Obserwuj nas na:

Nr 2/2021 (23)
Luty 2021

URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

JAK DOKUMENTOWAĆ WPŁYW COVID-19 NA TERMINOWĄ REALIZACJĘ ZAMÓWIENIA PUBLICZNEGO?

Artykuł 15r ust. 1 ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 nie uprawnia pracodawcy do pozyskiwania danych o stanie zdrowia pracownika celem ich przekazywania zamawiającemu w ramach realizacji zamówienia publicznego. Na tej podstawie także zamawiający nie ma prawa do pozyskiwania i przetwarzania tego rodzaju danych osobowych.

W celu ochrony płynności finansowej podmiotów działających na rynku zamówień publicznych w ustawie z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 wprowadzono mechanizmy przewidujące zmianę postanowień umowy w sprawie zamówienia publicznego, jeżeli okoliczności związane z COVID-19 miały wpływ na jej należyte wykonanie. Zgodnie z art. 15r wymienionej ustawy, strony umowy w sprawie zamówienia publicznego, w rozumieniu ustawy Prawo zamówień publicznych, niezwłocznie, wzajemnie informują się o wpływie okoliczności związanych z wystąpieniem COVID-19 na należyte wykonanie tej umowy, o ile taki wpływ wystąpił lub może wystąpić. Strony umowy potwierdzają ten wpływ, dołączając do informacji, o której mowa w zdaniu poprzednim, oświadczenia lub dokumenty, które mogą dotyczyć m.in. nieobecności pracowników lub osób świadczących pracę za wynagrodzeniem na innej podstawie niż stosunek pracy, które uczestniczą lub mogłyby uczestniczyć w realizacji zamówienia.

Wniosek Rzecznika Małych i Średnich Przedsiębiorców o interpretację przepisów

Rzecznik Małych i Średnich Przedsiębiorców zasygnalizował Prezesowi UODO, że zdarzają się sytuacje, w których zamawiający uzależniają uznanie wpływu COVID-19 na należyte wykonanie zamówienia publicznego od przekazania im pełnych informacji na temat stanu zdrowia pracowników oraz pracowników podwykonawców, wraz z niezanonimizowaną dokumentacją (decyzje, polecenia) potwierdzającą przebywanie danych osób na zwolnieniach lekarskich lub kwarantannie. Jednocześnie poprosił o wskazanie, czy przedsiębiorca będący stroną umowy o udzielenie zamówienia publicznego w rozumieniu ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych jest uprawniony do przekazywania danych osobowych, o których mowa w art. 9 ust. 1 RODO, dotyczących jego pracowników oraz podwykonawców swoim kontrahentom na podstawie art. 15r ust. 1 ustawy o COVID-19.

Brak podstaw prawnych

W odpowiedzi Prezes UODO wskazał, że w jego ocenie, art. 15r ust. 1 ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 nie stanowi podstawy prawnej dla pracodawcy do pozyskiwania danych o stanie zdrowia pracownika na potrzeby ich przekazywania zamawiającemu w ramach realizacji zamówienia publicznego. Nie ma przy tym znaczenia, czy kontrahent ten jest podmiotem publicznym czy prywatnym.

Powołany przepis nie daje także zamawiającemu podstaw do pozyskiwania i przetwarzania tego rodzaju danych osobowych.

Właściwa analiza

Dla dokonania oceny, czy art. 15r ust. 1 powołanej ustawy może stanowić podstawę przetwarzania danych osobowych o stanie zdrowia pracownika, w pierwszej kolejności należy przeanalizować, czy w aktualnie obowiązujących przepisach znajdują się podstawy do gromadzenia takich informacji, a następnie ocenić, czy takie dane mogą być udostępnione na podstawie wskazanej regulacji związanej z realizacją zamówienia publicznego. Przyjęcie takiego rozwiązania jest o tyle

istotne, że przepisy szczególne dotyczące przetwarzania danych o stanie zdrowia pracowników w sposób restrykcyjny regulują pozyskiwanie tych danych przez pracodawcę i co do zasady nie uprawniają go do ich przetwarzania.

Dane pod szczególną ochroną

Pozyskiwanie i wykorzystywanie przez przedsiębiorcę (pracodawcę) dokumentacji potwierdzającej przebywanie pracownika na zwolnieniach lekarskich lub kwarantannie oznacza przetwarzanie informacji o jego stanie zdrowia, a więc szczególnej kategorii danych, o których mowa w art. 9 ust. 1 RODO i które – ze względu na swój sensytywny charakter – powinny zostać objęte szczególną ochroną.

Ogólne rozporządzenie o ochronie danych co do zasady stanowi o zakazie przetwarzania szczególnych kategorii danych (art. 9 ust. 1). Pracodawca, chcąc jednak przetwarzać dane o stanie zdrowia jego pracownika, musi wykazać się jedną z przesłanek określonych w art. 9 ust. 2 RODO dopuszczających przetwarzanie tej kategorii danych. Natomiast przesłanki te odwołują się dodatkowo do odpowiednich gwarancji, co oznacza, że przetwarzanie szczególnych kategorii danych osobowych jest dopuszczalne wyłącznie w ściśle określonych okolicznościach.

Zgodnie z art. 221b Kodeksu pracy, dane szczególnych kategorii mogą być przetwarzane za zgodą osoby ubiegającej się o zatrudnienie bądź pracownika wyłącznie, gdy ich przekazanie następuje z inicjatywy tych osób (§ 1), a także wtedy, gdy podanie takich danych jest niezbędne ze względu na kontrolę dostępu do szczególnie ważnych informacji, których ujawnienie może narazić pracodawcę na szkodę, lub dostępu do pomieszczeń wymagających szczególnej ochrony (§ 2). Ponadto do przetwarzania takich danych osobowych mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania takich danych wydane przez pracodawcę (§ 3). Pracodawca zatem, zgodnie z zasadą rozliczalności, nie byłby w stanie wykazać, dlaczego pozyskuje i przekazuje innym podmiotom (kontrahentom) dane o stanie zdrowia pracownika dla celów związanych z realizacją zamówienia publicznego.

Wskazane wyżej argumenty, w ocenie Prezesa UODO, przemawiają za tym, że art. 15r ust. 1 ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 nie może stanowić podstawy prawnej dla przetwarzania przez pracodawcę innych danych o pracowniku (danych o stanie zdrowia) i w warunkach innych niż wynikające wprost z przepisów prawa pracy.

Rozwiązania przyjmowane i stosowane przez m.in. przedsiębiorców i pracodawców nie będą sprzeczne z przepisami o ochronie danych osobowych, jeżeli administrator będzie realizował je zgodnie z zasadami, o których mowa w art. 5 RODO, w szczególności z zasadą legalności oraz minimalizacji danych.

OZNACZANIE PACJENTÓW SZPITALA DZIECIĘCEGO

Przepisy szczególne precyzyjnie regulują, w jaki sposób oznacza się pacjentów w znaki identyfikacyjne, w tym jakie dane osobowe są w nich zawarte. W przypadku dzieci dopuszczalne może być umieszczanie na opasce identyfikacyjnej imienia i nazwiska dziecka, o ile dochodziłoby do tego za zgodą i przede wszystkim z inicjatywy jego rodziców lub opiekunów.

Kwestię związaną z identyfikacją pacjentów podmiotów leczniczych regulują przepisy sektorowe, tj. ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej, oraz akty wykonawcze do niej, w tym rozporządzenie Ministra Zdrowia z dnia 20 września 2012 r. w sprawie warunków, sposobu i trybu zaopatrywania pacjentów szpitala w znaki identyfikacyjne oraz sposobu postępowania w razie stwierdzenia ich braku.

To one wskazują (art. 36 ust. 3 i ust. 5 ustawy), że pacjentów szpitala zaopatruje się w znaki identyfikacyjne, a znak identyfikacyjny zawiera informacje pozwalające na ustalenie: imienia i nazwiska oraz daty urodzenia pacjenta, a w przypadku noworodka urodzonego w szpitalu - imienia i nazwiska matki, płci i daty urodzenia dziecka ze wskazaniem roku, miesiąca, dnia oraz godziny i minuty w systemie 24-godzinnym,

a w przypadku noworodka urodzonego z ciąży mnogiej także cyfry wskazujące na kolejność rodzenia się - zapisane w sposób uniemożliwiający identyfikację pacjenta przez osoby nieuprawnione. Z kolei przepisy powołanego rozporządzenia (§ 3) wskazują, że znak identyfikacyjny umieszcza się na opasce, a także na zdjęciu - w przypadku, o którym mowa w § 5 ust. 1, tj. wówczas, gdy założenie opaski dziecku, które nie ukończyło szóstego roku życia, w sposób określony w § 4 ust. 1 nie jest możliwe. Wtedy wykonuje się i umieszcza w widocznym miejscu na łóżku dziecka albo na inkubatorze, za zgodą matki lub osoby bliskiej, o której mowa w § 2 ust. 2, zdjęcie dziecka, na którym umieszcza się znak identyfikacyjny. Ponadto znak identyfikacyjny umieszcza się w indywidualnej dokumentacji medycznej pacjenta.

Ponieważ to przepisy prawa krajowego precyzyjnie regulują, w jaki sposób oznacza się pacjentów w znaki identyfikacyjne, w tym jakie dane osobowe są w tych znakach zawarte, to uznać należy, że podstawą legalizującą przetwarzanie tych danych jest art. 6 ust. 1 lit. c) RODO. Stanowi on, że przetwarzanie danych osobowych jest zgodne z prawem, gdy jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.

Jednak w opinii Prezesa UODO, ponieważ w przypadku oznaczana pacjentów szpitala dziecięcego pod uwagę należy brać również kwestie dotyczące bezpieczeństwa hospitalizowanych dzieci, uznać należy, że prawidłowa ich identyfikacja może mieć istotny wpływ na ich zdrowie i życie. Gdyby więc przetwarzanie na opasce – oprócz znaków identyfikacyjnych – dodatkowo również imienia i nazwiska dziecka odbywało się na zgodą i przede wszystkim z inicjatywy rodziców/opiekunów dziecka, można rozważyć dopuszczalność stosowania takiego rozwiązania. Należy jednak podkreślić, że administrator (podmiot leczniczy) nie ma podstaw prawnych, aby narzucać stosowanie powyższych rozwiązań pacjentom i ich rodzicom/opiekunom prawnym, ponieważ obowiązujące przepisy wyraźnie wskazują sposób, w jaki ma on obowiązek oznaczyć pacjentów – nawet bez zgody rodziców/opiekunów prawnych dzieci.

POZYSKIWANIE NUMERU PESEL NA POTRZEBY PROWADZENIA EGZEKUCJI ADMINISTRACYJNEJ

Dopiero na etapie prowadzonego postępowania egzekucyjnego uzasadnione jest przetwarzanie numeru PESEL strony postępowania.

W ostatnim czasie przedmiotem analizy organu ds. ochrony danych osobowych była sygnalizowana mu wątpliwość związana z tym, czy na etapie składania wniosków o wydanie zezwolenia na zajęcie pasa drogowego możliwe jest pozyskiwanie numeru PESEL w celu wykorzystania go na potrzeby ewentualnego postępowania egzekucyjnego.

W odpowiedzi Prezes UODO wskazał, że rozporządzenie Rady Ministrów z dnia 1 czerwca 2004 r. w sprawie określenia warunków udzielania zezwoleń na zajęcie pasa drogowego enumeratywnie wskazuje (§ 1 ust. 2), jakie dane powinien zawierać wniosek o wydanie zezwolenia na zajęcie pasa drogowego.

Są to:
1. imię i nazwisko oraz adres lub nazwa i siedziba podmiotu występującego o zajęcie pasa drogowego;
2. cel zajęcia pasa drogowego;
3. lokalizacja i powierzchnia zajętego pasa drogowego, a w przypadku reklam powierzchnia reklamy;
4. planowany okres zajęcia pasa drogowego.

Powołane przepisy nie uprawniają zatem do pozyskiwania numeru PESEL/NIP podmiotu składającego taki wniosek. Gdyby na tym etapie wymagano podania takich danych, dochodziłoby do naruszenia przepisów RODO, które stanowią, że przetwarzanie (w tym pozyskiwanie) danych osobowych musi odbywać się zgodnie

z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (art. 5 ust. 1 lit. a), zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (art. 5 ust. 1 lit. b) oraz adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (art. 5 ust. 1 lit. c).

Co istotne, numer PESEL to krajowy numer identyfikacyjny, który powinien podlegać szczególnej ochronie (zgodnie z art. 87 RODO). Jego przetwarzanie jest dozwolone, jeśli wynika to wprost z przepisów prawa. Jednocześnie pozyskiwanie danych na zapas, na wszelki wypadek, jak np. na potrzeby ewentualnego postępowania egzekucyjnego, które jest odrębnym postępowaniem, jeszcze nie zaistniałym w momencie prowadzenia postępowania administracyjnego dotyczącego wydania zezwolenia na zajęcie pasa drogowego, jest działaniem nadmiarowym, naruszającym zasadę legalizmu (art. 5 ust. 1 lit. a RODO) zasadę ograniczenia celu (art. 5 ust. 1 lit. b RODO) oraz zasadę minimalizacji danych (art. 5 ust. 1 lit. c RODO).

Ponadto ustawodawca w sytuacji, gdy uznaje konieczność podania numeru PESEL, ustanawia przepisy, które wprost nakładają obowiązek jego podania. W takim przypadku wypełniona zostaje przesłanka z art. 6 ust. 1 lit. c RODO, gdzie przetwarzanie tej danej jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.

Konieczność zamieszczenia numeru PESEL została uregulowana w art. 27 § 1 pkt 2 ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji, który stanowi, że to tytuł wykonawczy ma zawierać numer PESEL. Zatem dopiero na etapie prowadzonego postępowania egzekucyjnego uzasadnione jest przetwarzanie numeru PESEL strony postępowania.

WIZERUNEK PROTOKOLANTA W TRANSMISJI I NA NAGRANIACH OBRAD RADY GMINY

Upublicznienie wizerunku osoby protokółującej obrady rady gminy zarówno podczas transmisji, jak i na utrwalonym nagraniu posiedzenia jest zgodne z prawem i nie wymaga jej zgody.

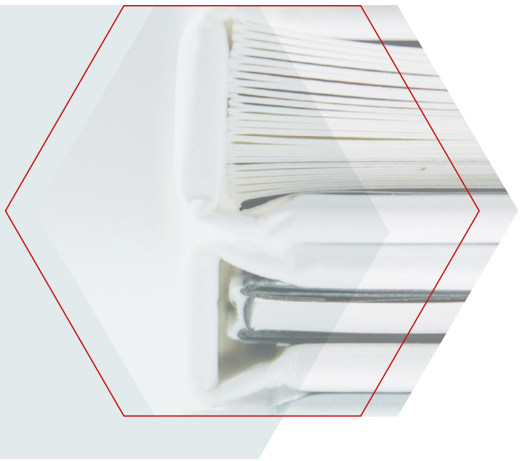
W opinii Prezesa UODO, obowiązek prowadzenia transmisji obrad rady gminy oraz ich utrwalania za pomocą urządzeń rejestrujących obraz i dźwięk (wprowadzony w art. 20 ust. 1b zdanie pierwsze ustawy z dnia 8 marca 1990 r. o samorządzie gminnym) stanowi jeden z przejawów zasady jawności i dostępności posiedzeń kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów (o której mowa w art. 18 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej). Tym samym upublicznienie w Biuletynie Informacji Publicznej i na stronie internetowej gminy oraz w inny sposób zwyczajowo przyjęty (o czym mowa w art. 20 ust. 1b zdanie drugie ustawy z dnia 8 marca 1990 r. o samorządzie gminnym) wizerunków osób obecnych na posiedzeniu rady gminy (a przez to przetwarzanie tej ich danej osobowej) odbywa się na podstawie przesłanki niezbędności takiego działania do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (o której mowa w art. 6 ust. 1 lit. e RODO) w związku z realizacją zasady dostępu do informacji publicznej. Nie wymaga zatem uzyskiwania zgody osób uczestniczących w obradach rady gminy.

Tak jest również w przypadku pracownika, którego obowiązkiem jest protokołowanie obrad rady gminy. Upublicznienie jego wizerunku w sposób wskazany w art. 20 ust. 1b ustawy o samorządzie gminnym w ramach transmisji i na utrwalonym nagraniu posiedzenia rady gminy jest zgodne z prawem i nie wymaga zgody tej osoby.

Warto przy tym zaznaczyć, że nie oznacza to jednocześnie bezterminowego ich przetwarzania w BIP, na stronie internetowej gminy czy w innym miejscu, w którym zwyczajowo udostępniane są nagrania z obrad rady gminy.

Jak wskazano w dostępnym na stronie internetowej Urzędu Ochrony Danych Osobowych materiale „Projektowanie ochrony danych osobowych w związku z transmisją i nagrywaniem obrad kolegialnych organów jednostek samorządu terytorialnego" obowiązkiem administratora jest dokonywanie analizy okresu przetwarzania danych zawartych w nagraniach zamieszczonych w Internecie.

„Zapewnienie przez administratora retencji danych osobowych zawartych w upublicznianych nagraniach wiąże się ze stałą ich analizą i przeglądem pod kątem oceny ich niezbędności do celów, dla których są przetwarzane. Jeżeli ustawodawca określił w aktach prawnych okres, po którym dane mają być usuwane, to administrator musi przestrzegać tych terminów. Jeśli jednak w przepisach brak jest szczegółowych |regulacji w tym zakresie, administrator ma obowiązek samodzielnie określić okres retencji danych, stosując się do wynikającej z RODO zasady ograniczenia przechowywania" – czytamy w powołanym materiale, w którym dostępnych jest więcej szczegółowych informacji dotyczących zasad prowadzenia nagrań i transmisji z posiedzeń kolegialnych organów jednostek samorządu terytorialnego.



DWA PROJEKTY KODEKSÓW POSTĘPOWANIA DLA PODMIOTÓW Z SEKTORA OCHRONY ZDROWIA Z POZYTYWNĄ OPINIĄ PREZESA UODO

Prezes UODO pozytywnie zaopiniował projekt „Kodeksu postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych" opracowany przez Federację Związków Pracodawców Ochrony Zdrowia „Porozumienie Zielonogórskie" oraz projekt „Kodeksu postępowania dla sektora ochrony zdrowia" opracowany przez Polską Federację Szpitali. W obu przypadkach niezbędne jest jednak doprecyzowanie kwestii związanych z podmiotami monitorującymi przestrzeganie tych regulacji.

Opinie wydane na podstawie art. 40 ust. 5 RODO wskazują, że w obu przypadkach treść merytoryczna – dotycząca przede wszystkim operacji przetwarzania danych – jest zgodna z RODO i stanowi odpowiednie zabezpieczenia w zakresie ochrony danych.

Kodeksy zostaną zatwierdzone decyzją Prezesa Urzędu po wydaniu certyfikatu akredytacyjnego dla podmiotów monitorujących ich postanowienia. Wskazanie w kodeksie postępowania akredytowanego podmiotu, który ma kontrolować jego przestrzeganie, jest bowiem warunkiem koniecznym do zatwierdzenia tego dokumentu.

W celu uzyskania akredytacji podmioty, które chcą zostać podmiotami monitorującymi, muszą wystąpić do Prezesa UODO. Wymogi akredytacji są dostępne na stronie internetowej Urzędu pod adresem: https://uodo.gov.pl/pl/138/1861.

Na stronie internetowej UODO można zapoznać się z nagraniem ze zorganizowanego 15.02.2021 r. webinarium o wymogach akredytacji podmiotów monitorujących przestrzeganie kodeksów postępowania.

Film z webinarium dostępny jest pod linkiem: https://uodo.gov.pl/pl/138/1946

Szczegółowe informacje dotyczące zaopiniowanych projektów kodeksów postępowania, w tym wydane opinie, są dostępne na stronie internetowej UODO pod linkiem: https://uodo.gov.pl/pl/138/1923

PRZECHOWYWANIE DOKUMENTACJI UCZESTNIKÓW WARSZTATÓW TERAPII ZAJĘCIOWEJ

Jeśli przepisy szczególne nie określają okresu retencji danych, to zastosowanie znajdują przepisy RODO, w tym zasada ograniczenia przechowywania danych. Stanowi ona, że dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy, niż jest to niezbędne do osiągnięcia celów, dla których je pozyskano.

Podmioty prowadzące warsztaty terapii zajęciowej (WTZ) sygnalizują, że przepisy regulujące ich działalność, tj. ustawa z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych oraz rozporządzenie ministra gospodarki, pracy i polityki społecznej z dnia 25 marca 2004 r. w sprawie warsztatów terapii zajęciowej, nie wskazują, jak długo mają one przechowywać dokumentację dotyczącą uczestników i byłych uczestników warsztatów. W efekcie, licząc się m.in. z możliwością kontroli ze strony PCPR czy NIK, przez lata gromadzą i przechowują bardzo dużo takich dokumentów, tym samym przetwarzają wiele danych osobowych. Zastanawiają się, jak długo mogą to robić.

W opinii UODO, w zakresie nieuregulowanym w przepisach szczególnych zastosowanie mają ogólne zasady przetwarzania danych osobowych określone w RODO, w tym w art. 5 ust. 1, takie jak legalność, minimalizacja danych, ograniczenie celu, prawidłowość, ograniczenie przechowywania, rzetelność, przejrzystość, integralność i poufność. Warto pamiętać, że zgodnie z zasadą ograniczenia przechowywania danych, o której mowa w art. 5 ust. 1 lit. e RODO, dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

Jednocześnie uznając konieczność ujednolicenia stosowanych praktyk związanych z retencją danych zawartych w dokumentacji z warsztatów, organ nadzorczy, na podstawie art. 52 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych zwrócił się do ministra rodziny, pracy i polityki społecznej o rozważenie wprowadzenia jasnych standardów prawnych w tym obszarze.

EDUKCJA

Urząd Ochrony Danych Osobowych na zaproszenie Mazowieckiego Kuratora Oświaty przystąpił do współpracy w ramach programu „Reaguj i wspieraj. Koalicja na rzecz tworzenia bezpiecznego środowiska nauczania na odległość".

Już po raz kolejny mamy okazję do współpracy na rzecz zapewnienia bezpieczeństwa uczniów oraz budowania kultury ochrony danych osobowych wśród rodziców oraz nauczycieli. Zgodnie z założeniami programu, został zaplanowany cykl webinariów przeznaczonych dla rodziców oraz kadry pedagogicznej szkół i placówek, które będą stanowiły źródło rzetelnej wiedzy, a także odpowiedzi na wiele ważnych pytań związanych z organizacją bezpiecznego procesu zdalnej edukacji.

W ramach udziału w programie przedstawiciele Urzędu omówią temat „Bezpieczeństwo danych osobowych w okresie kształcenia na odległość”, oraz przybliżą działania edukacyjne UODO skierowane do nauczycieli i dzieci. Wsparciem dla tego zadania jest program edukacyjny „Twoje Dane- Twoja Sprawa”. Transmisję wykładu zaplanowano na 11 marca 2021 roku. Przekaz skierowany będzie do kadry pedagogicznej.

Szczegółowe informacje na temat realizowanego przedsięwzięcia zostały udostępnione na stronie kuratorium:

https://www.kuratorium.waw.pl/pl/informacje/aktualnosci/15413,Program-Reaguj-i-wspieraj-Koalicja-na-rzecz-tworzenia-bezpiecznego-srodowiska-na.html

KARY

Belgia: 50 tys. euro za handel danymi

Belgijski organ ochrony danych osobowych (APD) nałożył na przedsiębiorstwo Family Service, które rozprowadza „różowe pudełka”, karę pieniężną w wysokości 50 tys. euro – za naruszenie przepisów RODO, w tym brak przejrzystości wobec swoich klientów w zakresie działalności związanej z handlem danymi osobowymi. Firma udostępniła dane ponad miliona klientów i ich dzieci partnerom biznesowym bez ich ważnej zgody.

APD wszczęła dochodzenie po otrzymaniu skargi na Family Service, firmę marketingową, która oferuje przyszłym matkom „różowe pudełka” – zawierają one próbki, oferty specjalne i arkusze informacyjne. Skarga dotyczyła w szczególności przekazywania danych osobowych organizacjom będącym stronami trzecimi bez ważnej zgody klienta i bez dostarczenia wystarczających informacji.

Postępowanie wykazało, że firma wypożyczała i/lub sprzedawała dane osobowe w celach komercyjnych. Praktyki te nie były jednak jasno i zrozumiale wskazane w komunikacji z klientami. „Różowe pudełka” były rozprowadzane za pośrednictwem ginekologów i szpitali, co mogło wywołać u klientów przekonanie, że inicjatywa pochodzi z sektora publicznego, a nie od prywatnego przedsiębiorstwa, którego podstawową działalnością jest handel danymi.

Pozyskane dane klientów były przekazywane nie tylko firmom oferującym usługi związane z małymi dziećmi, ale także innym partnerom, takim jak dostawcy danych.

Brak powiadomienia osób, których dane dotyczą, spowodował konkretne dla nich ryzyko utraty kontroli nad swoimi danymi. Ich dane były przetwarzane przez organizacje zewnętrzne, których nie znali, w celach, które nie zostały im przedstawione.

Ponadto APD przypomniała, że zgoda, aby mogła być uznana za ważną w rozumieniu RODO, musi spełniać określone warunki. Oprócz poinformowania, zgoda musi być wyrażona dobrowolnie, tj. osoba, której dane dotyczą, musi mieć rzeczywisty wybór co do tego, czy chce wyrazić zgodę na przetwarzanie swoich danych, czy też nie. Zgoda nie może być zatem uznana za dobrowolną, jeżeli jej brak oznacza utratę korzyści związanych z otrzymaniem „różowego pudełka” (takich jak np. oferowane w nim arkusze informacyjne).

Zgoda musi być konkretna. Osoba, której dane dotyczą, musi wyrazić zgodę w określonym celu. Jeżeli organizacja ubiega się o zgodę klienta na więcej niż jeden cel, klient musi mieć możliwość wyrażenia lub niewyrażenia zgody na każdy cel osobno. Jednakże w tej sprawie APD stwierdziło, że zgoda klienta na otrzymanie korzyści wynikających z „różowego pudełka” automatycznie oznaczała w tym przypadku zgodę na przekazywanie danych.

Źródło: https://autoriteprotectiondonnees.be/citoyen/commerce-de-donnees-personnelles-lapd-sanctionne-loffre-des-boites-roses

Norweski organ ds. ochrony danych nakłada karę na Coop Finnmark

Norweski organ nadzorczy nałożył karę w wysokości 40 tys. euro na spółkę Coop Finnmark SA. Sprawa dotyczy niezgodnego z prawem rozpowszechniania nagrania z kamery sklepu.

Kierownik sklepu nagrał swoim telefonem zapis monitoringu i go rozpowszechnił. Przedsiębiorstwo Coop Finnmark AS poinformowało o tej sprawie, dokonując zgłoszenia naruszenia ochrony danych osobowych 10 kwietnia 2019 r do organu nadzorczego.

Każde przetwarzanie danych osobowych wymaga podstawy prawnej, żeby było ono uznane za zgodne z prawem. W tej sprawie ukarane przedsiębiorstwo takiej podstawy prawnej do rozpowszechniania przez kierownika sklepu nagrań z monitoringu nie miało.

Organ ochrony danych uważa, że sprawa ta jest na tyle poważna, że kara jest odpowiednim środkiem naprawczym. Organ wziął pod uwagę fakt, że nagranie z kamery pokazywało dzieci, a jego rozpowszechnianie mogło potencjalnie skutkować poważnym zagrożeniem dla ich prywatności.

Źródło: https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-issues-fine-coop-finnmark_pl

Norwegia: kara za przekazywanie wiadomości e-mail

Norweski organ ochrony danych ukarał organizację karą pieniężną w wysokości 40 tys. euro za niezgodne z prawem skonfigurowanie automatycznego przekazywania maili pracowników.

Podstawą sprawy jest skarga pracownika, który odkrył, że jego pracodawca uruchomił automatyczne przekazywanie maili ze skrzynki odbiorczej pracownika. Czynność ta została uruchomiona w związku z nieobecnością pracownika z powodu choroby i pozostała aktywne dłużej niż miesiąc. Po zbadaniu sprawy organ ochrony danych osobowych uznał, że przekazywanie danych odbyło się z naruszeniem krajowych przepisów dotyczących dostępu pracodawcy do skrzynek poczty elektronicznej i innych elektronicznych informacji, a także RODO.
Nazwa organizacji nie została podana do wiadomości publicznej, aby chronić tożsamość skarżącego. Organizacja odwołała się od tej decyzji.

Źródło: https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-issues-fine-forwarding-e-mail_pl

NOWE PYTANIA W ZAKŁADCE IOD

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 pracownik działu kadr urzędu gminy może przetwarzać dane kierowników jednostek organizacyjnych?

Jaki jest status komisji antymobbingowej?

Czy inspektorowi ochrony danych należy nadawać upoważnienie do przetwarzania danych?

Czy GUS może zobowiązać gminy do przekazania mu innych danych niż te, które gmina może gromadzić?