarancje autonomii informacyjnej dzieci

W opublikowanych Wytycznych EROD poświęca sporo uwagi również zagadnieniu ochrony dzieci przed działaniem technik manipulacyjnych na platformach społecznościowych. EROD przekazuje w szczególności następujące spostrzeżenia:

- Należy mieć na uwadze, że *dark patterns* budzą wątpliwości dotyczące potencjalnego wpływu na dzieci, których dane przetwarzają dostawcy mediów społecznościowych. Najmłodsi mogą być bowiem mniej świadomi ryzyka i konsekwencji związanych z przetwarzaniem ich danych przez takie podmioty.
- Biorąc pod uwagę podatność dzieci na manipulację, *dark patterns* mogą nakłaniać najmłodszych do dzielenia się większą ilością informacji, ponieważ „imperatywne" wyrażenia mogą sprawić, że poczują się „zobowiązane" do dzielenia się informacjami na swój temat, aby np. „zyskać popularność wśród rówieśników".
- *Dark patterns* nierzadko sprowadzają się do tzw. sterowania emocjonalnego, polegającego na używaniu przez platformę sformułowań lub obrazów w sposób, który przekazuje użytkownikom informacje w bardzo pozytywnym świetle, sprawiając, że czują się oni dobrze lub bezpiecznie, albo w bardzo negatywnym, wywołując u nich strach lub poczucie winy.
- Działanie polegające na sterowaniu emocjami dzieci na etapie rejestracji na platformie może mieć na nie bardzo duży wpływ i nakłonić najmłodszych do podawania większej ilości danych osobowych.
- Gdy usługi platformy mediów społecznościowych są skierowane do dzieci, administratorzy powinni zagwarantować, że używany język, w tym jego ton i styl, jest odpowiedni, tak aby dzieci, jako odbiorcy wiadomości, łatwo zrozumiały przekazywane informacje.

Wytyczne EROD nr 03/2022 ws. *dark patterns* w interfejsach platform mediów społecznościowych znajdują się obecnie na etapie konsultacji. Opinie na temat Wytycznych można przesyłać do EROD do 2 maja 2022 r.

Wytyczne

Wytyczne Datatilsynet dotyczące przetwarzania danych osobowych w chmurze

Mateusz Kupiec

Chmura obliczeniowa to nazwa zbiorcza rozwiązań pozwalających korzystającym z nich podmiotom na dostęp za pośrednictwem sieci do wspólnej puli możliwych do konfiguracji zasobów przetwarzania (np. sieci, serwerów, aplikacji i usług) [1]. W chmurze organizacje przechowują wiele informacji, w tym dane osobowe. Najwięksi dostawcy usług chmurowych przetwarzają powierzone im informacje w centrach danych znajdujących się poza Europejskim Obszarem Gospodarczym, najczęściej w USA. Po wyroku w sprawie Schrems II i opublikowaniu przez EROD zaleceń 01/2020 dotyczących środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych zagadnienie transferu danych do państw trzecich stało się szczególnie skomplikowane.

Duński organ nadzorczy z zakresu ochrony danych osobowych (Datatilsynet), dostrzegając problemy, z jakimi muszą się zmierzyć podmioty korzystające z różnego rodzaju usług chmurowych, postanowił opublikować wytyczne dotyczące przetwarzania danych w chmurze.

Wytyczne Datatilsynet

W wytycznych Datatilsynet wiele miejsca poświęcono na analizę zagadnienia transferu danych do państw trzecich (w szczególności do USA) w związku z korzystaniem przez administratorów z narzędzi oferowanych przez dostawców usług chmurowych. Jednakże zakres przedmiotowy wytycznych jest znacznie szerszy, ponieważ organ omawia w nich typologię usług chmurowych, a także zagadnienie audytu dostawcy usług chmurowych oraz jego podwykonawców.

Ogólne zalecenie Datatilsynet, jakie wynika z wytycznych organu, sprowadza się do konieczności zapoznania się przez administratora z modelem działania konkretnego dostawcy usług chmurowych oraz dokonania analizy sytuacji prawnej w państwie trzecim, w którym się on znajduje.

Transfery danych w związku z przechowywaniem danych w chmurze

Omawiając zagadnienie transferów danych do państw trzecich, Datatilsynet przedstawia m.in. następujące wnioski:

- Administratorzy przed rozpoczęciem transferu powinni się upewnić, że dostawca usług chmurowych spoza EOG, z którego rozwiązań korzystają, może ich poinformować o wcześniej otrzymanych wnioskach służb o dostęp do powierzonych mu danych.
- Administrator musi wykazać, że kategorie danych osobowych, które zamierza powierzyć dostawcy usług chmurowych spoza EOG, nie były wcześniej objęte żadnymi wnioskami otrzymanymi przez konkretnego dostawcę.
- W przypadku prawa amerykańskiego nie jest wykluczone, że istnieją dane osobowe, które są wyłączone z zakresu przedmiotowego „informacji obcego wywiadu" (*foreign intelligence information*), o których mowa w sekcji 702 ustawy o nadzorze wywiadu zagranicznego (Foreign Intelligence Surveillance Act, dalej: „FISA"). Jednakże to administrator musi wykazać, że przekazywane przez niego dane nie podlegają pod FISA. Same oświadczenia dostawcy są niewystarczające do prawidłowego spełnienia tego obowiązku.
- Należy dokonać wyczerpującej oceny przepisów obowiązujących w państwach trzecich, w których znajdują się dostawcy usług chmurowych i ich (potencjalni) podwykonawcy. Administratorzy, dokonując takiej oceny, przed podjęciem decyzji o transferze danych powinni zatem przyjąć „najgorszy możliwy scenariusz" jako podstawę swojej analizy, tj. uznać, że wszystkie kraje trzecie, do których mają być przekazywane dane osobowe, mają „problematyczne" ustawodawstwo. Dopiero wtedy powinni zbadać, jakie dodatkowe środki techniczne muszą zostać wdrożone, aby zapewnić poziom ochrony danych zasadniczo równoważny z gwarancjami unijnymi.

[1] P. Mell, T. Grance, *The NIST Definition of Cloud Computing, NIST Special Publication 800-145*, 2011, s. 2, https://csrc.nist.gov/publications/detail/sp/800-145/final (dostęp 10.03.2022).

- Środki umowne i organizacyjne na ogół nie przeszkodzą amerykańskim służbom w uzyskaniu dostępu do danych osobowych będących przedmiotem transferu. Konieczne będzie zatem wdrożenie dodatkowych środków technicznych.
- Szyfrowanie nie będzie skutecznym środkiem technicznym, który zagwarantuje bezpieczeństwo danych będących przedmiotem transferu, jeżeli dostawca chmurowy będzie w posiadaniu kluczy szyfrujących.
- Sekcja 702 FISA upoważnia amerykańskie służby do uzyskiwania informacji o „osobach niebędących obywatelami USA", co do których można w sposób uzasadniony oczekiwać, że znajdują się poza USA w celu zbierania „informacji obcego wywiadu". Odbywa się to poprzez wydawanie poleceń dostawcom usług łączności elektronicznej, aby dostarczyli lub zorganizowali dostarczenie służbom danych osobowych przetwarzanych przez dostawcę.

Audyt dostawcy usług chmurowych oraz jego podwykonawców

Zdaniem Datatilynet administrator korzystający z usług chmurowych powinien:

- dokładnie zbadać przed powierzeniem dostawcy danych osobowych do przetwarzania, czy taki podmiot zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą;
- móc wskazać, którzy z podwykonawców dostawcy usług chmurowych biorą udział w przetwarzaniu – jeżeli ADO nie jest w stanie tego zrobić, powinien założyć, że wszyscy podwykonawcy dostawcy odgrywają rolę w przetwarzaniu powierzonych danych w ramach usługi;
- dokonywać większej liczby audytów lub inspekcji u dostawcy usług chmurowych, któremu powierzył przetwarzanie danych, jeżeli dostawca często zmienia podwykonawców.

Wytyczne

Opracowanie ENISA dotyczące inżynierii ochrony danych – teorii i praktyki we wdrażaniu środków ochrony i domyślnej prywatności w fazie projektowania procesów przetwarzania

dr inż. Andrzej Kaczmarek, CISA

Wraz z rozwojem technologii pojawiły się nowe techniki udostępniania, przetwarzania i przechowywania danych. Doprowadziło to do powstania nowych modeli przetwarzania danych (w tym danych osobowych), ale również wprowadziło nowe zagrożenia i wyzwania. Niektóre z nich to: brak kontroli i przejrzystości, możliwość ponownego, nieuprawnionego wykorzystania danych, wnioskowanie na podstawie danych i ponowna identyfikacja, a także profilowanie i zautomatyzowane podejmowanie decyzji. Z uwagi na wspomniane zagrożenia operacje przetwarzania muszą być dobrze przemyślane – z uwzględnieniem ważnej roli technologii jako elementu gwarancji bezpieczeństwa oraz środków technicznych i organizacyjnych, które muszą być odpowiednio wdrożone i skonfigurowane. Od strony technicznej wyzwanie polega głównie na przełożeniu określonych w RODO[1] zasad na konkretne wymagania i specyfikacje poprzez wybór, wdrożenie i skonfigurowanie odpowiednich środków technicznych i organizacyjnych, a także sposobu przetwarzania.

Takie podejście, nazywane inżynierią ochrony danych, może być postrzegane jako część ochrony danych już w fazie projektowania oraz jako domyślna ochrona danych. Ma na celu wspieranie wyboru, wdrażania i konfiguracji odpowiednich środków technicznych i organizacyjnych w celu spełnienia określonych zasad ochrony danych.

W omawianym opracowaniu ENISA, zatytułowanym „Inżynieria ochrony danych. Od teorii do praktyki"[2] i opublikowanym w lutym 2022 r., przyjrzano się szerzej inżynierii ochrony danych, aby wesprzeć praktyków i organizacje w praktycznym wdrażaniu technicznych aspektów ochrony danych w fazie projektowania i fazie domyślnej. Omówiono w nim m.in. anonimizację i pseudonimizację, maskowanie danych, bezpieczne przesyłanie i przechowywanie danych oraz przejrzystość i mechanizmy kontroli użytkownika nad danymi. Opracowanie powstało w kontekście zadań ENISA wynikających z rozporządzenia o bezpieczeństwie cybernetycznym (CSA)[3], polegających na wspieraniu państw członkowskich w konkretnych aspektach bezpieczeństwa cybernetycznego związanych z polityką i prawem UE w zakresie ochrony danych i prywatności. Prace te mają na celu zapewnienie podstaw do dalszej i bardziej szczegółowej analizy zidentyfikowanych kategorii technologii i technik przy jednoczesnym wykazaniu możliwości ich praktycznego zastosowania.

2. Inżynieria ochrony danych

Inżynieria prywatności jest dyscypliną wyłaniającą się z dziedziny projektowania systemów informatycznych, której celem jest zapewnienie narzędzi i technik umożliwiających stworzenie systemów zapewniających akceptowalny poziom prywatności oraz zgodność z wymaganiami funkcjonalnymi i niefunkcjonalnymi określonymi w polityce prywatności. Istnieją różne podejścia do zapewnienia prywatności w całym cyklu przetwarzania. ENISA np. w raporcie z 2015 r. dotyczącym koncepcji uwzględniania „Prywatności i ochrony danych w fazie projektowania"[4] przedstawiła osiem strategii uwzględnienia prywatności w fazie projektowania, zorientowanych zarówno na dane, jak i na proces przetwarzania. W innym podejściu[5] zaproponowano ramy składające się z sześciu celów. Do podstawowej trójki: „poufności", „integralności"

[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] European Union Agency for Cybersecurity (ENISA), Data Protection Engineering. From Theory to Practice, 2022, https://www.enisa.europa.eu/publications/data-protection-engineering (dostęp: 16.03.2022).
[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), http://data.europa.eu/eli/reg/2019/881/oj (dostęp: 23.03.2022).
[4]ENISA, *Privacy and Data Protection by Desig*n, 2015, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (dostęp: 16.03.2022).
[5] M. Hansen, M. Jensen, M. Rost, *Protection Goals for Privacy Engineering*, 2015 IEEE Security and Privacy Workshops, 2015.

i „dostępności" dodano trzy cele dodatkowe: „brak powiązań", „przejrzystość" oraz „możliwość interwencji". Do rozwiązań z zakresu inżynierii ochrony danych należy zaliczyć również technologie ochrony prywatności znane pod nazwą PET (*privacy enhancing technologies*), będące „spójnym zestawem środków, który chroni prywatność poprzez eliminację lub ograniczenie danych osobowych lub poprzez zapobieganie niepotrzebnemu i/lub niepożądanemu przetwarzaniu danych osobowych, a wszystko to bez utraty funkcjonalności systemu informatycznego". Strategie i cele ochrony danych osiągane w ramach inżynierii ochrony danych kładą nacisk na wbudowanie rozwiązań mających na celu spełnienie wymogów ochrony danych w operacjach przetwarzania. Środki te mają służyć ochronie przetwarzanych danych, których zastosowanie należy wykazać w szczególności podczas oceny skutków dla ochrony danych (art. 35 ust. 7 lit. d RODO).

3. Anonimizacja i pseudonimizacja

Anonimizacja, czyli proces polegający na usunięciu wszystkich informacji, które w jakikolwiek sposób umożliwiają identyfikację określonej osoby, której dane dotyczą, wymaga optymalizacji dwóch sprzecznych parametrów: użyteczności danych i ochrony przed ponowną identyfikacją. Znalezienie właściwego kompromisu w tym obszarze zależne jest od zastosowania i kontekstu, tj. zawartości i sposobu, w jaki dane są przedstawione, oraz celu, w jakim mają służyć. Zagadnienia te dość szeroko zostały omówione w opinii 05/2014 Grupy Roboczej Art. 29[6].

4. Maskowanie danych

Maskowanie to szeroki termin odnoszący się do funkcji, które po zastosowaniu do danych ukrywają ich prawdziwą wartość. Najbardziej znanymi przykładami są szyfrowanie i haszowanie. Zalicza się do nich także takie technologie, jak: szyfrowanie homomorficzne, koncepcje bezpiecznych obliczeń wielostronnych, zaufane środowisko wykonawcze, wyszukiwanie informacji prywatnych czy koncepcje danych syntetycznych. Główną użytecznością maskowania w odniesieniu do zasad ochrony danych jest integralność i poufność (bezpieczeństwo), a w zależności od techniki lub kontekstu przetwarzania może również obejmować rozliczalność i ograniczenie celu.

5. Dostęp do danych, przekazywanie i przechowywanie

Z punktu widzenia inżynierii ochrony danych kanały komunikacyjne powinny wykraczać poza bezpieczeństwo jako ich podstawową funkcjonalność. Powinny one zawierać dodatkowe cechy zwiększające prywatność, takie jak kontrola dostępu np. w zakresie tego, kto może mieć dostęp do treści komunikatu (w tym dostawcy, lokalizacja i dostęp do kluczy szyfrujących, lokalizacja i typ dostawcy, ujawnione informacje o użytkowniku itp.).

6. Przejrzystość, możliwość interwencji i kontrola użytkownika

Mając na uwadze potrzebę zapewnienia osobom, których dane są przetwarzane, ich praw przez administratora danych, kluczowym elementem każdej koncepcji ochrony danych jest umożliwienie osobom samodzielnego korzystania z praw do ochrony danych. Obejmuje to zarówno dostęp osoby do danych przetwarzanych na jej temat, celu i sposobu przetwarzania (przejrzystość), jak i możliwość wpływania na przetwarzanie jej danych osobowych przez administratora lub podmiot przetwarzający (możliwość interwencji). W związku z tym w środowisku badaczy prywatności pojawiło się wiele rozwiązań inżynierskich, które mogą pomóc we wdrożeniu tych praw i skorelowanych z nimi usług u administratora lub podmiotu przetwarzającego.

Pełna treść

PUBLIKACJE

„Ochrona danych osobowych w sektorze łączności elektronicznej”– rozdział autorstwa adw. Xawerego Konarskiego, który ukazał się w publikacji „Meritum. Ochrona Danych Osobowych”, pod red. naukową D.Lubasza.

„Ponowne wykorzystywanie – nowe otwarcie” – artykuł autorstwa adw. dr. hab. prof. INP PAN Grzegorza Sibiga, który ukazał się w nr 1/2022 miesięcznika „IT w administracji”

Czytaj więcej

„Interpretacje krajowych sądów” - artykuł autorstwa Mateusza Kupca, który ukazał się w nr 1/2022 ABI Expert

„Drony a realizacja zasad przetwarzania danych” - artykuł autorstwa Mateusza Kupca, który ukazał się w nr 1/2022 ABI Expert

WYDARZENIA

Webinarium - 6.04.2022 r.

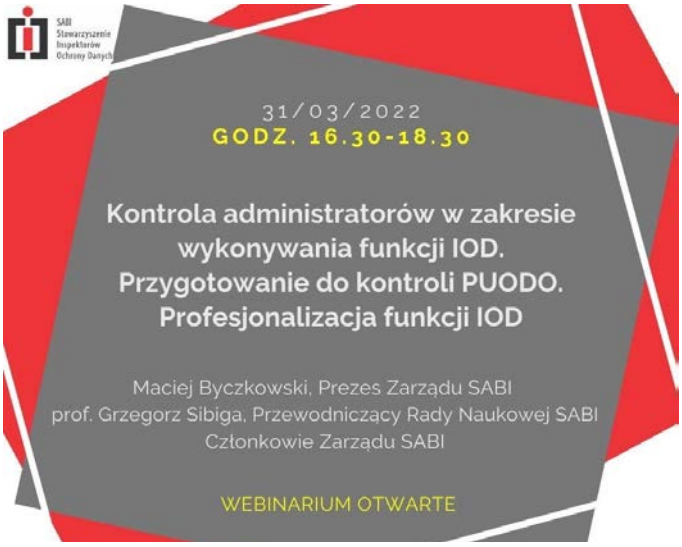
Wystąpienie adw. Xawery Konarskiego oraz r.pr. Dominiki Nowak podczas webinarium pt. „Odpowiedzialność administratora za procesora i obowiązki procesora”.

Konferencja - 31.03.2022 r.

Wystąpienia adw. dr hab. prof. INP PAN Grzegorza Sibiga podczas webinarium pt. „Kontrola ADO w zakresie wykonywania funkcji IOD. Przygotowanie do kontroli PUODO. Profesjonalizacja funkcji IOD” organizowanego przez SABI – Stowarzyszenia Inspektorów Ochrony Danych.

Kongres - 25.03.2022 r.

Wystąpienie adw. dr hab. prof. INP PAN Grzegorza Sibiga pt. „Obiektywne i subiektywne rozumienie pojęcia „danych osobowych”. Różnice w podejściu sądów i organów nadzorczych oraz ich konsekwencje” podczas VIII Polskiego Kongresu Ochrony Danych Osobowych organizowanego przez Wydawnictwo Must Read Media



Kongres - 4.03.2022 r.

Wystąpienie adw. dr hab. prof. INP PAN Grzegorza Sibiga pt. „DGA. Nowe zasady dostępności i wykorzystywania danych w obrocie cyfrowym w Unii Europejskiej" podczas II Kongresu Prawa Nowych Technologii organizowanego przez Wydawnictwo Must Read Media.

Szkolenie - 14.03.2022 r.

Szkolenie online z ochrony danych osobowych przeprowadzone przez Mateusza Kupca dla wolontariuszy pomagającym uchodźcom z Ukrainy na zaproszenie Rady Samorządu Studentów CM UJ

Szkolenie on-line - 26.02.2022 r.

„Czy dzieci mają prawo do prywatności w dobie cyfryzacji? Zagadnienia wybrane" poprowadzone przez Mateusza Kupca dla Sekcji Praw Dziecka przy Okręgowej Radzie Adwokackiej w Warszawie.

PODCASTY

Kancelaria Traple Konarski Podrecki i Wspólnicy uruchamia projekt podcastowy - TKP on air. Prawo. Biznes. Technologia.

W podcastach nie zabraknie tematów związanych z prawem własności intelektualnej, nowych technologii, szeroko rozumianym prawem gospodarczym oraz prawnymi aspektami funkcjonowania internetu.

Już teraz zapraszamy do wysłuchania pierwszego odcinka **„Czy NFT zrewolucjonizuje prawo własności intelektualnej?"** z udziałem mec. Anny Sokołowskiej – Ławniczak, mec. Michała Sobolewskiego i Patrycji Gierdal.

Zapraszamy do wysłuchania podcastu na naszej stronie internetowej lub na platformach:

- Spotify
- SoundCloud
- YouTube

ZESPÓŁ RODO

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

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

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

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

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

Patrycja Szurmak
Radczyni prawna, Associate
patrycja.szurmak@traple.pl

Bartłomiej Żeromski
Associate
bartlomiej.zeromski@traple.pl

Mateusz Kupiec
Junior Associate
mateusz.kupiec@traple.pl

Redaktor newslettera:
Mateusz Kupiec

Pytania prosimy kierować na adres:
rodo@traple.pl