Nr 2/2023 (46)
Luty 2023

URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

Zamieszczone w „Newsletter UODO dla IOD" publikacje nie stanowią oficjalnego stanowiska UODO.

PODSTAWA POZYSKIWANIA SZCZEGÓLNYCH KATEGORII DANYCH OSOBOWYCH OBYWATELI UKRAINY

Resort spraw wewnętrznych podzielił opinię UODO, iż to z przepisów rangi ustawy powinno wynikać uprawnienie do pozyskiwania szczególnych kategorii danych osobowych obywateli Ukrainy przez podmioty decydujące o przedłużeniu okresu przyznania świadczenia pieniężnego przysługującego z tytułu zapewnienia tym osobom zakwaterowania i wyżywienia. Jednocześnie zadeklarował wprowadzenie stosownej zmiany przy okazji najbliższych prac legislacyjnych w tym zakresie.

Od administratorów oraz inspektorów ochrony danych (IOD) z ośrodków pomocy społecznej i gmin, Urząd Ochrony Danych Osobowych otrzymywał liczne sygnały dotyczące problemów ze stosowaniem przepisów ustawy z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa oraz wydanych na jej podstawie aktów wykonawczych. Ich wątpliwości budzi bowiem podstawa prawna pozyskiwania danych osobowych szczególnych kategorii (np. informacji o niepełnosprawności) przez podmiot, który decyduje o przedłużeniu okresu przyznania świadczenia pieniężnego przysługującego z tytułu zapewnienia zakwaterowania i wyżywienia obywatelom Ukrainy. Organ nadzorczy, podzielając te opinie, zwrócił się więc do Ministra Spraw Wewnętrznych i Administracji z wnioskiem o zmianę obowiązujących przepisów.

Wskazał, że kwestie dotyczące przyznawania świadczenia pieniężnego przysługującego każdemu podmiotowi, który zapewni, na własny koszt, zakwaterowanie i wyżywienie obywatelom Ukrainy, zostały uregulowane w ustawie.

Natomiast warunki przedłużenia przyznania tego świadczenia określone zostały w rozporządzeniu Rady Ministrów z dnia 4 maja 2022 r. w sprawie maksymalnej wysokości świadczenia pieniężnego przysługującego z tytułu zapewnienia zakwaterowania i wyżywienia obywatelom Ukrainy oraz warunków przyznawania tego świadczenia i przedłużania jego wypłaty.

Zgodnie z jego § 4 ust. 1, gmina może przedłużyć okres wypłaty wymienionego świadczenia w przypadku zapewnienia zakwaterowania i wyżywienia obywatelowi Ukrainy, który spełnia jedno z określonych w tym przepisie kryteriów, np., posiada orzeczenie o niepełnosprawności lub stopniu niepełnosprawności lub orzeczenie, o którym mowa w art. 5 ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej

i społecznej oraz zatrudnianiu osób niepełnosprawnych; posiada dokument potwierdzający I lub II stopień niepełnosprawności wydany w ramach ukraińskiego systemu orzekania o niepełnosprawności lub też jest kobietą w ciąży lub osobą wychowującą dziecko do 12 miesiąca życia.

Jednocześnie przepisy te nie wskazują, w jaki sposób gminy mogą weryfikować oświadczenia składane przez wnioskodawców w zakresie spełnienia kryteriów do wydłużenia terminu wypłaty świadczeń.

Organ nadzorczy podniósł, że zgodnie z zasadą legalności określoną w art. 5 ust. 1 lit. a RODO, podmiot może przetwarzać dane osobowe wyłącznie wtedy, gdy istnieje uprawniająca go do tego podstawa.

Przy czym warunki dla przetwarzania danych szczególnych kategorii są bardziej restrykcyjne, co wynika z art. 9 ust. 1 RODO kształtującego generalny zakaz ich przetwarzania i art. 9 ust. 2, który określa odstępstwa od tego zakazu. Ma to istotne znaczenie w sytuacji przetwarzania danych osobowych przez podmioty publiczne, które jako administratorzy nie mogą pozyskiwać więcej danych niż wynika wprost z przepisów prawa i w zakresie adekwatnym do realizowanych na podstawie ustawy celów.

Zatem, aby taki podmiot mógł legalnie przetwarzać szczególne kategorie danych osobowych, takie uprawnienie musi wynikać z przepisu prawa w randze ustawy zawierającego określone gwarancje praw podstawowych i interesów osoby, której dane dotyczą (art. 9 ust. 2 lit. b RODO).

W związku z tym, UODO zwrócił się do Ministra Spraw Wewnętrznych i Administracji o przeanalizowanie obowiązujących regulacji pod kątem dokonania w nich stosownych zmian tak, aby nakładanie obowiązku przekazywania szczególnych kategorii danych osobowych wynikało z przepisów rangi ustawy przewidujących stosowne gwarancje dla osób, których dane te dotyczą.

W odpowiedzi resort wyraził gotowość uzupełnienia lub korekty przepisów wymienionej ustawy przy okazji najbliższych prac legislacyjnych.

POJAZDY KOMUNIKACJI MIEJSKIEJ BEZ MONITORINGU FONICZNEGO

Pracodawca w celu zapewnienia bezpieczeństwa pracowników lub ochrony mienia może zainstalować monitoring, ale powinien on umożliwiać jedynie rejestrację obrazu, a nie dźwięku. Nie ma więc podstaw prawnych, by w kabinie kierowcy w pojazdach komunikacji miejskiej montowane były kamery umożliwiające rejestrację dźwięku.

Przetwarzanie danych osobowych na potrzeby zatrudnienia podlega szczególnym zasadom ze względu na nierówność stron stosunku pracy. Dlatego prawodawca unijny upoważnił (art. 88 RODO) państwa członkowskie do przyjęcia bardziej szczegółowych przepisów mających zapewnić ochronę praw i wolności pracowników w związku z przetwarzaniem ich danych osobowych przez pracodawców.
Wyrazem dostosowania prawa polskiego do art. 88 RODO są regulacje wprowadzone do ustawy z dnia 26 czerwca 1974 r. Kodeks pracy ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych. Odnoszą się one m.in. do monitoringu wizyjnego w zakładzie pracy.
Przepisy Kodeksu pracy (k.p.) wskazują, kiedy i na jakich zasadach pracodawca może zainstalować monitoring. Jak stanowi art. 22^2 § 1 k.p., jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, pracodawca może wprowadzić szczególny nadzór nad terenem zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring). Przepis ten uprawnia wyłącznie do rejestracji obrazu, a nie dźwięku.
Uprawnienia do stosowania monitoringu fonicznego nie można także wywodzić z art. 22^3 § 4 Kodeksu pracy, który reguluje stosowanie innych form monitoringu. Żeby ta forma monitoringu mogła zostać zastosowana, musi to jasno wynikać z przepisu prawa rangi ustawy.
Stanowisko takie zostało poparte orzecznictwem sądów administracyjnych. Przykładem jest m.in. wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 28 października 2022 r. (sygn. akt II SA/Wa 1341/22), w którym sąd podzielił opinię UODO, że nagrywanie i utrwalanie dźwięku (głosu)

w zainstalowanym w ośrodku dla osób nietrzeźwych systemie monitoringu naruszało przepisy RODO. Nie istniała bowiem podstawa uprawniająca do takiego działania (o czym szerzej informowaliśmy w zamieszczonym na stronie internetowej UODO materiale **„WSA podzielił argumenty UODO. Rejestracja dźwięku tylko na podstawie prawa”**.)

Jednocześnie należy zwrócić uwagę, że zgodnie z przyjętymi przez Europejską Radę Ochrony Danych Wytycznymi 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo, zapis audiowizualny stanowi niewątpliwie większą ingerencję w prywatność niż monitoring wizyjny. Ponadto w pkt 9.3 ppkt 129 Wytycznych wskazano, że administrator przy wybieraniu rozwiązań technicznych odnoszących się do prowadzonego monitoringu nie powinien wybierać rozwiązań zawierających funkcje, które nie są niezbędne (wśród funkcji tych mieści się: nieograniczone śledzenie ruchów kamery, możliwość przybliżenia, transmisja radiowa, analiza i nagrania dźwiękowe). Zgodnie z przytoczonymi Wytycznymi funkcje, które nie są niezbędne, powinny zostać dezaktywowane.

LEPSZA OCHRONA DANYCH OSOBOWYCH PRZY ZGŁASZANIU ZDARZEŃ NIEPOŻĄDANYCH

Dzięki czynnemu udziałowi UODO w czasie prac legislacyjnych w projekcie ustawy o jakości w opiece zdrowotnej i bezpieczeństwie pacjenta udało się wprowadzić w aktualnie procedowanych przepisach rozwiązania zapewniające większą ochronę danych osobowych zarówno osoby zgłaszającej zdarzenia niepożądane, jak i pacjenta, którego zgłoszenie dotyczy oraz osoby uczestniczącej w zdarzeniu niepożądanym.

Organ nadzorczy był włączony w opiniowanie projektu ustawy o jakości w opiece zdrowotnej i bezpieczeństwie pacjenta już podczas rządowego etapu prac legislacyjnych. Większość uwag zgłoszonych w ich toku została uwzględniona, co przyczyniło się do podniesienia poziomu ochrony danych osobowych

przetwarzanych w związku ze zgłaszaniem zdarzeń niepożądanych, czyli zdarzeń zaistniałych w czasie lub w efekcie udzielenia bądź zaniechania udzielenia świadczenia opieki zdrowotnej, powodujących lub mogących spowodować negatywny skutek dla zdrowia lub życia pacjenta.

Doprecyzowane zostały przepisy normujące zgłaszanie przez personel podmiotu wykonującego działalność leczniczą osobie odpowiedzialnej (kierownikowi podmiotu wykonującego działalność leczniczą) zdarzeń niepożądanych, tak w kwestii zakresu danych osoby zgłaszającej, pacjenta, którego zgłoszenie dotyczy oraz osoby uczestniczącej w zdarzeniu niepożądanym, jak i okresu przechowywania powyższych danych oraz podmiotów, którym dane te mogą być udostępnianie. W następstwie uwag UODO w projekcie określono też, jakie dane ma zawierać lista wizytatorów biorących udział w procesie akredytacji podmiotów wykonujących działalność leczniczą. Rozstrzygnięto również, iż prowadzony przez ministra właściwego do spraw zdrowia Rejestr Zdarzeń Niepożądanych ma nie zawierać danych pozwalających na identyfikację pacjenta, którego dotyczy zdarzenie niepożądane.

W tej sytuacji na etapie procedowania tego projektu ustawy przez Sejm RP, UODO ponowił jedynie sugestię, by – w związku ze zmianami wprowadzanymi omawianym projektem do ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej – kwestię obserwacji (monitoringu) pomieszczeń w podmiocie wykonującym działalność leczniczą kompleksowo uregulować w akcie prawnym, nie zaś regulaminie organizacyjnym tworzonym przez kierownika podmiotu wykonującego taką działalność. Niemniej wobec: wprowadzenia w projekcie wiążących wytycznych co do kwestii, które muszą być unormowane w regulaminie organizacyjnym, nałożenia na kierownika podmiotu wykonującego działalność leczniczą bezpośredniej odpowiedzialności za wykorzystanie monitoringu zgodnie z przepisami prawa, wprowadzenia zasady związania celem przy przetwarzaniu nagrań obrazu uzyskanego w wyniku monitoringu, ustalenia maksymalnego okresu przechowywania takich nagrań wraz z obowiązkiem ich zniszczenia po upływie tego okresu, UODO uznał autonomię projektodawcy w tym zakresie.

UCZMY DZIECI ROZWAGI, BY MOGŁY OCENIĆ ZAGROŻENIA, JAKIE PŁYNĄ Z UDOSTĘPNIANIA DANYCH

O Nagrodzie im. Michała Serzyckiego i potrzebie edukowania dzieci jak bezpiecznie „żyć w sieci" mówi Iwona Niedzielska-Taźbier, szkolna koordynatorka ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa" w rozmowie z Eweliną Janczylik-Foryś.

Iwona Niedzielska-Taźbier – nauczycielka w Szkole Podstawowej nr 17 z Oddziałami Integracyjnymi im. 21. Brygady Strzelców Podhalańskich w Rzeszowie. Od 2018 roku pełni funkcję szkolnej koordynatorki programu „Twoje dane – Twoja sprawa". Jest autorką licznych wewnątrzszkolnych materiałów nt. ochrony danych osobowych i bezpieczeństwa w Internecie oraz inicjatorką wielu innych działań zorganizowanych w ramach programu edukacyjnego UODO dla szkół.

Podczas obchodów XVII Dnia Ochrony Danych Osobowych została Pani uhonorowana Nagrodą im. Michała Serzyckiego, przyznawaną przez Prezesa UODO osobom zasłużonym dla promowania idei ochrony danych osobowych i prawa do prywatności oraz edukację w tym zakresie.

Przypadła mi w udziale przyjemność odebrania Nagrody im. Michała Serzyckiego podczas XVII Dnia Ochrony Danych Osobowych w Ełku. To dla mnie bardzo duże zaskoczenie i wyróżnienie. W szkole zajmujemy się m.in. ochroną danych osobowych i bezpieczeństwem w sieci. Staramy się, aby treści przekazywane uczniom szkoły podstawowej były dostosowane do poziomu odpowiadającego ich możliwościom rozumienia tych zagadnień. Co za tym idzie, prezentowane przez nas treści są proste i odpowiednie do wieku uczniów. Inaczej rozmawiamy z dziećmi w klasach pierwszych, a inaczej z młodzieżą w klasach siódmych i ósmych.

Nasza szkoła uczestniczy w programie edukacyjnym „Twoje dane – Twoja sprawa" od 2018 roku. Na początku naszej drogi raczkowaliśmy, bo nie bardzo wiedzieliśmy, co i jak zrobić. Jednak z każdym rokiem, przystępując do kolejnej edycji programu, w oparciu o materiały przekazywane nam przez Urząd Ochrony Danych Osobowych, wypracowaliśmy własny schemat działania oraz materiały, które wykorzystujemy w pracy z uczniami.

Na zaangażowanie w realizację programu edukacyjnego składa się praca wielu osób – nie tylko moja praca, ale i całego zespołu.

Zatem na sukces Nagrody im. Michała Serzyckiego, którą Pani otrzymała, pracuje także wiele innych osób.

Oczywiście. Jestem koordynatorką programu „Twoje dane – Twoja sprawa", przygotowuję inicjatywy, planuję działania, opracowuję materiały i przekazuję je do realizacji wychowawcom. Bez wspólnej pracy i zaangażowania zarówno koordynatora programu, dyrekcji szkoły, jak i nauczycieli, nie można byłoby mówić o sukcesie.

Podczas Dnia Ochrony Danych Osobowych powiedziała Pani kilka ważnych rzeczy, do których chciałabym się odnieść. Pani zdaniem, biorąc pod uwagę cały program dydaktyczny, ochrona danych osobowych może się wydawać tematem mało ciekawym dla uczniów. Jednak doszliście Państwo do wniosku jako grono pedagogiczne, żeby podjąć ten temat w pracy z uczniami.

Pracuję w szkole 20 lat i widzę, jak bardzo zmienia się otaczająca nas rzeczywistość. Obecnie dzieci nie znają świata bez Internetu, telewizorów czy smartphonów. W szkole nie tylko uczymy konkretnych przedmiotów, ale też wychowujemy. Dzieci, korzystając z nowych technologii, nie mają w sobie odpowiedniej refleksji czy rozwagi, by ocenić zagrożenia. I tego chcemy uczyć dzieci, że jeżeli korzystają z Internetu, są obecne w mediach społecznościowych czy wypowiadają się na forach internetowych, to niech to robią z odpowiednią rozwagą. Niech nie udostępniają danych osobowych, jeśli tego robić nie muszą, ponieważ może to przynieść różne skutki w ich życiu. Świat się zmienia i ważne jest, aby postępować mądrze i bezpiecznie. W naszych domach jeszcze poświęcamy za mało uwagi prywatności czy ochronie danych osobowych. W szkole realizujemy wiele różnych programów, ale myślę, że ten jest jednym z bardziej znaczących.

Ta rozwaga, o której Pani mówi, nie dotyczy tylko dzieci, ale nas wszystkich, żeby z odpowiednią ostrożnością brać udział w mediach społecznościowych, pisać komentarze na forach internetowych, „żyć w sieci". Dlaczego Pani tak sądzi?

Staramy się uczyć takiej autorefleksji, pokazywać ewentualne konsekwencje zachowań. Mówimy: „Zastanów się, po co udostępniasz dane, komu je udostępniasz, jak to może zostać wykorzystane?". Zwracamy uwagę, że dzieci są tubylcami cyfrowymi, że nie znają świata bez Internetu, dlatego poruszając się w wirtualnej przestrzeni powinni być ostrożni. W klasach 7 na wywiadówce przekazujemy rodzicom w zwięzłej formie treści, o których w ramach programu rozmawiamy z dziećmi. Chcemy zasygnalizować im, żeby oni także jako ludzie dorośli zastanowili się nad tym, co robią ze swoimi danymi.

Myślę, że to ważne, że prezentujecie Państwo także treści rodzicom. Jakie są Pani doświadczenia w tym kontekście?

Rozpoczynając rok szkolny, podczas pierwszych zebrań z rodzicami, przedstawiamy im informacje na temat realizacji programu „Twoje dane – Twoja sprawa" w naszej szkole. Mamy potwierdzenie, że rodzice popierają program i fakt, że uczymy o ochronie danych osobowych i prawie do prywatności.

Podczas konferencji w Ełku wspomniała Pani także, że pod koniec roku szkolnego prosicie Państwo uczniów, aby przygotowywali prace na temat ochrony danych osobowych. Jakie płyną refleksje po przeczytaniu tych prac?

W tych pracach, a są to np. opowiadania, prezentacje lub prace plastyczne, widać wyraźnie, że uczniowie mają świadomość tego, czym jest prywatność, a odnosząc się do ochrony danych osobowych, wiedzą, że należy ją chronić. Tak jak mówiłam wcześniej, od 2018 roku uczestniczymy w programie edukacyjnym, więc i wiedza naszych uczniów jest już na jakimś poziomie. Materiały dostosowujemy do potrzeb uczniów. W pierwszych klasach uczymy podstaw. Wskazujemy, że pierwszym dokumentem tożsamości, jaki dzieci otrzymują, są legitymacje szkolne. I tak z roku na rok, w każdej klasie dodajemy dodatkowe elementy, a im uczniowie są starsi, tym bardziej złożone kwestie poruszamy.

Myśli Pani, że tak jak teraz panuje moda na pokazywanie swojego życia w sieci, tak kiedyś zapanuje moda na prywatność?

Myślę, że to wymaga solidnej edukacji, ale też i głębokiej refleksji. Temat ten jest niezwykle ważny. Ja osobiście nie mam konta w mediach społecznościowych jako jedna z nielicznych osób w moim otoczeniu. Ale mam też dzieci. Jako mama nastolatków, mówię do córki czy syna, że jeśli chcą się podzielić w mediach społecznościowych tym, co się stało w ich życiu, to po pierwsze powinni weryfikować osoby, którym udostępniają dane treści, a po drugie mogą dokonać selekcji tego, co chcą pokazać, czym chcą się pochwalić. Przede wszystkim myślmy o tym, co udostępniamy w Internecie i zachowajmy zdrowy rozsądek. Nie chodzi o to, aby zupełnie się zamknąć na Internet i na komunikowanie się w mediach społecznościowych. Jednak nieraz obserwuję co inne osoby udostępniają na swój temat i widzę, że to są naprawdę głęboko prywatne sprawy. Przykład, którym często się posługuję, odpowiadając na pytanie, kiedy ktoś pierwszy raz pojawia się w sieci? Dzieje się to wtedy, kiedy mama udostępnia w mediach społecznościowych zdjęcia dziecka wykonane podczas badania USG. Robi to po to, żeby wszyscy je zobaczyli. Można sobie zadać pytanie, czy to już jest ten moment, kiedy prywatność została zachwiana?

To bardzo dobry przykład, obrazujący naszą potrzebę nieustannego skupiania na sobie uwagi innych.

Kiedyś widziałam w Internecie taki film, w którym prezentowano historię wykonania jednego zdjęcia. Osoba prowadząca wskazała zarazem, co można odczytać z tego zdjęcia, jeśli się je „wrzuci do Internetu". Jesteśmy w stanie nie tylko ustalić lokalizację, ale i datę wykonania fotografii z podaniem dokładnej godziny. Nawet nie zdajemy sobie sprawy, że historia zdjęcia może kiedyś wpłynąć na naszą przyszłość. Zdjęcia, którymi teraz się chwalimy idą w świat, w przyszłości mogą posłużyć jako mem. Nawet jeśli po jakimś czasie je usuniemy, tracimy nad nimi jednak kontrolę, bo przecież one wcześniej mogły zostać przez kogoś skopiowane.

Różne badania wskazują, że coraz młodsze dzieci korzystają z urządzeń mobilnych czy z Internetu. Wiek tzw. inicjacji cyfrowej się przesuwa. Czy również zauważa Pani to zjawisko?

Kiedyś uczestniczyłam w takim szkoleniu na temat zdrowia psychicznego. Prowadzący spotkanie wskazywali, że najmłodsze dziecko, jakie mieli na terapii, które było uzależnione od Internetu miało 3 lata. Sądzę, że każdy z nas był świadkiem sytuacji, kiedy rodzice dają małym dzieciom, jeszcze w wózkach telefon, żeby dzieci były cicho w sklepie czy podczas wizyty u lekarza. Myślę sobie, że problemem nie jest tylko brak rozwagi w posługiwaniu się danymi, ale nieumiejętne posługiwanie się Internetem w ogóle, które prowadzi do tak negatywnych zjawisk jak problemy z uzależnieniem od niego już u dzieci. To my – dorośli – musimy przede wszystkim dawać dobry przykład naszym dzieciom. Edukacja jest równie ważna. Przyznam, że im dłużej uczestniczymy w programie „Twoje dane – Twoja sprawa", to tym bardziej widzę jego bardzo głęboki sens.

ŚWIADOMOŚĆ POLAKÓW WZRASTA, ALE ICH EDUKACJA WCIĄŻ JEST POTRZEBNA

O Nagrodzie im. M. Serzyckiego, powszechnej edukacji na temat ochrony danych osobowych i wyzwaniach w tej dziedzinie mówi Edyta Bielak-Jomaa, w rozmowie z Eweliną Janczylik-Foryś

Dr Edyta Bielak-Jomaa – Prezes Urzędu Ochrony Danych Osobowych w latach 2018–2019 oraz Generalny Inspektor Ochrony Danych Osobowych w latach 2015–2018. Wykładowca z zakresu ochrony danych osobowych, prawa pracy i zagranicznych migracji zarobkowych. Autorka ponad 50 opracowań nt. ochrony danych osobowych, prawa pracy i problematyki rynku pracy. Organizatorka licznych konferencji krajowych i międzynarodowych, debat i warsztatów poświęconych tym zagadnieniom.

Jak to jest otrzymywać Nagrodę im. Michała Serzyckiego, którą się samemu ustanowiło?

Bardzo miło! To jest oczywiście wielkie wyróżnienie, zaszczyt i honor otrzymać tę nagrodę. Cieszę się, że Prezes UODO dostrzegł w mojej działalności starania na rzecz ochrony danych osobowych oraz promocji edukacji w tej materii i docenił je.

Jak edukować o ochronie danych osobowych obywateli, administratorów oraz inspektorów ochrony danych? Jak uczyć o konsekwencjach naszych działań?

To jest bardzo dobre pytanie. Nie powinniśmy sobie zadawać pytania: „Czy edukować?", ale powinniśmy pytać „Jak edukować?". Po pierwsze, bezwzględnie musimy edukować. Po drugie, musimy edukować

w sposób przystępny, zatem ważna jest formuła tej edukacji. Myślę, że edukować trzeba wszystkich: administratorów, osoby fizyczne, dzieci. Trzeba mówić o wadze ochrony danych osobowych oraz o potrzebie ochrony prywatności. Do każdej z tych grup należy kierować nieco inny przekaz. Myślę, że administratorzy, którzy skupieni są na wypełnianiu swoich zadań, codziennych obowiązków związanych z przetwarzaniem danych osobowych, mają poczucie odpowiedzialności za przestrzeganie prawa. Według mnie trzeba wskazywać nie tylko na to, że administrator musi przetwarzać dane zgodnie z przepisami, ale pokazać także, że należy przykładać większą wagę do etycznego podejścia. Administratorzy powinni zwrócić uwagę, że przetwarzając dane, mogą wkraczać w sferę prywatności.

To dotyczy administratorów. A co z osobami fizycznymi?

Jeśli chodzi o osoby dorosłe, to myślę, że ważne jest uczulenie ich na to, aby dbali o swoją prywatność i świadomie podchodzili do udostępniania innym osobom danych na swój temat. Odnosząc się z kolei do edukacji dzieci, to myślę, że Urząd Ochrony Danych Osobowych świetnie sobie na tym polu radzi poprzez realizację ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa", który kierowany jest do uczniów i nauczycieli. Uważam, że mówiąc o metodach edukacji, powinniśmy uczyć o prywatności oraz o ochronie danych osobowych poprzez wskazywanie ryzyk czy zagrożeń, a także obrazowo przedstawiać konsekwencje naszych działań. Ważne, aby komunikaty zawierały treści zapisane językiem prostym i przejrzystym, czyli takim, który wszyscy zrozumiemy, ale też powinny być tworzone językiem korzyści.

Mówić językiem prostym. Jak to zrobić, jeżeli niektórzy uważają, że sama nomenklatura RODO jest trudna i zawiła?

Tak. Faktycznie często spotykam się z zarzutem, że RODO jest skomplikowane i trudne. Traktuję przepisy ogólnego rozporządzenia o ochronie danych jako wyzwanie, które po prostu trzeba podjąć i zrealizować. Otaczająca nas rzeczywistość nieustannie się zmienia. Pojawiają się coraz to nowe technologie, które wkraczają w obszar codziennego życia. Nie możemy się spodziewać, że każdy będzie rozumiał język ogólnego rozporządzenia czy będzie potrafił przewidzieć grożące mu ryzyka. Dlatego uważam, że wszyscy powinniśmy się na bieżąco uczyć. Słusznie podkreślają ci, którzy zajmują się ochroną danych, że przecież nie chodzi o to, żeby zakazać przetwarzania danych osobowych tylko, żeby przetwarzanie to oprzeć na odpowiedzialności i racjonalności. Natomiast z perspektywy osób fizycznych właściwe jest zachowanie czujności.

Wydaje się, że obywatele i administratorzy mają świadomość praw i obowiązków wynikających z RODO, o czym może świadczyć chociażby liczba składanych do Urzędu skarg czy zgłaszanych naruszeń ochrony danych. Czy po tylu latach obecności w Polsce systemu ochrony danych osobowych, nadal trzeba przypominać o podstawowych kwestiach?

Świadomość wśród społeczeństwa wzrasta, ale edukować nadal trzeba. Uważam, że znajomość przysługujących osobom fizycznym praw, jakim jest przykładowo złożenie skargi, powoduje też wzrost świadomości administratora czy podmiotu przetwarzającego. Jest to jasny sygnał skierowany do tych podmiotów, że wiemy, jakie mamy prawa i będziemy je realizować. Z kolei jeżeli administrator nie ma odpowiednio dostosowanych środków organizacyjnych czy technicznych, jakiegoś systemu związanego z ochroną danych, który prawidłowo by funkcjonował, to będzie musiał podjąć działania o charakterze naprawczym. Administratorzy także zdają sobie sprawę z konsekwencji naruszania przepisów RODO, ewentualnego postępowania administracyjnego, które może się zakończyć wydaniem decyzji o nałożeniu kary pieniężnej albo jakąś inną sankcją.

Wspomniała Pani o administracyjnych karach pieniężnych, które rzeczywiście wzbudzają największe zainteresowanie, ale też warto dodać, że nakładanie kar przez organ nadzorczy nie jest celem samym w sobie.

Tak, natomiast informacja o tym, że podmiot został ukarany działa na inne podmioty, na innych administratorów i ma ona wymiar wychowawczy oraz edukacyjny. Oczywiście wywołuje różne emocje, od takich najbardziej skrajnych – negujących zasadność, a nawet prawo do nakładania kary przez organ nadzorczy, po działania stymulujące administratorów do dokonania przeglądu czy analizy procesów w swoich organizacjach. Liczę na to, że świadomość wśród administratorów będzie na jeszcze wyższym poziomie, że zwrócą oni większą uwagę na procesy przetwarzania, z którymi mają do czynienia, i odpowiednio dostosują do nich procedury, wdrożą rozwiązania techniczno-organizacyjne. Natomiast najważniejsza jest świadomość, że system ochrony danych musi funkcjonować w przestrzeni organizacji, jako element systemu zarządzania nią.

Administratorom należy uzmysłowić, aby wprowadzili zasady związane z ochroną danych osobowych nie w sposób incydentalny, ale w ogóle zbudowali system ochrony danych osobowych w organizacji i włączyli go w model operacyjny zarządzania. W tej kwestii jest jeszcze chyba dużo do zrobienia?

Zawsze powtarzam, że ochrona danych osobowych nie powinna stanowić jakiegoś oddzielnego elementu w danej organizacji, o którym sobie dopiero przypominamy w momencie wystąpienia incydentu czy naruszenia. To, do czego powinni dążyć administratorzy, zarządzający organizacją, to jest właśnie umocowanie, czyli postrzeganie problematyki ochrony danych osobowych jako elementu całego systemu zarządzania organizacją. Tak jak w organizacji funkcjonują, w sposób uporządkowany, jasny i nie budzący wątpliwości, z punktu widzenia kierowania organizacją, procedury związane np. z zatrudnianiem pracowników czy księgowością, tak samo powinny być wdrożone i stosowane przepisy o ochronie danych osobowych. Co istotne, w tym kontekście, same procedury, dokumenty i technologia nie wystarczą. Kluczowe znaczenia ma bowiem prawidłowe określenia ról, zadań i obowiązków wszystkich osób,

które uczestniczą w przetwarzaniu danych. I wracamy do wagi edukowania np. pracowników, konieczności przeprowadzenia szkoleń, które zapewnią im dostęp do wiedzy, dzięki temu wyposażą w kompetencje zgodnego z zasadami przetwarzania danych. "Poukładanie" ochrony danych w organizacji, to nie tylko wyznaczenie inspektora ochrony danych i scedowanie na niego pełnej odpowiedzialności z tego tytułu. Niektórzy przyzwyczaili się do tego, że gdy mówimy o czymkolwiek, co jest związane z ochroną danych w organizacji, to wskazujemy zawsze na dwa podmioty odpowiedzialne…

…**administratora i inspektora ochrony danych…**

…oczywiście. A trzeba zwrócić uwagę na to, że każdy, kto przetwarza dane osobowe w organizacji, bez względu na to, jaką funkcję pełni czy jakie stanowisko zajmuje, odpowiada za nie, o ile jego obowiązki obejmują także przetwarzanie danych. Chcę przez to powiedzieć, że ochroną danych osobowych powinien interesować się każdy, a system zarządzania organizacją powinien składać się z kilku mniejszych elementów, w tym z ochrony danych osobowych. Administratorzy powinni podjąć wysiłek zorganizowania całego systemu, który będzie kompatybilny z innymi elementami wchodzącymi w zakres zarządzania organizacją.

Kiedy otrzymujemy jasne wytyczne, jesteśmy w stanie się do nich dostosować. Pracownik, rozpoczynając pracę, może zapoznać się z polityką bezpieczeństwa czy z innymi zasadami obowiązującymi w danej organizacji. Wie, że wymagane jest np. okresowe zmienianie hasła czy podwójne uwierzytelnianie. Czy administratorzy mogą „wymusić" na osobach fizycznych, użytkownikach, takie zachowania, które pozwolą zachować bezpieczeństwo danych?

Tak, oczywiście. Z technicznego punktu widzenia jest to absolutnie do zrobienia. I myślę, że wszystko to, co ma służyć zapewnieniu odpowiedniego poziomu bezpieczeństwa danych, powinno być wdrożone. Ale trzeba także zwrócić uwagę na racjonalność działania administratora. Zastosowanie odpowiednich środków technicznych i organizacyjnych powinno być związane i rozpatrywane w odniesieniu do całego kontekstu przetwarzania danych. Nie chciałabym, żebyśmy wskazywali na zmianę hasła czy podwójne uwierzytelnianie jako jedyne odpowiednie środki bezpieczeństwa. Administrator powinien znać organizację nie tylko pod kątem struktury i zasobów finansowych. Zazwyczaj administratorzy wskazują, że nie zdołali dostosować operacji przetwarzania do przepisów RODO, bo nie są w stanie ponieść środków finansowych zabezpieczenia systemu informatycznego, albo zapewnienie bezpieczeństwa danych upatrują wyłącznie w funkcjonującym systemie informatycznym. Potem jednak okazuje się, że poza zaimplementowaniem tego systemu, nie podjęto żadnych dodatkowych działań. Tymczasem wprowadzenie nawet najprostszych i niemal bezkosztownych rozwiązań mogłoby uchronić organizację przed naruszeniami i ich skutkami. Warto więc nie tylko przeprowadzić audyt, aktualizować systemy, tworzyć kopie zapasowe itd., ale trzeba także zdiagnozować zasoby organizacji. Przede wszystkim administrator musi mieć wiedzę w zakresie potrzeb, co do umiejętności, świadomości i wiedzy personelu, którym dysponuje i dostosować do tych

potrzeb formy wsparcia pracowników – szkolenia, warsztaty, instruktaż. Pozwoli to na nabycie umiejętności i nawyków praktycznych, ułatwiających przetwarzanie danych osobowych w sposób bezpieczny, odpowiedzialnie oraz z uwzględnieniem racjonalności działania. Przykładowo, jeżeli administrator podejmuje decyzję, że pracownicy wysyłając e-maile mają stosować zabezpieczenie w postaci szyfrowania pików z danymi osobowymi, wyposaża pracowników w odpowiedni program i szkoli pracowników na tę okoliczność, to konieczność stosowania takiego rozwiązania, mimo być może początkowych trudności, po kilku wysłanych e-mailach stanie się naturalna i nie będzie wywoływać ani niechęci, ani obaw przed dodatkowymi obciążeniami. Wydaje mi się więc, że bardzo często stosowanie najprostszych rozwiązań pozwala na zwiększenie świadomości osób przetwarzających dane, a w praktyce przekłada się na podniesienie poziomu bezpieczeństwa, również bezpieczeństwa administratora.

Jakie, Pani zdaniem, stoją wyzwania przed ochroną danych osobowych?

Chciałabym, aby na ochronę danych osobowych patrzeć jako na część większej całości. Wydaje się, że na tym etapie obowiązywania RODO, administratorzy powinni stosować przepisy bez większych trudności. Powinni więc w swoich organizacjach przyjmować określone rozwiązania, na podstawie rzetelnej analizy potrzeb, możliwości, wyzwań w obszarze ochrony danych, podejmować decyzje, co do wprowadzonych mechanizmów podnoszących poziom bezpieczeństwa danych i potem konsekwentnie je realizować. Niestety nadal dla wielu organizacji ciągle stanowi to problem. Proszę zauważyć, w najbliższym czasie nie zmniejszy się liczba aktów prawnych, które będą się odnosić bezpośrednio albo pośrednio do danych osobowych czy kwestii związanych z prywatnością, wręcz przeciwnie, przed nami „tsunami” legislacyjne. Projektowane na poziomie europejskim akty prawne będą wymagały również zmian w przepisach krajowych. Jeśli dodamy do tego, że co chwila pojawiają się jakieś nowe rozwiązania technologiczne, algorytmy matematyczne, sztuczna inteligencja znajduje zastosowanie w coraz to nowych obszarach życia i sektorach rynku, wyzwaniem będzie dostosowanie się administratorów do rzeczywistości legislacyjnej oraz rzeczywistości cyfrowej, dlatego umiejętność stosowania przepisów i technologii w praktyce działania administratorów, będzie wymagać stałego podnoszenia wiedzy i świadomości na temat potencjalnych niebezpieczeństw i ryzyk, w celu ich zminimalizowania.

KARY

Finlandia: kara 230 tys. euro za naruszenie ochrony danych osobowych pracowników

Fiński organ nadzorczy nałożył na spółkę Viking Line administracyjną karę pieniężną w wysokości 230 tys. euro za niezgodne z prawem przetwarzanie danych dotyczących zdrowia pracowników.

Fiński organ nadzorczy na podstawie złożonej skargi prowadził postępowanie w sprawie działalności Viking Line Oy Abp. Były pracownik administratora poinformował fiński organ nadzorczy, że mimo wniosku nie otrzymał wszystkich swoich danych osobowych przechowywanych w systemach przedsiębiorstwa. Według pracownika, administrator od 20 lat przechowywał jego dane dotyczące zdrowia w systemie kadrowym. Administrator zapisywał w tym systemie informacje dotyczące diagnoz w połączeniu z informacjami o nieobecnościach z powodu choroby. Według skarżącego niektóre zapisane informacje o diagnozach były nieprawidłowe, ponieważ nie było możliwe wprowadzenie do nich wszystkich kodów diagnoz. Zgodnie z fińską ustawą o ochronie danych osobowych, zapisywanie informacji o diagnozach w połączeniu z innymi danymi dotyczącymi zatrudnienia jest niezgodne z prawem. Administrator nie tylko niezgodnie z prawem zapisał w systemie kadrowym informacje o diagnozach swoich pracowników, ale również niektóre z tych danych były nieprawidłowe. Fiński organ nadzorczy uznał działania przedsiębiorstwa za szczególnie naganne w tym zakresie. Dane dotyczące zdrowia powinny były zostać natychmiast usuwane, gdy ich przechowywanie przestało być już niezbędne. Nieprawidłowe informacje o diagnozach były przechowywane za długo i mogły stanowić zagrożenie dla ochrony prawnej osoby fizycznej. Administrator nie poinformował swoich pracowników w odpowiedni sposób o przetwarzaniu ich danych osobowych. Fiński organ nadzorczy zauważył, że przedsiębiorstwo powinno było dostarczyć pracownikom wszystkie dane, o które wnosili.

Na Viking Line nałożono administracyjną karę pieniężną w wysokości 230 000 EUR za kilka naruszeń przepisów dotyczących ochrony danych. Administratorowi zostało również udzielone upomnienie. Fiński organ nadzorczy nakazał administratorowi dostosować swoje praktyki i poinformować pracowników o przetwarzaniu ich danych osobowych zgodnie z wymogami RODO.

Źródło: **decyzja organu nadzorczego**

MIĘDZYNARODOWE

Hiszpańska branża reklamowa ma swój kodeks postępowania

Hiszpański organ nadzorczy zatwierdził kodeks postępowania dla podmiotów zajmujących się działalnością reklamową, który obowiązuje od 28 stycznia 2023 r.

Kodeks postępowania AUTOCONTROL „Przetwarzanie danych w działalności reklamowej" zatwierdzony 17 stycznia 2023 r. przez hiszpański organ nadzorczy (AEPD), zawiera rozwiązania służące sprawniejszemu rozpatrywaniu skarg obywateli dotyczących tego sektora.

Niechciana reklama jest jedną z najczęstszych podstaw skarg składanych do hiszpańskiego organu nadzorczego, dlatego składanie skarg za pośrednictwem AUTOCONTROL i przy zastosowaniu kodeksu postępowania, otwartego dla wszystkich przedsiębiorstw prowadzących działalność reklamową, umożliwi ustanowienie dobrowolnej i bezpłatnej procedury mediacyjnej dla obywateli w celu zapewnienia im szybszej reakcji na składane przez nich skargi. Kodeks postępowania ma zastosowanie do przetwarzania danych w celach reklamowych przez podmioty, które go przyjęły. Dzięki opracowanemu przez AUTOCONTROL pozasądowemu systemowi rozstrzygania sporów powstałych między obywatelami a podmiotami stosującymi kodeks, w związku z przetwarzaniem danych w zakresie działalności reklamowej, AUTOCONTROL rozpatruje otrzymane skargi poprzez wszczęcie procedury mediacyjnej. Przedstawiciel organizacji w ciągu maksymalnie 15 dni proponuje działania, które uzna za właściwe w ramach mediacji. Maksymalny czas trwania procedury wynosi 30 dni.
W przypadku braku osiągnięcia porozumienia, skargi będą przekazywane do organu nadzorczego.

Informacje na temat kodeksu postępowania