



NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

- str. 2 **UDOSTĘPNIANIE INFORMACJI W ZWIĄZKU Z DOFINANSOWANIEM WYMIANY
PIECA WĘGLOWEGO NA PROEKOLOGICZNY**
- str. 3 **ZAKRES DANYCH OSOBOWYCH PRZY PEŁNOMOCNICTWIE**
- str. 4 **KONTAKTOWANIE SIĘ PARTII Z BYŁYM CZŁONKIEM**
- str. 5 **SCHRONISKO MA OBOWIĄZEK CHRONIĆ DANE OSOBOWE OSÓB
ADOPTUJĄCYCH ZWIERZĘTA**
- str. 6 **PROJEKT NOWELIZACJI USTAWY PRAWO O NOTARIACIE WYMAGA
DOPRACOWANIA**
- str. 7 **CO SIĘ STAŁO? ZASZŁO NARUSZENIE**
- str. 9 **MIĘDZYNARODOWE**
- str. 10 **KARY**
- Finlandia: pierwsze kary za naruszenie danych
 - Belgia: ukarano kandydata w wyborach lokalnych
 - Szwecja: spółdzielnia mieszkaniowa zakazała stosowania monitoringu wideo przy wejściu do budynku mieszkalnego
- str. 12 **KONSULTACJE SPOŁECZNE**
- str. 12 **KODEKS POSTĘPOWANIA DLA JEDNOSTEK OŚWIATOWYCH**
- str. 13 **PROJEKT KODEKSU POSTĘPOWANIA DLA FOTOGRAFÓW**
- str. 13 **NOWE ODPOWIEDZI NA PYTANIA INSPEKTORÓW**



UDOSTĘPNIANIE INFORMACJI W ZWIĄZKU Z DOFINANSOWANIEM WYMIANY PIECA WĘGLOWEGO NA PROEKOLOGICZNY

Prezydent miasta nie naruszył prawa do ochrony danych osobowych, udostępniając informacje związane z wysokością dofinansowania na likwidację źródeł tzw. niskiej emisji zanieczyszczeń powietrza.

Taką decyzję Prezes UODO wydał po rozpatrzeniu skargi osoby, której dotyczyły udostępnione informacje.

Skarżący wskazywał, że prezydent miasta w odpowiedzi na wniosek złożony w trybie ustawy o dostępie do informacji publicznej udostępnił dane osobowe jego i współwłaściciela nieruchomości oraz poinformował o wysokości udzielonego dofinansowania wraz z innymi danymi dotyczącymi umowy przyznającej dotację.

Z kolei prezydent miasta w złożonych w sprawie wyjaśnieniach zaznaczył, że przetwarza dane osobowe skarżącego na podstawie uchwały rady miasta w sprawie określenia zasad udzielania dotacji celowej na dofinansowanie ochrony środowiska i gospodarki wodnej na terenie miasta oraz trybu postępowania w sprawie udzielania dotacji i sposobu jej rozliczenia. Poinformował, że celem przetwarzania danych jest udzielenie dotacji celowej na zmianę systemu ogrzewania z węglowego na proekologiczny zgodnie ze złożonym wnioskiem. Zakres przetwarzanych danych ograniczony jest do danych znajdujących się w umowie zawartej między miastem a skarżącym, dotyczącej przyznania dotacji.

Jednocześnie prezydent podkreślił, że w odpowiedzi na wniosek o dostęp do informacji publicznej nie udostępnił danych skarżącego, bowiem te zawarte już były w złożonym wniosku. Przekazał jedynie informację publiczną w zakresie gospodarowania mieniem komunalnym.

Wskazał również, że udzielenie dotacji następuje na podstawie zawartej z miastem umowy, a zgodnie z linią orzecniczą sądów administracyjnych sam fakt zawarcia umowy z jednostką samorządu terytorialnego skutkuje tym, że dane osobowe w postaci imienia i nazwiska osoby fizycznej, która zawarła taką umowę, podlegają udostępnieniu jako informacja publiczna.

Po przeanalizowaniu sprawy Prezes UODO uznał, że prezydent miasta nie naruszył przepisów RODO. W wydanej w tej sprawie decyzji wskazał, że zgodnie z wyjaśnieniami udzielonymi przez prezydenta miasta, informacji publicznej udzielono w zakresie gospodarowania mieniem komunalnym, na podstawie ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej.



ZAKRES DANYCH OSOBOWYCH PRZY PEŁNOMOCNICTWIE

Obowiązkiem administratora jest ustalenie w każdym przypadku, jaki minimalny zakres danych osobowych jest dla niego wystarczający do identyfikacji konkretnej osoby fizycznej.

Jaki zakres danych osobowych powinien być, zgodnie z RODO, udostępniany w piśmie dotyczącym udzielenia pełnomocnictwa osobie fizycznej? Czy na te potrzeby może być pozyskiwany i podawany numer PESEL, który – zgodnie z art. 87 RODO – jako krajowy numer identyfikacyjny wymaga szczególnej ochrony? Czy można łączyć go z numerem dowodu osobistego? Z takimi pytaniami zwracają się do UODO różne podmioty.

W kierowanych do nich wyjaśnieniach organ ds. ochrony danych osobowych podkreśla, że jednoznaczne wskazanie danych osobowych, które powinny identyfikować pełnomocnika w każdym stanie faktycznym jest trudne. Niewątpliwie przestrzegać należy zasady minimalizacji danych i w każdym przypadku kierować się analizą przepisów szczególnych.

Pomocniczo UODO wskazuje, że o udzielaniu pełnomocnictw traktują Rozdział II Kodeksu cywilnego oraz art. 32 i 33 Kodeksu postępowania administracyjnego (kpa). Wymienione przepisy nie zawierają informacji o rodzaju danych osobowych umożliwiających identyfikację pełnomocnika. Warto jednak zwrócić uwagę na treść art. 126 § 2 pkt 2 Kodeksu postępowania cywilnego, w którym czytamy, że gdy pismo procesowe jest pierwszym pismem w sprawie, powinno zawierać m.in. oznaczenie przedmiotu sporu oraz numer Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL) lub numer identyfikacji podatkowej (NIP) powoda będącego osobą fizyczną, jeżeli jest on obowiązany do jego posiadania lub posiada go, nie mając takiego obowiązku.

Ponieważ pełnomocnik strony postępowania zastępuje ją w czynnościach procesowych, można przyjąć, że jego identyfikacja jest równie ważna, jak identyfikacja strony.

Zgodnie zaś z art. 63 § 2 kpa, podanie powinno zawierać co najmniej wskazanie osoby, od której pochodzi,

jej adres i żądanie oraz czynić zadość innym wymaganiom ustalonym w przepisach szczególnych. Podanie może być złożone również w formie elektronicznej, wtedy powinno być opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym, lub uwierzytelniane w sposób zapewniający możliwość potwierdzenia pochodzenia i integralności weryfikowanych danych w postaci elektronicznej (art. 63 § 3a pkt 1 kpa). Jak zaś stanowi art. 3 pkt 14a ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, podpis zaufany zawiera m.in. dane identyfikujące osobę, ustalone na podstawie środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej, obejmujące imię, nazwisko i numer PESEL.

Trudne jest więc jednoznaczne wskazanie danych osobowych, które powinny identyfikować pełnomocnika w każdym stanie faktycznym. Niemniej numer PESEL jest niewątpliwie daną identyfikacyjną i w obowiązującym stanie prawnym brak jest przepisów uniemożliwiających posługiwanie się nią w jego identyfikacji.

Niemniej warto podkreślić, że wśród wymienionych w art. 5 RODO zasad dotyczących przetwarzania danych osobowych, są również zasada zgodności z prawem i minimalizacji danych. Dotyczą one nie tylko ilości przetwarzanych danych i ich łączenia, np. numeru dowodu osobistego z numerem PESEL, ale również ich charakteru.

Obowiązkiem administratora jest ustalenie w każdym przypadku, jaki minimalny zakres danych osobowych jest dla niego wystarczający do identyfikacji konkretnej osoby fizycznej. Należy przy tym wziąć również pod uwagę przepisy szczególne, które w danych sprawach mogą określać cechy, jakie powinien posiadać pełnomocnik. W takich przypadkach zakres minimalnych danych do identyfikacji będzie zwiększony o cechy wymagane szczególnymi przepisami prawa.



KONTAKTOWANIE SIĘ PARTII Z BYŁYM CZŁONKIEM

Prezes UODO udzielił jednej z partii politycznych upomnienia za bezprawne przetwarzanie danych osobowych byłego jej członka. Polegało ono na wysyłaniu do niego zaproszeń na spotkania okolicznościowe kierowane do członków tej partii.

Decyzja taka została wydana w związku ze skargą osoby, która była zatrudniona w tej partii oraz przez pewien czas była jej członkiem. Jednak po złożeniu rezygnacji z członkostwa w partii oraz pomimo przesłania wniosku o usunięcie danych osobowych z rejestrów partii, były jej członek wciąż otrzymywał zaproszenia na różne spotkania okolicznościowe wysyłane do członków partii.

Prezes UODO, po przeanalizowaniu wszystkich okoliczności uznał, że działanie takie było bezprawne i wydał decyzję udzielającą partii upomnienia.

Zasady określone w RODO

W jej uzasadnieniu organ ds. ochrony danych osobowych wskazał, że dane osobowe w każdym przypadku muszą być przetwarzane przez administratora zgodnie ze wszystkimi zasadami określonymi w art. 5 RODO, w tym m.in. z tzw. zasadą legalności (art. 5 ust. 1 lit. a RODO) oraz zasadą ograniczonego celu (art. 5 ust. 1 lit. b RODO). Pierwsza z nich stanowi, że dane osobowe muszą być przetwarzane przez administratora zgodnie z prawem, tj. na podstawie przynajmniej jednej z przesłanek określonych w art. 6 RODO. Z zasady ograniczonego celu wynika natomiast, że dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

Pamiętać też należy, że przepisy RODO przyznają osobie, której dane dotyczą, liczne uprawnienia związane z przetwarzaniem jej danych osobowych przez administratora. Jednym z nich jest prawo do żądania usunięcia danych osobowych. Może ono zostać skutecznie zrealizowane jedynie w przypadku, gdy zostaną spełnione

przesłanki wprost wskazane w art. 17 ust. 1 lit. a)–f) RODO. Należy zwrócić uwagę, że prawo do usunięcia danych osobowych jest w określonych sytuacjach wyłączone. Stosownie bowiem do art. 17 ust. 3 RODO, prawo do usunięcia danych osobowych nie ma zastosowania w zakresie, w jakim przetwarzanie jest niezbędne m.in. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 17 ust. 3 lit. b RODO). W przypadku zaistnienia tej okoliczności, podmiot danych nie będzie uprawniony do żądania od administratora usunięcia jego danych osobowych.

Przepisy szczególne legalizujące przetwarzanie danych byłego pracownika

W wydanej decyzji Prezes UODO wskazał, że w analizowanej sprawie partia była zobowiązana do przechowywania dokumentacji pracowniczej skarżącego, który kiedyś był jej pracownikiem – tym samym miała prawo do przetwarzania w tym celu jego danych osobowych. Zgodnie bowiem z art. 94 pkt 9a Kodeksu pracy, pracodawca jest obowiązany prowadzić i przechowywać w postaci papierowej lub elektronicznej dokumentację w sprawach związanych ze stosunkiem pracy oraz akta osobowe pracowników (dokumentacja pracownicza). Zgodnie z pkt 9b tego przepisu, pracodawca jest także obowiązany przechowywać dokumentację pracowniczą w sposób gwarantujący zachowanie jej poufności, integralności, kompletności oraz dostępności, w warunkach niegroźących uszkodzeniem lub zniszczeniem przez okres zatrudnienia, a także przez okres 10 lat, licząc od końca roku kalendarzowego, w którym stosunek

pracy uległ rozwiązaniu lub wygaś, chyba że odrębne przepisy przewidują dłuższy okres przechowywania dokumentacji pracowniczej. W myśl natomiast art. 125a ust. 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, płatnik składek jest zobowiązany przechowywać listy płac, karty wynagrodzeń albo inne dowody, na podstawie których następuje ustalenie podstawy wymiaru emerytury lub renty – co do zasady – przez okres 50 lat od dnia zakończenia przez ubezpieczonego pracy u danego płatnika.

Tym samym przetwarzanie danych osobowych skarżącego we wskazanych wyżej celach było uprawnione, gdyż spełniało przesłankę z art. 6 ust. 1 lit. c RODO.

Jednocześnie Prezes UODO uznał, że wniosek skarżącego o usunięcie wszystkich jego danych osobowych

przetwarzanych przez partię nie mógł zostać przez nią zrealizowany. Prawo do usunięcia danych osobowych jest bowiem wyłączone, jeśli ich przetwarzanie jest niezbędne do wywiązania się z obowiązku prawnego (stosownie do treści powołanego art. 17 ust. 3 lit. b RODO).

Ograniczenia po ustaniu członkostwa

Natomiast od dnia, od którego skarżący przestał być członkiem partii, nie powinna ona przetwarzać jego danych osobowych w celach związanych z zapraszaniem go na wydarzenia okolicznościowe organizowane dla członków tej partii. Działanie takie Prezes UODO uznał za naruszające zasadę ograniczonego celu, o której mowa w art. 5 ust. 1 lit. b RODO, za co udzielił partii upomnienia.

SCHRONISKO MA OBOWIĄZEK CHRONIĆ DANE OSOBOWE OSÓB ADOPTUJĄCYCH ZWIERZĘTA

Dyrektor schroniska dla bezdomnych zwierząt słusznie nie udostępnił danych osobowych nowych właścicieli adoptowanego psa jego poprzedniej właścicielce – uznał Prezes UODO.



Sprawa rozpatrywana w ostatnim czasie przez organ ds. ochrony danych osobowych dotyczyła skargi osoby, która adoptowała psa ze schroniska dla bezdomnych zwierząt, a następnie – ze względu na brak możliwości sprawowania nad nim opieki – ponownie go tam oddała. Po pewnym czasie postanowiła jednak zwierzę odzyskać i zwróciła się do schroniska o wydanie danych osobowych (imienia, nazwiska, adresu) nowych właścicieli psa, w celu wniesienia przeciwko nim powództwa o wydanie psa. Podnosiła, że niezbędnym elementem wniosku z art. 194 k.p.c. jest oznaczenie imienia, nazwiska oraz miejsca zamieszkania przyszłej strony procesowej postępowania. Brak danych osobowych uniemożliwia nadanie sprawie dalszego biegu.

Schronisko odmówiło jednak udostępnienia danych osobowych nowych właścicieli psa. Dyrektor placówki wskazał, że osoby, które podpisują umowy adopcyjne, podają swoje dane osobowe i zgadzają się na piśmie, aby mogły być one przetwarzane dla potrzeb schroniska. Schronisko nie może ich udostępniać osobom postronnym, m.in. dlatego, żeby nie dopuścić do sytuacji, w których osoby

adoptujące zwierzęta będą później niepokojone przez poprzednich ich właścicieli, którzy po jakimś czasie chcą je odzyskać.

Po analizie zgromadzonego w tej sprawie materiału, Prezes UODO uznał, że dyrektor schroniska postąpił słusznie, nie udostępniając danych osobowych nowych właścicieli adoptowanego psa poprzedniej jego właścicielce. W opinii organu nadzorczego, powołanie się przez nią na konieczność pozyskania tych danych na potrzeby złożenia pozwu o wydanie psa jest niewystarczające.

Schronisko, jako administrator, ma obowiązek chronić dane osobowe osób adoptujących zwierzęta. Przede wszystkim ma przetwarzać je w tym celu, dla którego zostały zebrane, tj. w celu realizacji umowy adopcyjnej, i nie może udostępniać ich bez podstawy prawnej. Zdaniem organu do spraw ochrony danych osobowych, w niniejszej sprawie nie została wykazana żadna z przesłanek z art. 6 ust. 1 RODO dla zmiany pierwotnego celu przetwarzania danych przez schronisko i udostępnienia tych danych wnioskującemu.



PROJEKT NOWELIZACJI USTAWY PRAWO O NOTARIACIE WYMAGA DOPRACOWANIA

Nałożenie na notariuszy ustawowego obowiązku utrwalania przebiegu wszystkich czynności notarialnych za pomocą urządzenia rejestrującego obraz i dźwięk to rozwiązanie, które budzi zastrzeżenia Prezesa UODO.

Organ ds. ochrony danych osobowych, przedstawiając swoje uwagi do projektu nowelizacji ustawy Prawo o notariacie wskazał, że przyjęcie takiego rozwiązania - uzasadnianego „koniecznością zapewnienia pełnego udokumentowania czynności notarialnych oraz prawidłowości tychże czynności” - będzie się wiązało ze znaczną ingerencją w prywatność osób. I to nie tylko tych, które dokonują czynności notarialnych, ale także pozostałych, które tylko w nich uczestniczą. Ponadto samo utrwalanie czynności notarialnych nie będzie powodowało, że czynności te zyskają przymiot prawidłowych.

Dlatego w opinii Prezesa UODO należałoby dokonać powtórnej oceny, czy nagrywanie jest rzeczywiście niezbędne dla osiągnięcia wskazanych celów, czy też można wprowadzić inne, mniej inwazyjne i zgodne z RODO metody zapewniania odpowiedniego przebiegu czynności notarialnych.

Zakres danych nie może być nadmiarowy

Gdyby bowiem projektowane rozwiązania miały zostać wprowadzone w życie, dochodziłoby do przetwarzania wielu danych osobowych. Dlatego już teraz należy ocenić, czy ich zakres nie byłby nadmiarowy. Podczas przeprowadzania czynności notarialnych osoby ich dokonujące i uczestnicy tych czynności wymieniają bowiem między sobą różne informacje, często głęboko ingerujące w prywatność, niekiedy wręcz intymne. Utrwalanie wizerunku osób stawiających się w kancelarii notarialnej oznaczałoby z kolei przetwarzanie nie tylko wyglądu, ale także np. informacji o stanie zdrowia, niepełnosprawności, pochodzeniu osób, ich cechach charakterystycznych, relacjach je łączących. Proponowanemu utrwalaniu i dalszemu przetwarzaniu podlegałyby zatem także dane szczególnie kategorii, o których stanowią przepisy art. 9 RODO.

Potrzebna ocena skutków dla ochrony danych

Utrwalanie obrazu i dźwięku to również rodzaj przetwarzania związany z użyciem nowych technologii. Zatem wprowadzenie takich rozwiązań powinno być poprzedzone dokonaniem przez projektodawcę wpływu przyjmowanych rozwiązań na prywatność, tj. oceną skutków dla ochrony danych, o której mowa w art. 35 RODO. Uzasadnienie do projektu ustawy takiej oceny nie zawiera. Tymczasem mogłaby ona wykazać konieczność lub brak niezbędności wprowadzenia obowiązku utrwalania przebiegu czynności notarialnych za pomocą urządzenia rejestrującego obraz i dźwięk, zwłaszcza w kontekście wskazywanego uzasadnienia dla tych rozwiązań, tj. konieczności zapewnienia pełnego udokumentowania oraz prawidłowości tychże czynności.

Jaki okres retencji?

Ponownej weryfikacji poddać należałoby również przewidziany w projekcie, dziesięcioletni okres przechowywania nagrań zawierających dane osobowe, a także możliwość wydłużenia tego okresu.

Co powinno znaleźć się w ustawie?

Ponadto Prezes UODO zwrócił uwagę, że większość kwestii związanych z utrwalaniem obrazu i dźwięku z przeprowadzanych czynności notarialnych projektodawca proponuje uregulować w akcie rangi rozporządzenia. Tymczasem uzasadnione jest, aby to jednak w przepisach rangi ustawy, a nie aktu wykonawczego, określić tak podstawowe kwestie związane z nakładanym obowiązkiem utrwalania, jak: zasady udostępniania nagrań, cele takiego udostępniania, gwarancje należytego zabezpieczenia praw i wolności nagrywanych osób dokonujących czynności notarialnych.



CO SIĘ STAŁO? ZASZŁO NARUSZENIE

Minęły dwa lata odkąd stosujemy ogólne rozporządzenie o ochronie danych (RODO). Administratorzy mają coraz mniej problemów z tym, żeby zidentyfikować naruszenie ochrony danych. Natomiast w dalszym ciągu problemem jest analiza ryzyka, a więc ocena zaistniałego naruszenia pod kątem wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych. Dotyczy to także szkół.

Wyjaśnieniu najczęstszych problemów związanych z naruszeniem ochrony danych w placówkach oświatowych poświęcony był wykład on-line pt. „RODO w szkolnej ławce - vademecum naruszeń”, zorganizowany przez Urząd Ochrony Danych Osobowych 9 czerwca 2020 r. Jego bezpośrednimi adresatami byli dyrektorzy i nauczyciele, uczestniczący w X edycji programu edukacyjnego „Twoje dane – Twoja sprawa”. (<https://uodo.gov.pl/pl/434>). Jednak z uwagi na tematykę miał charakter otwarty.

Siedem przykładów naruszeń, których szkoły mogą uniknąć

Wśród zgłaszanych naruszeń do Urzędu Ochrony Danych Osobowych najczęstsze przypadki, które dotyczą placówek oświatowych, to:

- udostępnienie danych osobowych nieuprawnionym osobom w związku z wysyłaniem poczty elektronicznej
- zagubienie lub kradzież niezabezpieczonych (niezaszyfrowanych) urządzeń informatycznych z danymi osobowymi (smartfony, komputery przenośne)
- zablokowanie dostępności do danych osobowych
- zagubienie przez pracowników dokumentów zawierających dane osobowe
- wysyłanie dokumentów na niewłaściwy adres korespondencyjny
- niewłaściwa anonimizacja danych osobowych oraz niszczenie archiwalnej dokumentacji
- udostępnienie dokumentacji medycznej ucznia nieuprawnionej osobie trzeciej

Warto stworzyć procedurę zgłaszania naruszenia

Jednym z wątków, na który zwrócono uwagę podczas wykładu on-line, była kwestia analizy ryzyka. Dokonanie szybkiej i prawidłowej analizy ryzyka naruszenia praw lub wolności osób fizycznych ułatwiają opracowane oraz wdrożone w organizacji procedury zgłaszania naruszeń.

Jak wynika z RODO administrator ma 72 godziny od stwierdzenia naruszenia na zgłoszenie tego zdarzenia do organu nadzorczego. W przypadku identyfikacji tego naruszenia posłużenie się procedurą umożliwi administratorowi szybkie podjęcie decyzji, czy dany incydent należy zgłosić do Prezesa UODO, czy też jest to zdarzenie, które powoduje małe prawdopodobieństwo naruszenia praw i wolności osoby fizycznej, i można go wpisać tylko do wewnętrznej ewidencji.

Taka procedura zgłaszania naruszeń powinna przede wszystkim: określać cel, w jakim procedura została opracowana; zakres jej stosowania; katalog ewentualnych zagrożeń, jakie mogą wystąpić w związku z przetwarzaniem danych u konkretnego administratora; opis etapów zarządzania naruszeniem, począwszy od jego wykrycia, a kończąc na usunięciu; opis postępowania personelu administratora w przypadku wystąpienia naruszenia ochrony danych.

Istnieją narzędzia ułatwiające skuteczne zgłoszenie

Innymi wątkami, które omówiono podczas czerwcowego wykładu, były czynności składające się na zgłoszenie naruszenia. Zwrócono uwagę m.in. na to, że RODO określa minimalny zakres informacji, jakie administrator podaje organowi nadzorcemu (art. 33 ust. 3 RODO).

Zgłoszenie naruszenia organowi nadzorczemu dokonuje administrator. Jednak samo zgłoszenie nie wszczyna postępowania administracyjnego (analogicznie dzieje się podczas dokonania wstępnego zgłoszenia). Organowi nadzorczemu chodzi przede wszystkim o szybkość zgłoszenia naruszenia. Dla administratora oznacza to, że naruszenie może zgłosić każdy pracownik administratora, np. dyrektor szkoły, zastępca, sekretarka, pracownik administracyjny, ale też nauczyciel. Zgłoszenie również będzie przyjęte, jeśli np. nie będzie zawierało podpisu tradycyjnego lub w formie elektronicznej zgłaszającego lub jeżeli zgłaszający nie dołączy do takiego zgłoszenia pełnomocnictwa, chociaż zaleca się, aby takie osoby posiadały taki dokument.

Z kolei gdy chodzi o formę zgłoszenia, to RODO nic na ten temat nie stanowi. Również nie ma w RODO dyspozycji dla organu nadzorczego, w jakiej formie ma ono nastąpić, dlatego zgłaszający może skorzystać z wielu możliwości (<https://uodo.gov.pl/pl/134/233>). Jedną z nich jest dokonanie zgłoszenia w sposób tradycyjny, wysyłając je na adres Urzędu.

Uwaga!

Niestety, zdarza się, że zgłaszający używa starych formularzy. To wynika z tego, że w dalszym ciągu mogą one stanowić załącznik do opracowywanych procedur zgłaszania naruszeń do organu nadzorczego. Jeśli formularze są załącznikami do obecnie obowiązujących procedur, to warto je zaktualizować. Te najświeższe wzory można pobrać ze strony www.uodo.gov.pl.

Chcąc zgłosić naruszenie elektronicznie administrator może posłużyć się np. formularzem interaktywnym, również dostępnym na stronie UODO. Zawiera

on wszystkie niezbędne składniki zgłoszenia, dlatego administrator unika ryzyka pominięcia ważnych elementów opisu. Jednak używając wspomnianego formularza, np. podczas zgłoszenia wstępnego, dla organu nadzorczego będzie istotne, aby administrator określił orientacyjnie czas zgłoszenia uzupełniającego. Dla usprawnienia procesu zgłoszenia warto także posługiwać się sygnaturą. Niebagatelne znaczenie ma także rzeczowe wypełnianie punktów formularza poświęconych opisom naruszenia oraz środkom zaradczym.

Ponadto możliwe jest zgłoszenie naruszeń w formie elektronicznej przez: elektroniczną skrzynkę podawczą ePUAP lub za pomocą dedykowanego formularza elektronicznego albo pisma ogólnego poprzez platformę biznes.gov.pl, a nawet za pośrednictwem e-maila, chociaż to zdarza się rzadko. Przy czym w tym ostatnim przypadku dobrą praktyką byłoby szyfrowanie formularzy, informacji, przekazywanych organowi nadzorczemu, a to dlatego, że w zgłoszeniu trzeba m.in. podać tzw. środki zaradcze, a więc mimo że ogólnie, to jednak zgłaszający opisuje, jakie środki organizacyjne i techniczne obowiązują w jednostce administratora czy jakie administrator zamierza wprowadzić w związku z naruszeniem.

Więcej informacji przydatnych w zrozumieniu i stosowaniu podejścia opartego na ryzyku znajduje się w dwuczęściowym poradniku UODO pt. Jak rozumieć podejście oparte na ryzyku według RODO? oraz Jak stosować podejście oparte na ryzyku?, który jest dostępny pod linkiem <https://uodo.gov.pl/pl/383/208>.

Zapis webinarium dostępny pod linkiem <https://uodo.gov.pl/pl/434/1560>.



MIĘDZYNARODOWE

Zarówno organy unijne, jak i organy nadzorcze państw członkowskich podjęły działania, także o charakterze informacyjno-edukacyjnym, w walce z koronawirusem. Zapraszamy do zapoznania się z przykładem z Francji. CNIL wzywa do zachowania czujności w zakresie stosowania tzw. „inteligentnych” kamer i kamer termowizyjnych

W kontekście epidemii COVID-19, a w szczególności w obecnym okresie odchodzenia od izolacji i luzowania obostrzeń, we Francji przewiduje się wprowadzenie nowych technologii w postaci tak zwanych „inteligentnych” kamer i kamer termowizyjnych w celu ułatwienia zarządzania przez podmioty publiczne i prywatne kryzysem zdrowotnym lub jego skutkami. Zdaniem CNIL niektóre z przewidzianych środków nie są zgodne z ramami prawnymi mającymi zastosowanie do ochrony danych osobowych. Francuski organ nadzorczy uważa, że ważne jest pogodzenie celów zdrowotnych i wolności osobistych, jak prawo do prywatności i ochrony danych osobowych. Uchwycenie wizerunku ludzi w przestrzeniach publicznych bezsprzecznie wiąże się z ryzykiem dla ich podstawowych praw i wolności. Rozumiejąc cele przypisane tym nowym urządzeniom, CNIL zauważa, że ich wdrożenie wiązałoby się z systematycznym gromadzeniem i analizą danych dotyczących osób krążących w przestrzeni publicznej lub w miejscach otwartych dla publiczności. Ich niekontrolowany rozwój niesie ze sobą ryzyko uogólnienia poczucia inwigilacji wśród obywateli, stworzenia zjawiska przyzwyczajenia i trywializacji inwazyjnych technologii oraz wygenerowania zwiększonej inwigilacji, mogącej podważyć prawidłowe funkcjonowanie naszego demokratycznego społeczeństwa.

CNIL uważa, że istnieje ryzyko, iż za pomocą kamer termowizyjnych nie uda się zidentyfikować osób zakażonych, ponieważ niektóre z nich nie mają objawów i można je również obejść, przyjmując leki przeciwgorączkowe. Francuski organ dodaje, że prawa osób fizycznych muszą być respektowane i nie mogą być ani ograniczone, ani zawieszone w sytuacji zagrożenia zdrowia. Walka z epidemią COVID-19 skłoniła niektórych graczy do rozważenia zastosowania „inteligentnych” kamer zaprojektowanych w szczególności w celu pomiaru temperatury, wykrywania obecności lub zapewnienia, że dystans społeczny lub noszenie masek jest przestrzegane. Nie kwestionując w żaden sposób zasadności celu, jakim jest walka z rozprzestrzenianiem się epidemii, CNIL uważa za konieczne zwrócenie uwagi na fakt – z zastrzeżeniem analizy poszczególnych przypadków – iż wydaje się, że znaczna część tych urządzeń nie jest zgodna z ramami prawnymi mającymi zastosowanie do ochrony danych osobowych.

Źródło: Tłumaczenie artykułu ze strony WWW francuskiego organu ochrony danych

<https://www.cnil.fr/fr/la-cnil-appelle-la-vigilance-sur-lutilisation-des-cameras-dites-intelligentes-et-des-cameras>

KARY



Finlandia: pierwsze kary za naruszenie danych

Fiński organ ochrony danych nałożył trzy kary administracyjne za naruszenia ochrony danych. Po raz pierwszy rada sankcji nałożyła kary administracyjne za naruszenie przepisów o ochronie danych.

Braki w informacjach przekazywanych w związku z powiadomieniami o zmianie adresu

Osoby, które złożyły skargę do Rzecznika Ochrony Danych, otrzymały komunikaty od różnych firm o powiadomieniu o zmianie adresu do Posti Oy, która jest wiodącym operatorem usług pocztowych w Finlandii. Dochodzenie przeprowadzone przez Urząd Rzecznika Ochrony Danych ujawniło, że Posti nie poinformował osób, których dane dotyczą, o przysługujących im prawach, w tym o prawie do sprzeciwu wobec ujawnienia danych, w związku z powiadomieniami o zmianie adresu.

Firma powinna była wyraźnie poinformować swoich klientów o ich prawie do sprzeciwu wobec przetwarzania ich danych osobowych. Posti przedłożyło takie powiadomienia tylko klientom, którzy zakupili dodatkowe usługi oprócz powiadomienia o zmianie adresu.

Naruszenie dotknęło 161 000 klientów w samym 2019 r. Rada ds. Sankcji nałożyła na Posti Oy grzywnę administracyjną w wysokości 100 000 euro.

Ocena wpływu ochrony danych na przetwarzanie danych dotyczących lokalizacji pracowników została zaniedbana

Druga decyzja dotyczyła skargi jaka wpłynęła do Rzecznika Ochrony Danych na temat sposobu, w jaki podmiot Kymen Vesi Oy przetwarzał dane lokalizacji swoich pracowników poprzez śledzenie pojazdów za pomocą systemu informacji o pojeździe. Administrator

nie dokonał oceny skutków wymaganej przez RODO przed rozpoczęciem przetwarzania danych dotyczących lokalizacji. Dane o lokalizacji wykorzystano między innymi do monitorowania godzin pracowników.

Ocena wpływu na ochronę danych jest wymagana, jeśli przetwarzanie może spowodować wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą. Rada ds. Sankcji nałożyła na Kymen Vesi Oy grzywnę administracyjną w wysokości 16 000 euro.

Dane osobowe osób ubiegających się o pracę zostały zebrane niepotrzebnie

W trzecim przypadku Rzecznik Ochrony Danych został powiadomiony o firmie zbierającej niepotrzebne dane osobowe od osób ubiegających się o pracę i pracowników. Zgodnie z fińską ustawą o ochronie prywatności w życiu zawodowym pracodawca może przetwarzać dane niezbędne tylko w związku ze stosunkiem pracy. Firma prosiła o informacje dotyczące takich kwestii, jak przekonania religijne, stan zdrowia, możliwa ciąża i status rodzinny osób, których dane dotyczą.

Rzecznik ds. Ochrony Danych nakazał firmie usunięcie niepotrzebnych danych. Rada ds. Sankcji nałożyła również na spółkę grzywnę administracyjną w wysokości 12 500 euro.

Źródło: nieoficjalne tłumaczenie informacji ze strony EDPB
https://edpb.europa.eu/news/national-news/2020/finnish-dpa-imposed-three-administrative-fines-data-protection-violations_pl

Link do decyzji:

https://tietosuoja.fi/en/article/-/asset_publisher/tietosuoja/tuutetun-toimiston-seuraamuskollegio-maarsi-kolme-seuraamusmaksua-tietosuojarikkomuksista

Belgia: ukarano kandydata w wyborach lokalnych

Izba procesowa belgijskiego Urzędu Ochrony Danych nałożyła grzywnę w wysokości 5 000 euro na kandydata w wyborach lokalnych za korzystanie z rejestru pracowników gminy w celu wysyłania im listów zawierających propagandę wyborczą. Gmina belgijska złożyła skargę na kandydata.

Izba procesowa ustaliła, że rejestr pracowników nie jest przeznaczony do celów innych niż wewnętrzne zarządzanie gminą, dlatego wysyłanie propagandy wyborczej jest naruszeniem przepisów. Izba procesowa nie mogła znaleźć podstawy prawnej dla zgodnego z prawem przetwarzania danych z rejestru pracowników.

Izba procesowa uważa również, że inne stanowiska pozwanego w służbie publicznej powinny były doprowadzić go do większego poszanowania zasad dotyczących kampanii wyborczej, w tym zasad ochrony danych.

Źródło: nieoficjalne tłumaczenie informacji ze strony EDPB
https://edpb.europa.eu/news/national-news/2020/belgian-data-protection-authority-imposed-fine-5000-eur-local-election_pl

Link do decyzji:

https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Decision_CC_30-2020_FR.pdf

Szwecja: spółdzielnia mieszkaniowa z zakazem stosowania monitoringu wideo przy wejściu do budynku mieszkalnego

Szwedzki Urząd Ochrony Danych (DPA) zbadał wykorzystanie przez spółdzielnię mieszkaniową nadzoru wideo na terenie jej nieruchomości. Szwedzki organ ochrony danych otrzymał skargi, że spółdzielnia mieszkaniowa

monitoruje klatkę schodową w budynku mieszkalnym stowarzyszenia.

Szwedzki organ nadzorczy stwierdził, że zastosowano nie tylko monitoring wideo, ale i nagrywanie dźwięku.

Ponadto szwedzki organ ochrony danych zauważył, że nagrywanie audio stanowi dodatkową ingerencję w sferę prywatną, w szczególności w przypadku nagrywania w budynku mieszkalnym, i że nie ma żadnych okoliczności, które uzasadniałyby taką ingerencję w tym przypadku.

Szwedzki organ ochrony danych stwierdził również, że ukarany podmiot nie poinformował właściwie mieszkańców o nadzorze wideo. Podmiot nie podał informacji o kontrolerze danych, gdzie można uzyskać dalsze szczegółowe informacje oraz o nagrywaniu dźwięku, co jest szczególnie poważnym pominięciem.

Szwedzki Urząd Ochrony Danych nakazał spółdzielni mieszkaniowej zatrzymanie nadzoru wideo klatki schodowej i wejścia, zaprzestanie nagrywania dźwięku z kamery monitorującej przez skrzynkę rozdzielczą i poprawić informacje dotyczące nadzoru wideo. Ponadto nałożył na podmiot grzywnę administracyjną w wysokości 20 000 koron szwedzkich (około 2 000 euro). Przy obliczaniu kwoty grzywny wzięto pod uwagę fakt, że była to mniejsza spółdzielcza spółdzielnia mieszkaniowa.

Źródło: nieoficjalne tłumaczenie informacji ze strony EDPB
https://edpb.europa.eu/news/national-news/2020/co-operative-housing-association-banned-using-video-surveillance-entrance_pl

Link do decyzji:

<https://www.datainspektionen.se/nyheter/bostadsrattsforening-far-inte-kamerabevaka-entre-och-trapphus/>



KONSULTACJE SPOŁECZNE

Projekt wymogów akredytacji podmiotów monitorujących kodeksy postępowania

Do 19 lipca potrwają konsultacje społeczne projektu wymogów akredytacji podmiotów monitorujących kodeksy postępowania prowadzonych przez Prezesa Urzędu.

Zapraszamy zainteresowane podmioty do przesyłania uwag i postulatów do Wydziału Kodeksów i Certyfikacji na adres e-mail: dol@uodo.gov.pl. W tytule prosimy wskazać hasło „Konsultacje wymogów akredytacji”.

Po przeanalizowaniu wszystkich uzyskanych uwag, na podstawie art. 41 ust. 3 RODO, Prezes Urzędu przedłoży projekt Europejskiej Radzie Ochrony Danych z wykorzystaniem mechanizmu spójności przewidzianego w art. 63 RODO.

Przypomnijmy, projekt wymogów akredytacji podmiotów monitorujących kodeksy postępowania został przygotowany na podstawie art. 41 ogólnego rozporządzenia o ochronie danych (RODO), przy uwzględnieniu art. 29 ustawy o ochronie danych osobowych oraz wytycznych Europejskiej Rady Ochrony Danych nr 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679.

Szczegółowe informacje o kodeksach są dostępne pod adresem: <https://uodo.gov.pl/pl/426>.

KODEKS POSTĘPOWANIA DLA JEDNOSTEK OŚWIATOWYCH

Przypominamy o trwających konsultacjach projektu kodeksu postępowania dla oświaty. Zachęcamy, aby wziąć w nich udział i wypowiedzieć się w tej sprawie!



Wszystkie podmioty zainteresowane stosowaniem RODO w jednostkach oświatowych mogą wziąć udział w konsultacjach, które trwają od 1 czerwca do 30 września 2020 r.

Aktualna treść projektu kodeksu jest dostępna na stronie internetowej: <http://rodo-w-oswiacie.pl/kodeks-postepowania-calosc/>

Prezes UODO zachęca do tworzenia kodeksów branżowych (art. 40 ust. 1 RODO) i wspiera ich autorów. Jednak organ nadzorczy nie uczestniczy w procesie

konsultacji. Dlatego też prosimy o nieprzesyłanie uwag do UODO, tylko bezpośrednio do autora projektu kodeksu.

Zachęcamy wszystkie zainteresowane osoby oraz podmioty do przekazywania autorowi wszelkich uwag oraz sugestii do treści projektu kodeksu bezpośrednio na adres e-mail: kontakt@rodo-w-oswiacie.pl lub za pośrednictwem formularza kontaktowego, znajdującego się na stronie internetowej autora projektu kodeksu: <http://rodo-w-oswiacie.pl/kontakt/>



PROJEKT KODEKSU POSTĘPOWANIA DLA FOTOGRAFÓW

Trwają konsultacje projektu kodeksu postępowania dla fotografów. Projekt kodeksu został skierowany przez autora do konsultacji, a te trwają od 1 lipca do 31 sierpnia 2020 r.

Wszystkie podmioty zainteresowane stosowaniem ogólnego rozporządzenia o ochronie danych (RODO) w branży fotograficznej mogą wziąć udział w konsultacjach projektu kodeksu postępowania w tym sektorze. Treść projektu kodeksu oraz więcej informacji na jego temat są dostępne na stronie internetowej:

<https://bezpiecnywizerunek.pl/>

Zachęcamy do przekazywania autorowi wszelkich uwag oraz sugestii do treści projektu kodeksu, bezpośrednio na adres e-mail: rodo@soinlaw.com lub za pośrednictwem formularza kontaktowego, znajdującego się na stronie internetowej: <https://bezpiecnywizerunek.pl/>.

Prosimy o przesyłanie uwag bezpośrednio do autora projektu kodeksu.

NOWE ODPOWIEDZI NA PYTANIA INSPEKTORÓW

Znajdująca się na naszej stronie internetowej zakładka „Inspektor Ochrony Danych” w sekcji „Zadania IOD” została wzbogacona o kolejne zagadnienia.



Wyjaśnienia dotyczą takich kwestii, jak:

Czy z laboratorium należy zawrzeć umowę powierzenia?

Czy wojewoda może utworzyć bazę wyników badań w kierunku wirusa SARS-CoV-2?

Co z obowiązkiem informacyjnym wobec członków zarządu osób prawnych?

Czy lekarzom należy nadawać upoważnienia?

Drodzy Inspektorzy Ochrony Danych!

Dziękujemy za Waszą aktywność i przesłane oceny Newslettera UODO.

Otrzymaliśmy prawie 950 odpowiedzi na ankietę ewaluacyjną!