Urząd Ochrony Danych Osobowych

NEWSLETTER
UODO DLA INSPEKTORÓW OCHRONY DANYCH

Obserwuj nas także na:

Numer 5/2019 (5)
Sierpień 2019

Trwają konsultacje Wytycznych EROD w sprawie monitoringu wizyjnego. Zachęcamy do wzięcia w nich udziału!

Podczas lipcowego posiedzenia plenarnego Europejskiej Rady Ochrony Danych (EROD) przyjęła m.in. wytyczne w sprawie monitoringu wizyjnego (Wytyczne 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo) mające na celu zapewnienie spójnego stosowania RODO w tym zakresie. Wytyczne wyjaśniają kwestie zastosowania RODO do korzystania zarówno z tradycyjnych, jak i inteligentnych urządzeń wideo. W przypadku tych ostatnich wytyczne koncentrują się na zasadach dotyczących przetwarzania szczególnych kategorii danych. Znajdziemy w nich ponadto podpowiedzi co do przesłanek legalności przetwarzania danych za pomocą takich urządzeń, zastosowania wyłączenia przepisów w związku z czysto osobistym lub domowym charakterem czynności oraz udostępniania materiału filmowego osobom trzecim.

Obecnie trwają publiczne konsultacje tego dokumentu. Uwagi należy kierować najpóźniej do 9 września 2019 r. na adres: EDPB@edpb.europa.eu.

czytaj więcej na stronie EROD

Zaktualizowany wykaz rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony

W Monitorze Polskim został ogłoszony Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony. Podstawą ogłoszenia komunikatu jest art. 54 ust. 1 pkt 1 ustawy o ochronie danych osobowych w związku z art. 35 ust. 4 i 6 RODO. Wykaz został zaktualizowany po uwzględnieniu opinii wydanej przez Europejską Radę Ochrony Danych i obejmuje dodatkowo czynności przetwarzania związane z oferowaniem towarów lub usług osobom, których dane dotyczą, lub z monitorowaniem ich zachowania w kilku państwach członkowskich lub mogące znacznie wpłynąć na swobodny przepływ danych osobowych w Unii Europejskiej. Wykaz zawiera 12 kategorii rodzajów operacji przetwarzania wraz z przykładami operacji, w których może wystąpić wysokie ryzyko naruszenia praw lub wolności oraz przykładami potencjalnych obszarów obejmujących te operacje.

Zawarte w wykazie przykładowe rodzaje operacji przetwarzania, które w opinii Urzędu Ochrony Danych Osobowych wymagają oceny skutków dla ochrony danych, mają pomóc administratorom w lepszym zrozumieniu kryteriów/rodzajów operacji mogących skutkować koniecznością przeprowadzenia oceny skutków dla ochrony danych.

Wykaz stanowi załącznik do Komunikatu Prezesa Urzędu Ochrony Danych Osobowych.

komunikat Prezesa UODO

Tematy numeru

Szkolenia UODO dla inspektorów ochrony danych

Transmisje z wydarzeń organizowanych przez UODO

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
kancelaria@uodo.gov.pl
godziny pracy urzędu 8:00-16:00

European Data Protection Board

DOKUMENTY PRZYJĘTE PRZEZ EROD NA LIPCOWYM POSIEDZENIU PLENARNYM

Podczas swojego 12. posiedzenia plenarnego Europejska Rada Ochrony Danych przyjęła m.in. opinie w sprawie: duńskich standardowych klauzul umownych dla podmiotów przetwarzających, kryteriów akredytowania podmiotów monitorujących kodeksy postępowania czy ciągłości kompetencji organów nadzorczych. Na posiedzeniu omówiono ponadto m.in. skutki amerykańskiej ustawy US CLOUD Act.

PRZYJĘTE OPINIE EUROPEJSKIEJ RADY OCHRONY DANYCH:

• w sprawie duńskich standardowych klauzul umownych dla podmiotów przetwarzających

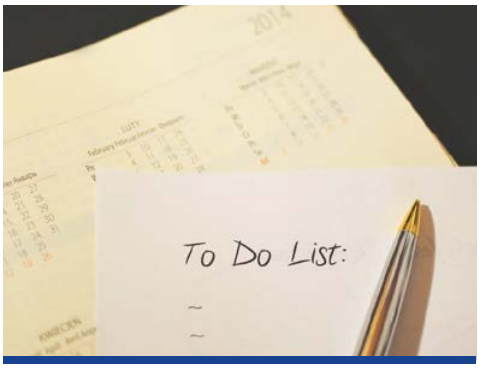
EROD wydała opinię w sprawie projektu standardowych klauzul umownych dotyczących przetwarzania danych osobowych przez podmiot przetwarzający, przedłożonego przez duński organ nadzorczy. Opinia zawiera zalecenia, które organ nadzorczy powinien wziąć pod uwagę, aby proponowane standardowe klauzule umowne mogły zostać uznane za zgodne z art. 28 ust. 8 RODO.

czytaj więcej

• w sprawie kryteriów akredytacji podmiotów monitorujących kodeksy postępowania

EROD wydała opinię do przedłożonego przez austriacki organ nadzorczy projektu decyzji w sprawie kryteriów akredytacji podmiotów monitorujących kodeksy postępowania. W opinii wskazała, że wszystkie kodeksy obejmujące podmioty niepubliczne muszą posiadać akredytowane podmioty monitorujące zgodnie z RODO.

czytaj więcej



• w sprawie ciągłości kompetencji organu nadzorczego w przypadku zmiany okoliczności dotyczących głównej lub pojedynczej jednostki organizacyjnej

EROD przyjęła opinię w sprawie ciągłości kompetencji organu nadzorczego, w przypadku gdy zmieniają się okoliczności dotyczące głównej lub pojedynczej jednostki organizacyjnej. Może to mieć miejsce w sytuacji, w której główna jednostka organizacyjna zostanie przeniesiona na inne terytorium w ramach EOG, główna jednostka organizacyjna zostanie przeniesiona do EOG z kraju trzeciego lub gdy nie będzie już głównej lub pojedynczej jednostki organizacyjnej w EOG. W takich okolicznościach, zdaniem EROD, kompetencje wiodącego organu nadzorczego mogą zostać przeniesione na inny organ nadzorczy. Procedura współpracy określona w art. 60 RODO będzie nadal obowiązywać, a nowy organ nadzorczy będzie zobowiązany do współpracy z byłym i innymi organami nadzorczymi, których sprawa dotyczy w celu osiągnięcia konsensusu. Zmiana może nastąpić, dopóki właściwy organ nadzorczy nie podejmie ostatecznej decyzji.

czytaj więcej

• w sprawie projektu wykazu rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych zgłoszonego przez cypryjski organ nadzorczy

EROD przyjęła opinię w sprawie wykazu rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych (DPIA) przedłożonego jej przez cypryjski organ nadzorczy (art. 35 ust. 4 RODO).

czytaj więcej

• w sprawie francuskiego, hiszpańskiego i czeskiego wykazu rodzajów operacji przetwarzania, które nie podlegają wymogowi dokonania oceny skutków dla ochrony danych (art. 35 ust. 5 RODO)

EROD przyjęła opinie w sprawie wykazów rodzajów operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych, zgodnie z art. 35 ust. 5 RODO, przedłożonych jej przez francuski, hiszpański i czeski organ nadzorczy.

Francja | Hiszpania | Czechy

• w sprawie eHDSI (wspólna z EIOD)

EROD przyjęła wspólną opinię z Europejskim Inspektorem Ochrony Danych (EIOD) na temat aspektów ochrony danych osobowych przetwarzania danych pacjentów w eHealth Digital Service Infrastructure (eHDSI).

czytaj więcej

INNE PRZYJĘTE DOKUMENTY:

Wspólna odpowiedź EROD i EIOD dla komisji LIBE na temat skutków amerykańskiej ustawy US CLOUD Act

EROD przyjęła wspólną odpowiedź z Europejskim Inspektorem Ochrony Danych (EIOD) dotyczącą wniosku Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego (LIBE) o ocenę prawną w sprawie wpływu amerykańskiej ustawy US CLOUD Act na unijne ramy prawne ochrony danych oraz upoważnienie Komisji do negocjacji z USA w celu zawarcia porozumienia w sprawie transgranicznego dostępu do elektronicznych materiałów dowodowych we współpracy sądowej w sprawach karnych.

czytaj więcej

Zalecenia dotyczące wykazu EIOD zgodnie z art. 39 ust. 4 rozporządzenia 2018/1725 (wykaz DPIA)

EROD przyjęła zalecenia w sprawie wykazu, o którym mowa w art. 39 ust. 4 rozporządzenia 2018/1725, przedłożonego jej przez Europejskiego Inspektora Ochrony Danych (EIOD).

treść zaleceń

Udostępnianie danych osoby zgłaszającej nieprawidłowości

Zdarza się, że organy administracji publicznej, które otrzymują informacje onieprawidłowościach i wnioski o zbadanie sygnalizowanych spraw, udostępniają dane osób je wnoszących tym, których one dotyczą. To praktyka nieznajdująca podstaw w przepisach Kodeksu postępowania administracyjnego (kpa). Jednocześnie narusza ona prywatność osób kierujących tego typu korespondencję i słusznie budzi ich sprzeciw, zwłaszcza gdy proszą o zachowanie poufności.

Jednym z przykładów takich niewłaściwych praktyk jest rozpatrywana przez Prezesa UODO sprawa dotycząca działania starosty. Został on zawiadomiony przez mieszkańca o możliwym naruszeniu przez właściciela jednej z działek przepisów w zakresie ochrony środowiska i prawa budowlanego. Starosta, uznając, że nie jest właściwy do rozpatrzenia tej sprawy, przekazał otrzymane pismo według właściwości do trzech innych urzędów. Jednocześnie zawiadomienie o przekazaniu wniosku wysłał nie tylko wnioskodawcy, ale również właścicielowi działki, którego dotyczyły zarzuty. Tym samym właściciel działki uzyskał takie dane dotyczące informatora, jak imię i nazwisko oraz adres zamieszkania.

Prezes UODO uznał, że sytuacja taka nie powinna mieć miejsca i skierował do starosty wystąpienie, by zwrócić uwagę na niewłaściwość takiej praktyki i zapobiec jej stosowaniu w przyszłości. Podkreślił w nim, że starosta, uznając się za niewłaściwego do rozpatrzenia sprawy, nie wszczął nawet postępowania administracyjnego. Gdyby jednak to zrobił, to osoba zawiadamiająca o potencjalnych naruszeniach, ale nierobiąca tego ze względu na swój interes prawny lub obowiązek, nie powinna stać się jego stroną. Nieracjonalne i nieuzasadnione jest bowiem traktowanie jako strony każdego, kto informuje organ o zaobserwowanych uchybieniach. Przepisy kpa (art. 61 § 1) umożliwiają organom administracji publicznej zbadanie tego typu sygnałów przez wszczęcie postępowania z urzędu. Wówczas (zgodnie z art. 28 kpa) jego stroną staje się wyłącznie osoba, której stawiane są zarzuty, a nie osoba zawiadamiająca o możliwych naruszeniach. Ta ostatnia nie jest więc wprawdzie informowana o przebiegu postępowania oraz o jego wynikach, ale jednocześnie nie dochodzi do ujawniania jej danych osobowych, a przez to naruszenia jej prywatności.

treść wystąpienia

Spółdzielnia mieszkaniowa była uprawniona do udostępnienia najemcy lokalu danych jego współwłaścicieli oraz informacji o wnoszonych miesięcznych opłatach

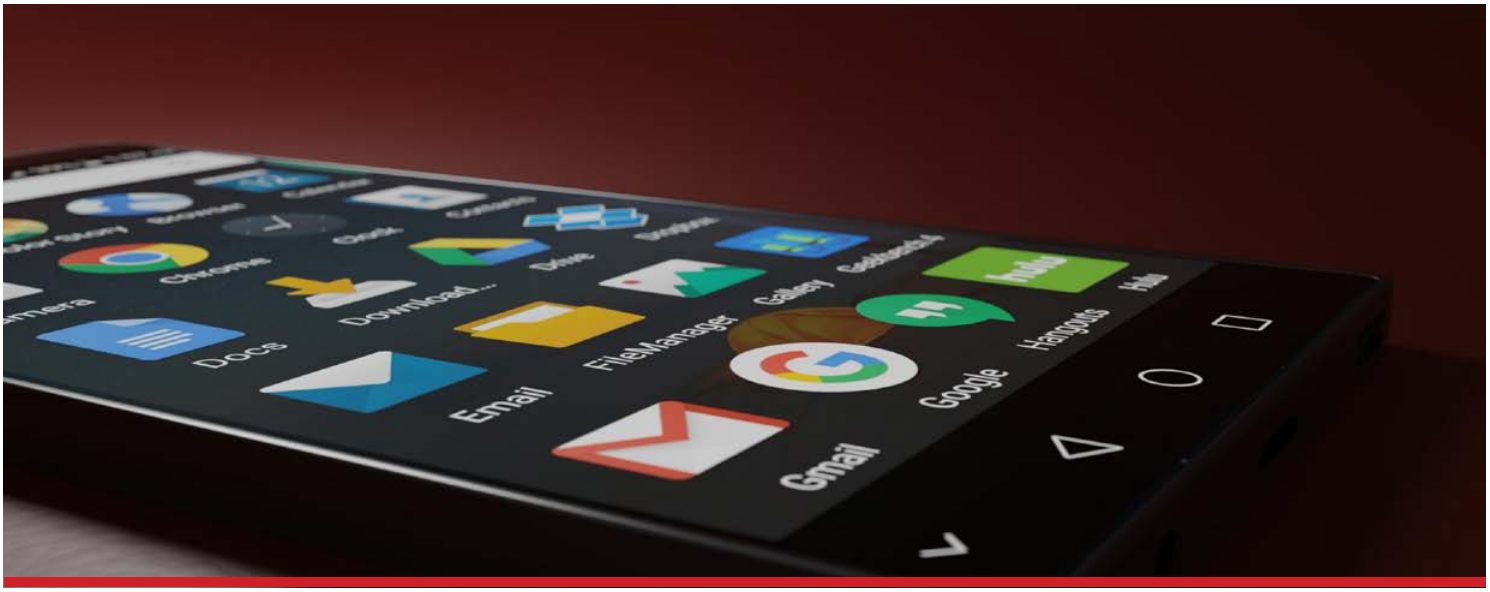
Takie stanowisko Prezes UODO wyraził w decyzji, w której analizował działanie jednej ze spółdzielni mieszkaniowych. Spółdzielnia, na wniosek osoby, która wynajęła lokal i zamierzała wystąpić o dodatek mieszkaniowy, udostępniła – po stosownej weryfikacji jej uprawnień – m.in. informacje o wysokości opłat, jakie za ten lokal wnosili jego współwłaściciele oraz ich dane osobowe, a także kod identyfikacyjny lokatora.

Prezes UODO nie dopatrzył się w tym działaniu naruszenia prawa. Wskazał, że zgodnie z przepisami ustawy z dnia 21 czerwca 2001 r. o dodatkach mieszkaniowych (Dz. U. z 2017 r., poz. 180 ze zm.), dodatek mieszkaniowy przysługuje m.in. najemcom oraz podnajemcom lokali mieszkalnych. Przyznaje go wójt, burmistrz lub prezydent miasta, w drodze decyzji administracyjnej, na wniosek osoby uprawnionej do jego uzyskania (art. 7 ust. 1 ustawy). Wzór tego wniosku określają zaś przepisy rozporządzenia Rady Ministrów z dnia 28 grudnia 2001 r. w sprawie dodatków mieszkaniowych (Dz. U. z 2001 r. Nr 156, poz. 1817 ze zm.). Zawiera on m.in. rubryki, w których wnioskodawca podaje „łączną kwotę wydatków na mieszkanie za ostatni miesiąc (według okazanych dokumentów)", przy czym prawdziwość tych informacji wymaga potwierdzenia ze strony „zarządcy domu" (pkt 12 wniosku).

Prezes UODO uznał, że w świetle powołanych przepisów działanie spółdzielni stanowiło realizację prawnie usprawiedliwionych interesów najemcy i było uprawnione w kontekście art. 6 ust. 1 lit. f RODO.

Zaznaczył przy tym, że nie można uznać, by interesy właścicieli wymagające ochrony ich danych osobowych były nadrzędne w stosunku do interesów najemcy lokalu. Przyjęcie takiego założenia oznaczałoby bowiem uniemożliwienie najemcy ubiegania się o przyznanie dodatku mieszkaniowego. Zatem jego uprawnienia w tym zakresie byłyby jedynie iluzoryczne. Z tych samych względów nie można uznać, iż jedyną osobą uprawnioną do przekazania najemcy informacji potrzebnych do ubiegania się o dodatek mieszkaniowych jest ta, która zawarła z nim umowę najmu lokalu. Stanowisko takie oznaczałoby bowiem uzależnienie możliwości ubiegania się przez najemcę lokalu o przyznanie dodatku mieszkaniowego od woli jego właściciela.

treść decyzji



Wskazówki UODO dotyczące bezpiecznego korzystania z aplikacji mobilnych

Aplikacje mobilne wymagają coraz to szerszego dostępu do różnych zasobów, a szczególnie naszych danych osobowych. Dostrzegając narastającą skalę zjawiska, Prezes UODO wydał wskazówki, jak bezpiecznie korzystać z aplikacji mobilnych, w których przypomina o najważniejszych zasadach prawidłowego i świadomego korzystania z tych nowoczesnych narzędzi. Podkreślił w nich między innymi, jak ważne jest dokładne zapoznawanie się z warunkami korzystania z aplikacji.

Administratorzy, którzy udostępniają użytkownikom aplikację, powinni dbać o właściwe spełnianie obowiązku informacyjnego zwłaszcza w sposób przejrzysty i zrozumiały informować o celach i zakresie przetwarzanych danych.

Ostatnio na podobny problem zwrócił uwagę hiszpański organ ochrony danych osobowych. W swojej decyzji ukarał on podmiot zarządzający najwyższą klasą hiszpańskich rozgrywek piłkarskich - Liga de Fútbol Profesional (LFP), za naruszenie określonej w RODO zasady przejrzystości. Oferowana przez ten podmiot aplikacja mobilna zawierała funkcjonalności, które umożliwiały zbieranie danych za pomocą mikrofonu wbudowanego w urządzenie mobilne. Hiszpański organ nadzorczy ocenił, że zbieranie tych danych powinno odbywać się przy świadomości użytkowników za każdym razem, gdy aplikacja uruchomia mikrofon.

KORZYSTANIE Z UPRAWNIENIA DO NAKŁADANIA KAR PRZEZ ORGANY NADZORCZE W UE

Jednym z założeń unijnej reformy systemu ochrony danych osobowych było zapewnienie realnego przestrzegania obowiązujących w tej dziedzinie przepisów prawa. Dlatego RODO wyposażyło organy nadzorcze w określone uprawnienia naprawcze, m.in. do nakładania administracyjnych kar pieniężnych i udzielania upomnień. Przedstawiamy przykłady takich sytuacji z ostatniego czasu:

Francuski organ nadzorczy nałożył karę za nadmierne monitorowanie pracowników

Francuski organ nadzorczy (CNIL) nałożył karę w wysokości 20 000 Euro na spółkę, która stosowała wobec pracowników nadzór wideo w sposób ciągły. Organ nadzorczy wydał również nakaz, aby spółka podjęła środki w celu zapewnienia identyfikacji dostępu do wspólnej służbowej poczty elektronicznej.
CNIL dwukrotnie ostrzegał firmę w kwestii zasad, których należy przestrzegać podczas instalowania kamer w miejscu pracy. Wskazywał w szczególności, że pracownicy nie powinni być monitorowani w sposób ciągły, a także powinni otrzymać informację o zainstalowaniu kamery.

Kontrola CNIL wykazała, że:
- zainstalowana w biurze kamera monitorowała nieprzerwanie sześciu tłumaczy na ich stanowisku pracy;
- pracownicy nie otrzymali wystarczającej informacji o tym fakcie;
- stanowiska komputerowe nie były zabezpieczone hasłem, a tłumacze uzyskiwali dostęp do firmowej poczty e-mail za pomocą jednego unikalnego hasła.

CNIL wezwał spółkę do przestrzegania przepisów o ochronie danych i zastosowania następujących zaleceń:
- przesunięcia kamery w taki sposób, aby nie nagrywała pracowników w sposób ciągły;
- poinformowania o obecności kamer;
- wdrożenie środków bezpieczeństwa dotyczących dostępu do stanowisk komputerowych i identyfikacji dostępu do profesjonalnej poczty elektronicznej.

Z powodu niepełnego zastosowania się przez spółkę do zaleceń CNIL, organ ten decyzją nałożył karę administracyjną na spółkę. Ocenił, że stosowanie monitoringu wideo pracowników wymaga zachowania szczególnej ostrożności. Podkreślił również, jak ważne jest właściwe i odpowiednie reagowania na wezwania organu nadzorczego do usunięcia uchybień.

treść komunikatu (fr)

Kara rumuńskiego organu ochrony danych

Rumuński organ ochrony danych nałożył karę na Unicredit Bank S.A. za naruszenie art. 25 ust. 1 RODO, tj. brak wdrożenia przez to przedsiębiorstwo odpowiednich środków technicznych i organizacyjnych w celu skutecznej realizacji zasad ochrony danych. Chodziło między innymi o zasadę minimalizacji danych oraz zastosowanie niezbędnych zabezpieczeń w przetwarzaniu zgodnych z RODO. Zaniedbania te doprowadziły do ujawnienia danych takich jak osobisty numer identyfikacyjny oraz adres konta w dokumentach zawierających szczegóły transakcji, które udostępniono w Internecie w okresie między 25 maja 2018 r. a 10 grudnia 2018 r. Dane te dotyczyły 337 042 osób.
Administrator został ukarany grzywną w wysokości 613 912 lei, co stanowi równowartość 130 000 euro.

treść komunikatu (en)

Belgijski organ nadzorczy upomniał za nieprzestrzeganie prawa dostępu do danych

Belgijski organ nadzorczy upomniał federalną służbę publiczną ds. zdrowia Service Public Fédéral (SPF) Santé Publique, za nieudzielenie odpowiedzi na wniosek obywatela, który chciał zrealizować prawo dostępu do swoich danych.
Sprawa dotyczyła pracownika medycznego, któremu odmówiono nominacji na stanowisko zastępcy PGC Limburg (Provincial Medical Commission of Limburg). Aby poznać motyw odmowy nominacji pracownik postanowił skorzystać z prawa dostępu do swoich danych osobowych. SPF Santé Publique nie odpowiedziała na ten wniosek, dlatego pracownik złożył skargę do organu nadzorczego. Po zapoznaniu się ze sprawą belgijski organ nadzorczy uznał, że nastąpiło zaniedbanie ze strony SPF Santé Publique. W skierowanym do podmiotu upomnieniu podkreślił, że RODO przyznaje osobom fizycznym prawa, które pozwalają im chronić ich dane. Jednym z nich jest prawo dostępu do ich danych, do sprostowania, usunięcia lub sprzeciwu i w każdym momencie osoby te mogą dochodzić tych praw.

treść komunikatu (fr)

Brytyjski organ nadzorczy wydał oświadczenie o zamiarze ukarania Marriott International Inc

Brytyjski organ nadzorczy ds. ochrony danych osobowych prowadzący dochodzenie w imieniu innych organów ochrony danych w państwach członkowskich UE, wydał oświadczenie o zamiarze ukarania Marriott International Inc. Marriott w listopadzie 2018 r., zgłosił do ICO incydent cybernetyczny, w wyniku którego doszło do wycieku danych osobowych ok. 339 mln gości (ok. 30 mln odnosiło się do mieszkańców 31 państw Europejskiego Obszaru Gospodarczego). Dochodzenie ICO wykazało, że do naruszenia danych osobowych doszło w 2014 r., ustalono, że ujawnienie informacji o klientach nie zostało odkryte aż do 2018 r.

Wedle ICO, Marriott nie dołożył należytej staranności zakupując Starwood w zakresie ochrony danych osobowych, a także nie wdrożył odpowiednich środków technicznych i organizacyjnych aby zabezpieczyć swoje systemy. Jak wskazała Komisarz ds. Informacji Elizabeth Denham: „RODO wyjaśnia, że podmioty przetwarzające muszą być odpowiedzialne za przechowywane przez nie dane osobowe. Może to obejmować dochowanie należytej staranności przy dokonywaniu przejęć korporacyjnych i wprowadzenie odpowiednich środków rozliczalności nie tylko danych osobowych, które zostały pozyskane, ale także sposobu ich ochrony. Dane osobowe posiadają realną wartość, dlatego podmioty je przetwarzające mają prawny obowiązek zapewnić ich bezpieczeństwo, tak jak w przypadku innych aktywów. Jeśli tak się nie stanie i gdy będzie to konieczne, nie zawahamy się podjąć zdecydowanych działań, aby chronić prawa obywateli."

Warto zaznaczyć, że ICO poinformował opinię publiczną o zamiarze ukarania, nie zaś o ukaraniu podkreślając jednocześnie, że podejmując kolejne kroki w sprawie weźmie pod uwagę wyjaśnienia złożone przez Marriott oraz wskazówki innych organów nadzorczych z państw, których mieszkańcy zostali dotknięci naruszeniem.

treść komunikatu (en)

UODO przygotował w projekcie T4DATA nowe narzędzie do samokształcenia IOD

Już działa platforma z wykładami online specjalistów z Urzędu Ochrony Danych Osobowych adresowana do inspektorów ochrony danych pełniących tę funkcję w administracji publicznej. Platforma jest dostępna pod adresem https://t4data.uodo.gov.pl/ i w miejscu tym UODO będzie udostępniał cyklicznie materiały edukacyjne online. Naszym zamierzeniem w ramach wykładów jest umożliwienie inspektorom zarówno usystematyzowania wiedzy z zakresu ochrony danych osobowych, jak i zapoznanie się z praktycznymi aspektami stosowania RODO.

Aby skorzystać z platformy wystarczy się na niej zarejestrować. Każdy użytkownik uzyska także możliwość samodzielnej weryfikacji zdobytej wiedzy poprzez testy sprawdzające. Będzie mógł również ocenić wykład, z którym się zapoznał.

Platforma zawiera również wykłady zarejestrowane podczas szkoleń lokalnych dla IOD, zrealizowane przez UODO w ramach projektu T4DATA na przełomie maja i czerwca 2019 r. w Poznaniu, Gdyni, Rzeszowie i Warszawie. Zostały one ocenione przez wielu ich uczestników jako bardzo pomocne w codziennej praktyce inspektorów, co jest dla nas powodem dużej satysfakcji.

Wspomniany projekt „T4DATA – szkolenie organów ochrony danych i inspektorów ochrony danych" to wspólne przedsięwzięcie organów ochrony danych z Polski, Włoch, Hiszpanii, Bułgarii oraz Chorwacji. Projekt powstał, aby ułatwić organom nadzorczym ds. ochrony danych tych państw oraz inspektorom ochrony danych z podmiotów publicznych dostęp do wiedzy o praktycznych konsekwencjach stosowania i możliwych interpretacjach RODO. Projekt T4DATA jest współfinansowany ze środków Unii Europejskiej z Programu „Prawa, Równość i Obywatelstwo (2016–2020)".

Projekt współfinansowany w ramach Programu Unii Europejskiej Prawo, Równość i Obywatelstwo (2014-2020)

Wzrost zainteresowania mediów działalnością UODO

Wakacje w pełni, ale praca wre. Zauważyli to także dziennikarze, którzy w lipcu skupili wyjątkową uwagę na działaniach UODO. Łącznie na temat naszych inicjatyw powstało aż 1676 materiałów prasowych. To o 100 proc. więcej niż przed miesiącem.

Lipiec obfitował w kilka wiodących tematów. Przede wszystkim uwagę opinii publicznej przyciągnęło stanowisko UODO, w którym stwierdzono, że nie ma podstawy prawnej, która umożliwiałaby pracodawcom samodzielną kontrolę pracowników alkomatem.

Ponadto media szeroko komentowały działania UODO, które nastąpiły na skutek czerwcowego wystąpienia Prezesa UODO do Ministra Cyfryzacji. Prezes UODO zwrócił wówczas uwagę na potrzebę zmiany przepisów, które dostosują aktualne regulacje prawne dotyczące kwalifikowanego podpisu elektronicznego do zasad wyrażonych w RODO.

Dziennikarze często prezentowali także stanowisko, które UODO wyraziło w związku z wejściem w życie ustawy o dokumentach publicznych. Zwrócono w nim uwagę, że nie każda kopia dokumentu publicznego będzie miała cechy autentyczności, nie mniej podmiot, który skopiuje np. dowód osobisty może odpowiadać za przetwarzanie zbyt szerokiego zakresu danych osobowych.

Ogromnym zainteresowaniem dziennikarzy cieszył się także materiał poradniczy poświęcony ochronie danych w aplikacjach mobilnych, a wskazówki w nim zawarte wykorzystali w swoich materiałach dziennikarze zarówno mediów ogólnopolskich, jak i lokalnych.

Powstały także publikacje poświęcone propozycji zmian przepisów dotyczących procedury „Niebieskiej karty", które doprowadziłyby do precyzyjnego określenia jakie dane osobowe mają być dostępne.

Duże zainteresowanie mediów wzbudziły także postanowienia Prezesa UODO o wszczęciu postępowania wobec Kancelarii Sejmu.

W dalszym ciągu do najaktywniejszych mediów, które często informowały w minionym miesiącu o działalności UODO, wśród prasy tradycyjnej należą dzienniki, np. Dziennik Gazeta Prawna oraz Rzeczpospolita, a także dzienniki branżowe, np. Gazeta Podatkowa. Do tego grona w lipcu dołączyły także dzienniki regionalne. Z kolei wśród mediów internetowych o wspomnianych działaniach UODO informowały zarówno ogólnopolskie serwisy informacyjne, jak i liczne portale lokalne oraz branżowe.

Nowe odpowiedzi w zakładce „Inspektor Ochrony Danych”

Do funkcjonującej na naszej stronie zakładki „Inspektor Ochrony Danych”/„Zadania IOD” dodaliśmy nowe zagadnienia. Kolejne zagadnienia dotyczą następujących kwestii:

- Jak identyfikować podopiecznych Domu Pomocy Społecznej w związku z podawaniem leków?
- Czy żłobek jest administratorem danych stażysty skierowanego na staż przez Powiatowy Urząd Pracy?
- Jak długo powinny być udostępniane w BIP oświadczenia majątkowe, np. radnego, wójta?
- Czy prywatny numer telefonu sołtysa stanowi informację publiczną?

Na stronie UODO dostępna jest nowa zakładka „Kodeksy i Certyfikacja”

W nawiązaniu do informacji z poprzedniego wydania newslettera o przyjęciu przez EROD Wytycznych 1/2018, Wytycznych 4/2018 i Wytycznych 1/2019 oraz w związku z dużym zainteresowaniem kwestiami kodeksów i mechanizmów certyfikacji, na stronie internetowej UODO uruchomiona została nowa zakładka Kodeksy i certyfikacja. Zawiera ona podstawowe informacje o tworzeniu kodeksów, przyszły rejestr zatwierdzonych dokumentów oraz informacje o mechanizmach certyfikacji. Zakładka ta będzie na bieżąco aktualizowana.

przejdź do zakładki