URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO

Nr 3/05/23

www.uodo.gov.pl

SPIS TREŚCI

Drodzy Czytelnicy!

Od kilku lat maj – nie tylko dla pracowników Urzędu Ochrony Danych Osobowych czy ekspertów z zakresu ochrony danych osobowych, ale wszystkich, dla których prawa człowieka mają znaczenie – jest miesiącem szczególnym. 25 maja 2018 roku rozpoczęto stosowanie ogólnego rozporządzenia o ochronie danych (RODO). W tym roku mamy dodatkowo okazję do świętowania ćwierćwiecza systemu ochrony danych w Polsce. Te rocznice wskazują, że ochrona danych osobowych w naszym kraju ma swoją długoletnią tradycję. RODO nie zmieniło w istotny sposób regulacji w tym zakresie, ale dało administratorom dużą samodzielność. Wyznacza im cele, które mają osiągnąć, lecz nie narzuca sposobu, w jaki powinni to robić. Dzięki temu mają możliwość dopasowania swoich procesów przetwarzania danych osobowych czy stosowanych w tym zakresie rozwiązań do swojej specyfiki i kultury organizacyjnej.

Osoba fizyczna w centrum uwagi, a także wzrost świadomości i budowanie odpowiednich postaw to priorytety przyświecające 4-letniej kadencji Prezesa Urzędu Ochrony Danych Osobowych, Jana Nowaka. W tym czasie Urząd podjął wiele działań w trosce o prawa jednostki, tak aby prawo do ochrony danych osobowych i prawo do prywatności uznawano za gwarantowane prawa człowieka. Działania te miały charakter nie tylko legislacyjny, związany z rozpatrywaniem wnoszonych przez obywateli skarg czy zgłaszanych przez administratorów naruszeń.

To także wiele różnorodnych działań edukacyjno-informacyjnych, w tym angażowanie się w liczne webinaria, udział przedstawicieli UODO w konferencjach, prezentowanie wyników badań na temat ochrony danych osobowych.

Teraz przed UODO kolejne nowe wyzwania. Powstał pierwszy w Polsce Instytut Prawa Ochrony Danych Osobowych (IPODO). Instytut zajmujący się zagadnieniami ochrony danych został powołany na Akademii Ekonomiczno-Humanistycznej pod patronatem i we współpracy z Urzędem Ochrony Danych Osobowych. Jego celem jest m.in. propagowanie najlepszych praktyk i rozwiązań w zakresie przetwarzania i ochrony danych czy wsparcie w rozwoju polskiej gospodarki poprzez popularyzowanie innowacyjnych rozwiązań służących ochronie prywatności i danych. Zakresem swoich działań będzie wspierać także inne instytucje i organizacje zajmujące się tą tematyką.

Aspirujemy do bycia głównym ośrodkiem zajmującym się ochroną danych w Polsce, skupiając w Radzie Naukowej czy Grupach Roboczych Instytutu najlepszych specjalistów w tej dziedzinie. Poprzez zaangażowanie Urzędu w funkcjonowanie Instytutu jest zagwarantowany przepływ wiedzy i doświadczenia od jedynego właściwego i wyspecjalizowanego w tej tematyce organu nadzorczego. Zapraszamy do współpracy.

Jesteśmy przekonani, że na system ochrony danych osobowych w Polsce oraz na przepisy RODO warto patrzeć jako na okazję do uporządkowania całej sfery związanej z przetwarzaniem danych osobowych. To także szansa na budowanie przewagi konkurencyjnej, gdyż dbałość o ochronę wykorzystywanych danych ma przełożenie na zaufanie zarówno klientów, jak i partnerów biznesowych.

Adam Sanocki
Dyrektor Departamentu
Komunikacji Społecznej UODO,
Rzecznik Prasowy

1 ROZMOWA Z EKSPERTEM

CZŁOWIEK I JEGO PRAWA DO OCHRONY DANYCH OSOBOWYCH I PRYWATNOŚCI TO PRIORYTET

Jan Nowak, Prezes Urzędu Ochrony Danych Osobowych w rozmowie z Adamem Sanockim podsumowuje swoją kadencję oraz wskazuje dalsze wyzwania z zakresu ochrony danych osobowych i prawa do prywatności.

Dobiegła końca Pana pierwsza kadencja w roli Prezesa Urzędu Ochrony Danych Osobowych. Co z tego, co Pan wcześniej zamierzał zrealizować, obejmując tę funkcję, udało się osiągnąć w ciągu tych czterech lat?

Niezwykle ważną zmianą, która ma dalekosiężne i pozytywne konsekwencje jest zmiana struktury organu nadzorczego, co miało miejsce kilka miesięcy po objęciu przeze mnie stanowiska Prezesa Urzędu Ochrony Danych Osobowych. Zmiana ta nastąpiła 1 grudnia 2019 roku. Dzięki niej pewne obszary Urzędu zaczęły działać jeszcze sprawniej niż wcześniej. W miejsce zespołów tematycznych zajmujących się kompleksowo określonymi sektorami, zostały utworzone departamenty, które skupiły się na realizacji konkretnych zadań wynikających z RODO.

Dziś, na przykładzie Departamentu Skarg, widzimy, że była to słuszna decyzja. Pomimo wciąż utrzymującego się bardzo wysokiego poziomu wnoszonych skarg, liczba spraw zakończonych wydaniem decyzji stale wzrasta, w porównaniu z latami ubiegłymi. I o to chodziło. To element, który wpisuje się w cele, jakie sobie wyznaczyłem, czyli dążenie do tego, by Urząd był bliżej obywateli i działał skuteczniej.

Zatrzymajmy się na chwilę przy skargach, gdyż wzbudzają one wiele emocji wśród osób je składających.

Urząd funkcjonuje w tym zakresie coraz skuteczniej. Mamy do czynienia ze skomplikowaną materią, której problem często jest bardzo złożony.

Zacznijmy od tego, że organ nadzorczy, na długo zanim zaczęliśmy stosować RODO zdawał sobie sprawę, że składanych skarg będzie przybywać. Dlatego już wtedy zabiegał o wprowadzenie stosownych zmian w prawie, które doprowadziłyby do uproszczenia postępowań związanych z rozpatrywaniem skarg. Ustawodawca nie uwzględnił jednak naszych postulatów. W konsekwencji procedury wymagane przez Kodeks postępowania administracyjnego, wciąż niepotrzebnie wydłużają czas toczących się postępowań.

Należy mieć też na uwadze, że administratorzy, wobec których wszczęte jest postępowanie, nie zawsze odbierają korespondencję albo udzielają informacji niepełnych, sprzecznych ze sobą, a to też przekłada się na przedłużenie prowadzonych postępowań.

To wszystko ma bardzo duże znaczenie m.in. dla czasu trwania postępowań przy dużej skali skarg, które trafiają do Urzędu. W 2020 roku do Urzędu Ochrony Danych Osobowych wpłynęło w sumie 6,4 tys. skarg. Rok później było ich już 8,3 tys., a w ubiegłym roku wpłynęło ich prawie 7 tys. Tymczasem w 2017 roku, czyli w roku poprzedzającym rozpoczęcie stosowania RODO skarg

było znacznie mniej, bo 2950. Pamiętajmy, że UODO zajmuje się jeszcze analizowaniem naruszeń ochrony danych osobowych, które zgłaszają nam administratorzy oraz ma też inne zadania, w tym działalność edukacyjną. Dochodzimy tu do kolejnego wyzwania, jakim są potrzeby kadrowe organu nadzorczego. Ten element wymaga zdecydowanego wzmocnienia, ale na to potrzebne są dodatkowe środki finansowe w budżecie Urzędu. Odpowiednia organizacja pracy, co już nastąpiło za sprawą zmiany struktury Urzędu, nie jest w tym zakresie wystarczająca.

Wspomniał Pan o edukacji. Co się zmieniło w tym elemencie przez te cztery lata?

Przede wszystkim dzięki konsekwentnie realizowanym działaniom edukacyjnym, dużej aktywności mediów cały czas znacząco wzrasta świadomość obywateli na temat ochrony danych osobowych i praw, jakie im przysługują na gruncie RODO. To w dużej mierze zasługa aktywności podejmowanych także przez UODO i współpracy organu nadzorczego z innymi organami administracji publicznej, czy instytucjami.

Od 13 lat z dużymi sukcesami prowadzony jest program edukacyjny „Twoje dane – Twoja sprawa", kierowany do uczniów i nauczycieli. Co roku w programie bierze udział ponad 50 tys. uczniów i ponad 4,5 tys. nauczycieli. W ciągu roku we wszystkich województwach odbywa się ponad 1000 inicjatyw edukacyjnych.

Oprócz tego organizujemy liczne webinaria, szkolenia, konkursy i konferencje wojewódzkie w celu głębszego zainteresowania tematyką i podnoszenia świadomości obywateli w różnych częściach Polski. Liczne inicjatywy edukacyjne, kierowane do różnych grup, organizowane są w ramach corocznych obchodów Dnia Ochrony Danych Osobowych.

Ponadto podczas minionej kadencji odbył się szereg inicjatyw ukierunkowanych na specyfikę pewnych grup. Przykładem jest tegoroczne szkolenie dla Krajowej Izby Radców Prawnych oraz szkolenia z zakresu ochrony danych osobowych dla pracowników Kancelarii Prezesa Rady Ministrów. W 2022 roku uczestniczyliśmy w odprawie szkoleniowej Biura Nadzoru Wewnętrznego MSWiA, podczas której urzędnicy UODO dokonali oceny naruszeń zgłaszanych organowi nadzorczemu przez służby nadzorowane przez Ministra Spraw Wewnętrznych i Administracji. Nasi eksperci uczestniczyli także w szkoleniu dla Dyrektorów Generalnych Służby Cywilnej.

Tych przykładów jest zbyt wiele, aby je wszystkie wymienić. Odbywają się także konferencje online z udziałem ekspertów UODO, które cieszą się bardzo dużym zainteresowaniem internautów. Ponadto wiele informacji przekazujemy przez naszą stronę internetową. Liczne komunikaty mają bowiem bardzo duży walor edukacyjny.

Codziennie odbieramy kilkadziesiąt połączeń telefonicznych i odpowiadamy na wiele pytań osób fizycznych, administratorów czy inspektorów ochrony danych. Dużym zainteresowaniem cieszy się także „Biuletyn UODO", który publikujemy co miesiąc, a obecnie subskrybuje go ponad 9 tys. czytelników i liczba ta stale rośnie, co świadczy, że tworzymy treści wartościowe i potrzebne.

1 ROZMOWA Z EKSPERTEM

Liczne wydarzenia i edukacja społeczeństwa niewątpliwie mają duże znaczenie. A co jeszcze w tej kadencji miało duże znaczenie dla ochrony danych osobowych?

Jednym z ważniejszych elementów, który chciałbym wyróżnić, było zatwierdzenie przeze mnie pierwszego kodeksu postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych i przyznanie pierwszego certyfikatu potwierdzającego akredytację podmiotu monitorującego. To niezwykle ważne wydarzenie nie tylko dlatego, że pierwszy kodeks był długo wyczekiwany, ale dlatego, że przystępowanie przez podmioty medyczne do zatwierdzonego kodeksu zapewni lepszą ochronę danych pacjentów i uporządkuje działania administratorów w tym sektorze. Pamiętajmy, że kodeksy są niezwykle ważnym narzędziem przewidzianym przez RODO. Umożliwiają ustanowienie reguł, które przyczyniają się do właściwego stosowania przepisów ogólnego rozporządzenia o ochronie danych w sposób praktyczny i przejrzysty. Uwzględniają przy tym specyfikę danej branży lub prowadzonych w niej czynności przetwarzania.

Kiedy możemy się spodziewać zatwierdzenia kolejnych kodeksów?

Możemy przypuszczać, że jeszcze w tym roku kolejne kodeksy postępowania zostaną zatwierdzone, ponieważ w przypadku kilku inicjatyw – zostały już złożone wnioski o ich zatwierdzenie. Są to kodeksy przygotowane przez Polską Federację Szpitali, Krajową Izbę Doradców Podatkowych, Organizację Firm Badania Opinii i Rynku, Polską Radę Centrów Handlowych, Sieć Badawczą Łukasiewicz – PORT Polski Ośrodek Rozwoju Technologii, czy kodeks postępowania i dobrych praktyk w zakresie ochrony danych osobowych w działaniach marketingu bezpośredniego Polskiego Stowarzyszenia Marketingu SMB. Oczywiście do zatwierdzenia niezbędne jest wyznaczenie podmiotów monitorujących dla tych kodeksów i ich akredytacja. Trwają też prace nad projektem kodeksu postępowania, który miałby zastosowanie do przetwarzania danych osobowych przez przedsiębiorców prowadzących działalność hotelarską. Nad tą inicjatywą pracuje Izba Gospodarcza Hotelarstwa Polskiego. Działa także obiecująca grupa inspektorów ochrony danych z sektora sądownictwa, która chce uregulować jednolicie czynności przetwarzania w sądach, ale niewchodzące w zakres sprawowania wymiaru sprawiedliwości. Projekt kodeksu branży hotelarskiej jest przygotowywany do konsultacji społecznych. Stan zaawansowania prac pozwala przypuszczać, że w tym roku rozpocznie się postępowanie o jego zatwierdzenie, a może i akredytację podmiotu monitorującego. Trudno natomiast ocenić kiedy dokładnie powstanie projekt kodeksu dla sądownictwa. Autorzy mapują obecnie zagadnienia, które chcą ujednolicić pomiędzy apelacjami. Ale wierzę, że odniosą sukces. Podsumowując, takie doprecyzowanie i ustandaryzowanie przetwarzania danych osobowych czy to w branży hotelarskiej, czy w sektorze sądownictwa niewątpliwie przyczyni się do zapewnienia wyższego poziomu ochrony danych osobowych. Prace nad każdym kodeksem są czasochłonne i wymagają konsultacji. Kodeks musi spełniać określone wymagania. Pamiętajmy, że to nie może być samo powtórzenie przepisów RODO

czy blankietowe rozwiązania. To musi być pogłębiony dokument, który w szczegółach podpowie administratorom, jakie rozwiązania w danej branży należy zastosować, by właściwie chronić przetwarzane przez administratorów dane. Chcę tu dodać, że to, iż prace nad kodeksami idą w dobrym kierunku, to także zasługa zmiany struktury UODO, w ramach której działa Wydział Kodeksów i Certyfikacji.

Funkcjonujemy w dynamicznie zmieniającym się świecie, w którym coraz więcej aspektów wymaga uregulowania, by chronić naszą prywatność. Ponadto są też próby zmiany prawa, które budzą wątpliwości z punktu widzenia naszej prywatności. Jak UODO reagował i reaguje na tą prawno-technologiczną rzeczywistość?

Organ nadzorczy reaguje odpowiednio do swoich kompetencji i zgodnie z obowiązującymi Urząd przepisami prawa. Przede wszystkim Prezes UODO korzysta z przysługujących mu uprawnień na podstawie art. 52 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. A więc, gdy widzi taką potrzebę, to np. występuje do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie lub zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych. W minionej kadencji kilkadziesiąt razy korzystałem z takiej możliwości. Wystąpienia te dotyczyły zagadnień legislacyjnych, które wpływały na ochronę danych osobowych i prywatność dużych grup osób, odnosiły się do wykorzystywania nowoczesnych technologii, w tym do zautomatyzowanego przetwarzania danych, a także przetwarzania szczególnych kategorii danych osobowych, jak np. danych o stanie zdrowia. Warto przypomnieć, że UODO nie posiada inicjatywy ustawodawczej. Ponadto jako organ nadzorczy opiniujemy rocznie ok. 700 aktów prawnych, które dotyczą przetwarzania danych osobowych. Część uwag UODO jest uwzględniana w procesie legislacyjnym, co przekłada się nie tylko na lepszą ochronę prywatności obywateli, ale też na ukształtowanie jasnych zasad, na jakich ich dane są przetwarzane.

Jakie to były zmiany prawne?

Jednym z takich przykładów jest choćby zmiana ustawy o notariacie i postulatu wprowadzenia monitoringu wideo i głosowego w kancelariach notarialnych, do której zgłosiliśmy bardzo wiele uwag. Uwagi zgłaszaliśmy również do projektu ustawy Prawo komunikacji elektronicznej, Prawo bankowe, czy do wielu projektów rozporządzeń. Również do aplikacji ProteGO Safe zgłosiliśmy Ministerstwu Cyfryzacji swoje zastrzeżenia. Wzbudzała nasze zaniepokojenie z uwagi na możliwą ingerencję w prywatność użytkowników. W tym przypadku zakwestionowaliśmy choćby podstawę prawną, na jakiej mają być przetwarzane dane osobowe użytkowników tej aplikacji. Opiniowanie projektów aktów prawnych jest jednym z istotnych zadań organu przyznanych mu mocą przepisów RODO. Są to prawo i obowiązek organu, realizowane w celu ustalania przepisów krajowych spójnych z filozofią RODO. Istotną rolą organu nadzorczego realizowaną m.in. w drodze opiniowania projektów aktów prawnych jest zapewnianie wielu różnym środowiskom wsparcia eksperckiego na etapie

tworzenia oraz stosowania prawa. Wsparcie takie – coraz częściej pozytywnie przyjmowane przez projektodawców – przynosi zamierzone rezultaty, jak zapobieżenie wejściu w życie lub wyeliminowanie z obrotu prawnego przepisów niezgodnych z RODO, tj.: nieprzejrzystych, narażających wykonawców norm – administratorów na naruszanie zasad dotyczących przetwarzania danych osobowych, niezapewniających poszanowania gwarantowanych przez RODO praw osób, których dane są przetwarzane.

wniosek

Część podmiotów pracujących nad nowymi regulacjami prawnymi korzysta z eksperckiego wsparcia organu nadzorczego na bardzo wczesnym etapie działań koncepcyjnych.
Jednym z elementów tego wsparcia jest postulowanie przeprowadzania testu prywatności, zwłaszcza w związku z opiniowaniem projektów przewidujących stosowanie nowoczesnych sposobów przetwarzania danych osobowych na odległość, w rozbudowanych systemach informatycznych, czy przetwarzania szczególnych kategorii danych osobowych. Dzięki temu prawodawcy coraz częściej wykonują analizę ryzyk i ocenę skutków projektowanych rozwiązań dotyczących przetwarzania danych osobowych. Służy to zachowaniu istotnego balansu, tj. poszanowaniu prawa z zakresu ochrony danych osobowych bez uszczerbku dla istotnych celów wprowadzanych regulacji. Jest to pozytywnie oceniana tendencja coraz częstszego dostrzegania przez projektodawcę walorów takiej oceny skutków dla prywatności i jej przeprowadzanie z korzyścią dla podmiotów danych, ale i dla wykonawców norm zgodnych z zasadami RODO.

Dobrym i ciekawym przykładem mogą być długo procedowane przepisy ustawy o badaniach klinicznych stosowanych u ludzi. W tym przypadku projektodawca zgodził się z koniecznością doprecyzowania tworzonych przepisów m.in. w zakresie wyłączeń stosowania przepisów RODO na rzecz jedynie ich ograniczenia, uwzględniając przy tym poszczególne etapy badania klinicznego. W projekcie pojawiły się rozwiązania, które stanowią istotny przykład godzenia praw z zakresu badań klinicznych i ograniczenia praw osób, których dane mają być przetwarzane. Ponadto powyższe ograniczenia zostały przez projektodawcę doprecyzowane w zakresie konkretnego etapu badania klinicznego, jak również uwzględnił on dane osobowe, które nie będą podlegały powyższym ograniczeniom. Dodatkowo po zgłoszonych uwagach projekt uzupełniono o przepisy dotyczące bezpieczeństwa danych. Także w toku prac legislacyjnych dotyczących projektu ustawy o Centralnej Informacji Emerytalnej znaczna część uwag zgłoszonych przez organ nadzorczy w 2019 roku została uwzględniona de facto w nowym projekcie ustawy o Centralnej Informacji Emerytalnej z 2022 roku.

.

Powyższe działania są przykładami na to, że przy tworzeniu prawa możliwe jest wypracowanie norm, kwestii, które wymagają analizy, dyskusji oraz wprowadzenia stosownych zmian, które stanowią pewien balans pomiędzy koniecznością uregulowania określonych zagadnień (celu regulacji) a zachowaniem spójności z przepisami o ochronie danych. Niestety stanowią one niewielką część opiniowanych projektów. Nadal, w opinii organu nadzorczego, jest wiele przepisów oraz kwestii, które wymagają analizy, dyskusji oraz wprowadzenia stosownych zmian.

Jedna z głośniejszych spraw związanych z legislacją dotyczyła badania przez pracodawców pracowników na obecność alkoholu.

Dyskusja wokół tego problemu rozpoczęła się po opublikowaniu stanowiska UODO w tej sprawie. Zostało ono przedstawione w związku z licznymi pytaniami, jakie były kierowane do Urzędu przez administratorów, którzy mieli słuszne wątpliwości. Zwróciliśmy uwagę, że w stanie prawnym, jaki wówczas mieliśmy, nie było podstaw do przeprowadzania takich prewencyjnych kontroli przez pracodawców i przetwarzania pozyskanych wtedy danych. Wskazaliśmy przy tym, jakie w tamtym czasie istniały możliwości prawne, aby nie dopuścić do pracy osoby, co do której istniało podejrzenie, że spożywała alkohol. Mam poczucie, że Urząd w tym temacie zmotywował wiele instytucji i osób do podjęcia rzeczowej dyskusji i wypracowania właściwych rozwiązań, które z jednej strony dawałyby poczucie bezpieczeństwa pracownikom, a z drugiej strony zabezpieczenie dla pracodawców przed zarzutami nadmiarowej ingerencji w prywatność osób poddawanych

zbiorczym i systematycznym badaniom. Od samego początku deklarowaliśmy też projektodawcy naszą gotowość współpracy przy tworzeniu regulacji, które oprócz stworzenia podstawy prawnej do takich kontroli, zapewnią gwarancje bezpieczeństwa dla pracowników, którzy są sprawdzani na obecność alkoholu w organizmie. Od niedawna takie regulacje już obowiązują.

Na koniec nie sposób nie odnieść się do faktu, że koniec Pana pierwszej kadencji zbiega się z piątą rocznicą obowiązywania RODO. Jakie widzi Pan wyzwania na kolejne lata obowiązywania rozporządzenia?

30 kwietnia 2023 roku minęło ćwierć wieku obowiązywania w Polsce przepisów o ochronie danych osobowych. Można więc śmiało powiedzieć, że ogólne rozporządzenie o ochronie danych, które od pięciu lat jest stosowane w polskim porządku prawnym, nie powstało w próżni. RODO bowiem opiera się na podstawowych wartościach istniejącego już w Polsce systemu, utrzymując zasady ochrony danych. Mamy więc ogromne doświadczenie w stosowaniu przepisów prawa o ochronie danych osobowych, które następnie stało się podwaliną obecnego systemu ochrony danych w Unii Europejskiej, przyczyniając się do jego harmonizacji. Wiedza z zakresu ochrony danych osobowych wśród administratorów, podmiotów przetwarzających oraz osób, których dane dotyczą, stale wzrasta. Niemniej jednak, konieczne jest stałe edukowanie społeczeństwa, z uwagi na rozwój technologiczny i związane z nim nowe zagrożenia dla ochrony danych. Ważne jest budowanie świadomości administratorów, podmiotów przetwarzających i wszystkich podmiotów zaangażowanych w proces przetwarzania danych w celu zapewnienia, aby przebiegał on w sposób zgodny z prawem i zapewniający ochronę praw osób, których dane dotyczą. Szybki postęp technologiczny i związane z nim ogromne liczby przetwarzanych informacji, to duże wyzwanie dla Urzędu Ochrony Danych Osobowych. Jako Prezes tego Urzędu, zawsze będę stał po stronie człowieka i jego prawa do ochrony danych osobowych i prywatności.

Dziękuję za rozmowę.

1 ROZMOWA Z EKSPERTEM

ZMIANY NA PLUS

Jakub Groszkowski, Zastępca Prezesa Urzędu Ochrony Danych Osobowych w rozmowie z Adamem Sanockim podsumowuje pięć lat stosowania RODO.

RODO jest z nami od pięciu lat. Co się zmieniło na przestrzeni tych lat?
Bardzo wiele się zmieniło. I to pomimo faktu, że przepisy o ochronie danych osobowych funkcjonują w Polsce od 25 lat, to dopiero za sprawą RODO, czyli ogólnego rozporządzenia o ochronie danych, niektórzy dowiedzieli się, że dane trzeba chronić, a inni – jakie prawa im przysługują. Znacząco wzrosła świadomość obywateli właśnie w zakresie przysługujących im praw. Jest to zauważalne choćby z uwagi na dużą liczbę skarg, jakie trafiają do Urzędu Ochrony Danych Osobowych (UODO). O ile zanim zaczęto stosować RODO skarg do organu nadzorczego (wówczas GIODO, czyli Generalnego Inspektora Ochrony Danych Osobowych) było rocznie mniej niż 3 tys., to kolejne lata przyniosły znaczący ich wzrost, a jego dynamika nastąpiła właśnie po 25 maja 2018 r., kiedy to zaczęliśmy stosować przepisy rozporządzenia. Obecnie obywatele zgłaszają do Urzędu ok. 7–8 tys. skarg rocznie.

Może to nie świadomość w zakresie przysługujących osobom praw, a zniesienie opłaty skarbowej?
To też by świadczyło o tym, że ludzie mają świadomość tego, że zmieniły się przepisy i nie ma już tej opłaty. Jednak opłata ta była symboliczna (10 zł), dlatego raczej to nie jej zniesienie ma tu wpływ, a jeśli nawet to bardzo marginalny. UODO obserwuje, że ta świadomość wśród obywateli stale się zwiększa. I widać to nie tylko po skali skarg, ale i po tym, jak te skargi są formułowane. Obecnie w skargach jest mniej błędów formalnych niż było ich początkowo, jak np. brak podpisu skarżącego czy określenie żądania związanego ze skargą. Dalej te błędy są, ale jest ich mniej. Ponadto przeprowadzone w 2021 roku badanie przez serwis ChronPESEL.pl i Krajowy Rejestr Długów pod patronatem Urzędu Ochrony Danych Osobowych pokazuje, że świadomość na temat ochrony danych jest już dość wysoka. W tym badaniu 84 proc. badanych deklarowało, że wie, jak zadbać o bezpieczeństwo swoich danych. Dużo osób, bo ponad 60 proc. wskazywało też, że wie, jakie działania należy podjąć w przypadku wyłudzenia lub kradzieży danych osobowych.

Oprócz wielu skarg mamy także dużą liczbę zgłaszanych naruszeń ochrony danych osobowych. Czy to Pana niepokoi?
Pamiętajmy, że celem zgłaszania naruszeń Prezesowi UODO w ciągu 72 godzin jest m.in. dokonanie przez organ nadzorczy oceny, czy administrator prawidłowo wypełnił obowiązek zawiadomienia o naruszeniu osób, których dane dotyczą, o ile faktycznie wystąpiła sytuacja, w której ma obowiązek to zrobić, oraz czy podjął odpowiednie działania w celu zminimalizowania ryzyka wystąpienia podobnego naruszenia w przyszłości. I to powoduje, że na samym zgłoszeniu naruszenia się nie kończy, ale na podjęciu konkretnych działań administratora w celu lepszej ochrony danych osobowych, które przetwarza. Tak więc przekłada się to na sukcesywną poprawę ochrony danych.

Trzeba przyznać, że zgłaszanych naruszeń jest jednak dużo. W 2019 roku administratorzy zgłosili ponad 6 tys. naruszeń, w 2020 roku 7,5 tys., a w 2021 roku prawie 13 tys. Należy mieć jednak na uwadze, że niektórzy administratorzy danych zgłaszają naruszenia, w przypadku których nie ma takiego obowiązku i wystarczy je odnotować w wewnętrznym rejestrze. Do UODO trzeba bowiem zgłaszać te naruszenia, w przypadku których istnieje ryzyko naruszenia praw i wolności osób fizycznych, których dane dotyczą, a więc np. ryzyko tzw. kradzieży tożsamości.
Analiza naruszeń pokazuje też, że świadomość administratorów również rośnie. Wiele podmiotów mocno angażuje się nie tylko w identyfikację przyczyn naruszenia, ale i wdrażanie rozwiązań, które mają ograniczać takie przypadki w przyszłości.
Musimy się jednak liczyć z tym, że do naruszeń będzie dochodziło. Często powstają one w wyniku błędu ludzkiego, nawet bardzo prostego, ale zmienia się także technologia, która przynosi nowe zagrożenia. Dlatego RODO wymaga, by ochrona danych osobowych była ciągłym procesem, a nie jednorazowym działaniem. I to administratorzy też coraz częściej rozumieją.

Konieczność zgłaszania naruszeń to nie jedyne obowiązki wynikające z RODO. Wiele z nich od samego początku wzbudzało wielkie emocje i nie spotkało się ze zrozumieniem administratorów, którzy mieli wątpliwości jak stosować nowe obowiązki w praktyce. Czy dziś jest inaczej?

Pod wieloma względami jest dużo lepiej. Owszem, początkowo narosło wiele mitów wokół RODO. Firmy były naciągane na usługi czy produkty, które z samym RODO nie miały wiele wspólnego albo były na wyrost. Administratorzy przed 25 maja 2018 r. mieli bardziej zero-jedynkowe podejście do ochrony danych – dostosowywali się bezpośrednio do treści przepisów, co teoretycznie miało wystarczająco chronić dane. Doskonale było to widoczne choćby na przykładzie wymagań zabezpieczeń technicznych, gdzie minimalny standard określało jedno z rozporządzeń. W praktyce ten minimalny standard szybko przestał odpowiadać potrzebom obywateli. Czyli na papierze wszystko było w porządku, ale w praktyce te minimalne wymogi okazały się być daleko w tyle za rozwojem technologii i nowymi zagrożeniami, które się wraz z nim pojawiły.
Problemem była więc zmiana podejścia administratorów do stosowania przepisów RODO w praktyce. Akt ten wymaga od nich dużej samodzielności w analizie prowadzonych procesów przetwarzania danych. Tego administratorzy musieli się nauczyć. Nie mogli skopiować wszystkich rozwiązań od innego podmiotu, bo każdy z nich mierzył się z innymi ryzykami, na jakie narażone są przetwarzane przez niego dane, inną ich skalą czy retencją.
RODO nie da się wdrożyć raz i na tym poprzestać. Regulacje wymogły na administratorach konieczność ciągłego dostosowywania procedur bezpieczeństwa ochrony danych, ich analizowania i testowania przyjętych rozwiązań technicznych oraz organizacyjnych. O ile wszystkie te zmiany początkowo nie były dla administratorów łatwe, dziś to podejście dla większości z nich jest

Sama zmiana podejścia to jednak nie wszystko. Oprócz RODO w obrocie prawnym są też przepisy branżowe i to w wielu przypadkach powodowało dodatkowe wątpliwości.

W dalszym ciągu wiele regulacji wymaga dostosowania ich do przepisów ogólnego rozporządzenia. Ten brak faktycznie powoduje niepewność u administratorów. Niektóre krajowe regulacje zostały jednak zmienione, rozwiązując część problemów. Administratorzy pomimo tych zmian nadal mają wątpliwości co do stosowania niektórych regulacji w praktyce. Jako przykład mogę podać monitoring wizyjny. Polski ustawodawca postanowił wprowadzić odpowiednie regulacje w Kodeksie pracy czy w ustawach obejmujących działanie samorządów oraz w prawie oświatowym. Jednak i one powodują, że administratorzy nie zawsze są pewni stosowanych przez siebie rozwiązań w tym zakresie. Dlatego organ nadzorczy, odpowiadając na to zapotrzebowanie rynku, przygotowywał odpowiednie wskazówki poruszające te zagadnienia. Oprócz materiałów dotyczących monitoringu powstały także wskazówki dotyczące przetwarzania danych w rekrutacji, w placówkach oświatowych czy podczas kampanii wyborczych, jak i samych wyborów. Również liczne szkolenia dla inspektorów ochrony danych z poszczególnych sektorów pozwalały przybliżyć oraz zrozumieć wiele zagadnień tym, którzy mają z nimi styczność na co dzień.

RODO wprowadziło kary i chyba tego administratorzy obawiają się najbardziej. Czy słusznie?

Nie. Administracyjnych kar pieniężnych, biorąc pod uwagę ilość postępowań prowadzonych przez organ nadzorczy, jest niewiele. Nie sprawdziły się więc scenariusze wieszczone przez niektóre zewnętrzne podmioty, że posypią się wielomilionowe kary. Widmo tych sankcji było pewnym straszakiem, wykorzystywanym do napędzania koniunktury na szkolenia, których jakość nie zawsze była wysoka. Owszem, kary są środkiem, po który Prezes UODO musi niekiedy sięgnąć. Tak się stało w 67 przypadkach, a najwyższej karze nałożonej przez polski organ nadzorczy daleko do maksymalnej, przewidzianej w RODO. Rekordowa kara pieniężna w Polsce za naruszenie przepisów o ochronie danych osobowych wyniosła 4,9 mln zł, a zgodnie z RODO jej górna wysokość może wynieść nawet 20 mln euro lub 4 proc. całkowitego rocznego obrotu firmy z poprzedniego roku. Kary mają nie tylko wymusić na administratorach właściwe postępowanie, znaczenie ma również ich wymiar prewencyjny oraz edukacyjny – i to nie tylko dla tych, którzy zostali ukarani. Inni administratorzy analizują kto i za co dostał karę, po czym modyfikują swoje procesy przetwarzania danych czy zabezpieczenia, gdy widzą, że ich działanie jest podobne, co też może narazić ich na taką odpowiedzialność.

Czyli mobilizują administratorów do działania?

Tak. To widać szczególnie na przykładzie podmiotów, do których organ nadzorczy kieruje pisma i niekiedy pozostają one bez odpowiedzi. RODO pozwala skutecznie reagować w takiej sytuacji, gdyż Prezes UODO ma prawo do nałożenia kary za brak współpracy z organem nadzorczym oraz za nieudzielenie mu informacji niezbędnych do realizacji jego zadań. I ta skuteczność przejawia

się w tym, że w 2022 roku wszczęliśmy 34 postępowania w przedmiocie nałożenia administracyjnej kary pieniężnej i już samo wszczęcie postępowania w 22 przypadkach doprowadziło do podjęcia przez podmioty współpracy z Prezesem UODO. W konsekwencji organ nadzorczy podjął decyzję o odstąpieniu od nałożenia kary i poprzestał na udzieleniu stronom upomnień.

Dużo mówimy o postrzeganiu RODO przez administratorów, a co – poza licznymi skargami – zmieniło się z punktu widzenia obywateli, czyli osób, których dane są przetwarzane przez administratorów zarówno w sektorze publicznym, jak i prywatnym?

Przepisy RODO dały każdemu z nas większą kontrolę nad naszymi danymi osobowymi, m.in. rozszerzając zakres obowiązków informacyjnych i zobowiązując administratorów danych, by komunikowali się z nami w zwięzły, łatwo dostępny i zrozumiały sposób. RODO pozwala na łatwiejszy dostęp do własnych danych. Ułatwia też przenoszenie danych osobowych między usługodawcami. Zmianą na plus jest to, że wszystkie sprawy dotyczące ochrony naszych danych możemy kierować do krajowego organu ochrony danych, nawet gdy są one przetwarzane w innym państwie. Co prawda takie sprawy trafiają do organu ds. ochrony danych osobowych w danym państwie, ale złożenie skargi we własnym kraju to duża wygoda. Przepisy RODO są też stosowane przez przedsiębiorstwa działające poza UE, które oferują swoje usługi obywatelom lub mieszkańcom państw unijnych. Wiele takich podmiotów dostosowało i ciągle dostosowuje swoje usługi do RODO.

Tak zwane prawo do bycia zapomnianych mogło jednak niektórych rozczarować.

Organ nadzorczy od samego początku mówił, że korzystanie z tego prawa będzie obarczone koniecznością spełnienia szeregu warunków. Niestety, ale w mediach utrwalił się bardzo uproszczony przekaz na temat tego prawa, który sugerował, że jak zażądamy usunięcia naszych danych, to administrator automatycznie będzie musiał to zrobić. W praktyce jest inaczej, gdyż dane nie mogą być usunięte choćby wtedy, gdy ich przetwarzania przez administratora wymaga prawo. Żądania takiego nie zrealizuje także administrator, który musi dane nadal przetwarzać do ustalenia, dochodzenia lub obrony roszczeń albo muszą być one przetwarzane do celów archiwalnych. Tymczasem niektórzy byli przekonani, że ich żądanie będzie bezwarunkowo zrealizowane. Niektórych mogło też rozczarować to, że ich dane mogą być przetwarzane bez wyrażania przez nich na to zgody, a na innych podstawach. Często spotykaliśmy się z przekonaniem, że „skoro nie dawałem zgody, to nie można moich danych przetwarzać". Tymczasem w wielu przypadkach administratorzy dysponują do tego inną podstawą. Takie przekonanie u wielu osób mogło się wiązać z tym, że niejednokrotnie administratorzy odbierali zgody na przetwarzanie danych w sytuacji, gdy dysponowali do tego inną podstawą prawną. W ten sposób niejako wprowadzali w błąd osoby, których dane dotyczą, gdyż były one przekonane, że ich dane są przetwarzane na podstawie zgody, którą w dowolnym momencie można wycofać. Przykładem takiej sytuacji jest klauzula zgody w formularzach rekrutacyjnych, która w wielu przypadkach jest błędna. Dane na potrzeby rekrutacji

Pracodawca przetwarza na podstawie przepisów Kodeksu pracy, który podkreśla też taki zakres danych może być do tego celu przetwarzany. Może być oczywiście, że zgoda będzie jednak konieczna, gdy pojawia się dodatkowy cel przetwarzania, jakim jest np. kolejna rekrutacja choćby na inne stanowisko.

Czyli RODO możemy podsumować na plus?

Bez wątpienia. Wzorce z RODO zaczynają funkcjonować także w państwach spoza Unii Europejskiej i to nie tylko dlatego, że podmioty z tych państw kierują swoje usługi czy produkty do mieszkańców Unii. Inne państwa stawiają sobie rozwiązania z RODO za wzór przy tworzeniu własnych regulacji. To, że RODO funkcjonuje – i to coraz lepiej – nie oznacza, że można poprzestać tylko na egzekwowaniu tego prawa. W dalszym ciągu trzeba działać także na polu edukacyjnym. Dlatego UODO nie ustaje w swoich licznych działaniach, co widać na przykładzie choćby programu edukacyjnego „Twoje dane – Twoja sprawa". Odbywa się też wiele szkoleń czy konferencji, które dostępne są online. Powstają także liczne materiały informacyjne na stronie internetowej Urzędu, które również mają charakter edukacyjny. Takie działania w dalszym ciągu będziemy wspierać i je rozwijać.

Dziękuję za rozmowę.

MOŻLIWOŚĆ PEŁNIENIA FUNKCJI IOD PRZEZ KOMPLEMENTARIUSZA SPÓŁKI KOMANDYTOWEJ

Komplementariusz, gdy jest jednocześnie wspólnikiem spółki komandytowej i osobą reprezentującą tę spółkę zgodnie z umową spółki komandytowej, czyli prowadzi sprawy spółki (kieruje jej działalnością) i decyduje o celach i sposobach przetwarzania danych osobowych, nie może równolegle zajmować stanowiska inspektora ochrony danych.

Zgodnie z art. 102 ustawy z 15 września 2000 r. – Kodeks spółek handlowych (ksh) spółką komandytową jest spółka osobowa mającą na celu prowadzenie przedsiębiorstwa pod własną firmą, w której wobec wierzycieli za zobowiązania spółki co najmniej jeden wspólnik odpowiada bez ograniczenia (komplementariusz), a odpowiedzialność co najmniej jednego wspólnika (komandytariusza) jest ograniczona. Komandytariusz (stosownie do art. 121 §1 ksh) nie ma prawa ani obowiązku prowadzenia spraw spółki, chyba że umowa spółki stanowi inaczej. Zgodnie natomiast z art. 117 ksh, spółkę reprezentują komplementariusze, których z mocy umowy spółki albo prawomocnego orzeczenia sądu nie pozbawiono prawa reprezentowania spółki. Zatem zasadą jest prowadzenie spraw spółki przez komplementariusza i reprezentowanie jej przez niego.
Tym samym komplementariusz jako wspólnik spółki komandytowej i osoba reprezentująca tę spółkę zgodnie z umową spółki komandytowej, tj. prowadząca sprawy spółki (odpowiadająca za jej zobowiązania całym swoim majątkiem osobistym i kierująca jej działalnością), nie może jednocześnie pełnić funkcji inspektora ochrony danych. Prowadziłoby to bowiem do sytuacji, w której IOD oceniałby i monitorował samego siebie.
Organ nadzorczy wielokrotnie wskazywał, że z tego właśnie powodu niedopuszczalne jest powołanie na IOD osoby będącej kierownikiem (zarządzającym) podmiotem posiadającym status administratora lub podmiotu przetwarzającego, przykładowo: członka zarządu stowarzyszenia, dyrektora szkoły, wójta, członka zarządu spółki. Zgodnie z art. 38 ust. 3 RODO, IOD ma podlegać bezpośrednio najwyższemu kierownictwu administratora lub podmiotu przetwarzającego, nie zaś być członkiem organu zarządzającego tym podmiotem.
Natomiast w sytuacji, gdy komplementariusz spółki komandytowej nie jest uprawniony do jej reprezentowania (patrz art. 117 ksh) należałoby ocenić, czy fakt bycia wspólnikiem, który zawierając umowę spółki komandytowej decyduje o przedmiocie jej działalności, i jednocześnie komplementariuszem, który zgodnie z art. 102 ksh ponosi pełną odpowiedzialność wobec wierzycieli za zobowiązania spółki, wyklucza możliwość pełnienia funkcji IOD w tej spółce komandytowej. Wydaje się, że konieczna będzie w takich okolicznościach analiza treści umowy spółki komandytowej i ustalenie m.in., czy taki komplementariusz, jako członek władz spółki, może decydować o celach i sposobach przetwarzania danych osobowych.

2 UODO SYGNALIZUJE

STATUS BANKU TKANEK I KOMÓREK

Choć banki tkanek i komórek działają w strukturach uczelni wyższych, to same ustalają cele i sposoby przetwarzania danych osobowych związane z gromadzeniem, przetwarzaniem czy przechowywaniem tkanek i komórek, dlatego też pełnią funkcję administratorów w rozumieniu RODO.

IOD jednej z uczelni wyższych zwrócił się do UODO z prośbą o pomoc w ustaleniu statusu banków tkanek i komórek (BTiK). Jak wskazał, funkcjonują one w strukturach organizacyjnych uczelni wyższych i są powoływane decyzjami ministra zdrowia na podstawie przepisów ustawy z 1 lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów (dalej jako ustawa transplantacyjna) oraz ustawy z 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. Nadzorującym je właściwym organem ministra zdrowia jest Krajowe Centrum Bankowania Tkanek i Komórek, które prowadzi m.in. na swojej stronie internetowej ogólnodostępny rejestr powołanych BTiK. Jednocześnie BTiK są jednostkami organizacyjnymi uczelni wyższych. Nie pobierają tkanek i komórek bezpośrednio od pacjentów, ponieważ nie są podmiotami leczniczymi. Najczęściej wykonują usługę dla podmiotów trzecich, którymi mogą być: szpitale, inne banki tkanek i komórek, wytwórnie farmaceutyczne lub sponsorzy badań klinicznych wskazujący wytwórnię farmaceutyczną. Na ogół również w przypadku BTiK działających w strukturach uczelni decyzja ministra zdrowia obejmuje pozwolenie na dwa procesy występujące niezwłocznie po sobie: gromadzenie i dopuszczenie do obiegu. Ponadto wraz z tkankami i komórkami do uczelnianych BTiK zgodnie z ustawą transplantacyjną jest przekazywana dokumentacja medyczna pacjenta (dane go identyfikujące oraz m.in. wyniki badań diagnostycznych, wyniki badań antygenów zgodności tkankowych).

2 UODO SYGNALIZUJE

Biorąc pod uwagę powyższe regulacje oraz przepisy ustawy z 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce, które określają, co należy do głównych zadań uczelni wyższych, IOD spytał UODO, kogo należy uznać za administratora. W odpowiedzi Urząd przypomniał, że aby określić status podmiotu w procesie przetwarzania danych osobowych należy kierować się definicjami administratora i podmiotu przetwarzającego zawartymi w RODO (wyjaśnionymi w Wytycznych EROD 7/2020 dotyczących pojęć administratora i podmiotu przetwarzającego na gruncie RODO). UODO zaznaczył, że należy również wziąć pod uwagę przepisy wskazujące zadania określonego podmiotu i zakres jego odpowiedzialności za ich realizację, a jednocześnie stanowiące podstawę uprawniającą go do przetwarzania na te potrzeby danych osobowych.

Sposób utworzenia

Za uznaniem BTiK jako odrębnego administratora przemawia już sam sposób utworzenia tego podmiotu na podstawie ustawy transplantacyjnej. W myśl art. 27 ust. 5 ustawy, udzielenie pozwolenia, odmowa udzielenia pozwolenia oraz cofnięcie pozwolenia, o którym mowa w art. 26 ust. 2 ustawy transplantacyjnej, czyli pozwolenia na wykonywanie czynności, o których mowa w art. 25, następuje w drodze decyzji administracyjnej. Jej adresatem jest jednostka organizacyjna zwana „wnioskodawcą". Z zamieszczonego na stronie internetowej Krajowego Centrum Bankowania Tkanek i Komórek dokumentu „Wniosek o uzyskanie pozwolenia Ministra Zdrowia na wykonywanie czynności, o których mowa w art. 25 w ramach działalności banku tkanek i komórek" wynika przy tym, że ustawodawca wprost przewidział, iż stroną postępowania o udzielenie pozwolenia, o którym mowa w art. 25 ustawy transplantacyjnej, może być BTiK pozostający w strukturze innego podmiotu.

Uprawnienia i zadania wynikające z przepisów ustawy transplantacyjnej

Z przepisów ustawy transplantacyjnej można wywnioskować, że BTiK cechuje określona autonomia w podejmowaniu decyzji związanych z ustalaniem celów i sposobów przetwarzania danych osobowych. Przepisy te określają bowiem dokładne zasady, które musi spełnić jednostka organizacyjna, aby mogła wykonywać czynności związane z gromadzeniem, przetwarzaniem, czy przechowywaniem tkanek i komórek (dokładne czynności określa art. 25 ustawy), a także wskazują nadzór właściwego ministra do spraw zdrowia nad tą działalnością (art. 26 i nast.). Ponadto na BTiK nałożono obowiązek opracowania i wdrożenia systemu zapewniającego jakość, który ma określać w szczególności sposób monitorowania stanu tkanek i komórek w drodze między dawcą a biorcą oraz wszelkich wyrobów medycznych i materiałów mających bezpośrednio kontakt z tymi tkankami i komórkami (art. 29 ust. 1 ustawy). System zapewnienia jakości obejmuje w szczególności takie dokumenty, jak: standardowe procedury operacyjne, wytyczne, instrukcje postępowania, formularze sprawozdawcze, karty dawców, informacje w sprawie miejsca

przeznaczenia tkanek lub komórek (art. 29 ust. 2). Wszystko to wiąże się z autonomią w podejmowaniu decyzji co do stworzenia takiego systemu, obejmującego również zasady przetwarzania danych osobowych. Przepisy wskazują, że BTiK zawierają pisemne umowy o współpracy w określonym zakresie z podmiotem, którego działalność wpływa na jakość i bezpieczeństwo tkanek i komórek przetworzonych we współpracy z tym podmiotem, więc to BTiK jest obowiązany zweryfikować przestrzeganie przez taki podmiot wymagań określonych w przepisach ww. ustawy oraz określonych w systemie zapewnienia jakości (art. 31 ustawy). Wreszcie przepisy ustawy transplantacyjnej określają obowiązki BTiK w zakresie gromadzenia i przechowywania dokumentacji tkanek i komórek oraz przekazywania do Krajowego Centrum Bankowania Tkanek i Komórek rocznych raportów dotyczących podejmowanych czynności (art. 34 i nast.). BTiK jest obowiązany prowadzić, gromadzić i przechowywać dokumentację dotyczącą podejmowanych czynności dotyczących tkanek i komórek przez okres 30 lat od dnia wydania tkanek lub komórek w celu przeszczepienia lub zastosowania u ludzi, w sposób umożliwiający identyfikację dawców i biorców tkanek lub komórek (art. 34 ust. 1).

wniosek

To nie uczelnia wyższa, w której strukturach funkcjonuje BTiK, ustala cele i sposoby przetwarzania danych osobowych związane z gromadzeniem, przetwarzaniem, czy przechowywaniem tkanek i komórek, lecz robią to właśnie BTiK. Właściwe decyzje co do zapewnienia odpowiednich środków technicznych i organizacyjnych dotyczące chociażby działania wspomnianego systemu jakości, również podejmowane są przez kierownika BTiK. A zatem można uznać, że to BTiK są administratorami w rozumieniu RODO.

MONITORING WIZYJNY W CZASIE RZECZYWISTYM MUSI BYĆ ZGODNY Z RODO

Analiza przepisów RODO, wskazówki EROD, a także wydawane przez organ nadzorczy decyzje i orzecznictwo nie pozostawiają wątpliwości, że monitoring wizyjny prowadzony w czasie rzeczywistym podlega zasadom określonym w RODO.

Jeśli przy stosowaniu monitoringu wizyjnego służącego wyłącznie do podglądu na żywo ochranianych miejsc (tj. monitoringu w czasie rzeczywistym, przy korzystaniu z którego nie nagrywamy obrazu, a jedynie na bieżąco prowadzimy obserwację na monitorze) mamy możliwość zidentyfikowania obserwowanych osób, to uznać należy, że dochodzi do przetwarzania danych osobowych, które powinno być prowadzone z poszanowaniem zasad określonych w RODO.

Definicje z RODO

Wniosek taki wysnuć można już na podstawie analizy definicji podstawowych pojęć zawartych w art. 4 RODO. Zgodnie z nimi dane osobowe to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Przy czym możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań. Z kolei przetwarzanie oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Zatem biorąc pod uwagę powyższe definicje oraz to, że przy podglądzie na żywo obraz z kamer jest przesyłany do monitora osoby prowadzącej obserwację, uznać należy, że dochodzi do przetwarzania danych osobowych w rozumieniu RODO. Nawet jeśli jest ono tymczasowe i krótkotrwałe. Mogą też zdarzać się rozwiązania, w których zapis z kamer – mimo że nie jest utrwalany np. na dysku twardym – to jednak pozostaje w urządzeniu.

Warto w tym kontekście zaznaczyć, że w przypadku przesyłania danych (obrazu) pomiędzy urządzeniami, co jest istotą monitoringu, może dochodzić również do przechwycenia transmisji, co dodatkowo wpływa na ryzyko naruszenia praw i wolności osób obserwowanych. Należy zatem przyjąć i wdrożyć odpowiednie zabezpieczenia dla takiego procesu przetwarzania.

Powyższe argumenty przesądzają, że stosowanie monitoringu wizyjnego w czasie rzeczywistym musi odbywać się z poszanowaniem zasad określonych w RODO.

2 UODO SYGNALIZUJE

Wytyczne EROD

Także informacje zawarte w Wytycznych EROD 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo (wersja 2.0 przyjęta 29 stycznia 2020 r. i opublikowana na **stronie internetowej UODO**) wskazują, że monitoring bez zapisu stanowi formę przetwarzania danych osobowych, przez co podlega postanowieniom RODO.

Jak czytamy w ust. 92 dotyczącym prawa dostępu do danych, „W przypadku monitoringu wizyjnego oznacza to, że jeżeli nie przechowuje się ani nie przesyła żadnych danych po zakończeniu okresu, w którym miało miejsce monitorowanie w czasie rzeczywistym, administrator mógłby jedynie przekazać informację o tym, że nie są już przetwarzane żadne dane osobowe (oprócz ogólnych obowiązków informacyjnych, określonych w art. 13, zob. sekcja 7, Przejrzystość i obowiązki informacyjne)". Jednocześnie EROD w powołanych wytycznych wskazuje (ust. 29), że: „Monitoring w czasie rzeczywistym może być czasem bardziej inwazyjny niż przechowywanie i automatyczne usuwanie nagrań po upływie określonego terminu (np. jeżeli ktoś nieustannie spogląda na monitor, może to być podejście o wiele bardziej inwazyjne niż w przypadku braku jakiegokolwiek monitora i przechowywania nagrań bezpośrednio w „czarnej skrzynce"). W tym kontekście należy uwzględnić zasadę minimalizacji danych (art. 5 ust. 1 lit. c). Należy również pamiętać, że zamiast korzystania z monitoringu wizyjnego administrator może skorzystać z usług personelu ochrony, który jest w stanie natychmiast zareagować i zainterweniować".

Szkolenia i decyzje organu oraz wyroki

To, że prowadzenie monitoringu w czasie rzeczywistym – tak jak inne formy monitoringu wizyjnego – podlega zasadom określonym w RODO, przedstawiciele UODO wyjaśniali m.in. podczas prowadzonego w 2019 r. **szkolenia dla IOD.**
Jednocześnie stanowisko takie znajduje potwierdzenie w wydawanych przez organ decyzjach. W jednej z nich (znak: DS.523.189.2020) Prezes UODO dokonał m.in. oceny stosowania przez firmę wideodomofonu w celu identyfikacji, a następnie weryfikacji uprawnienia do wejścia na teren budynku. Wskazał, że za jego pośrednictwem dokonywana była krótkotrwała komunikacja (również za pomocą podglądu wizyjnego) – obraz z kamery przesyłany był bowiem na ekran recepcjonisty. Po analizie wszystkich okoliczności sprawy organ nadzorczy uznał, że przetwarzanie danych osobowych skarżącego za pomocą wideodomofonu nie naruszało jego praw i wolności i było prowadzone na podstawie art. 6 ust. 1 lit. f RODO, tj. ze względu na prawnie uzasadniony interes administratora polegający na kontroli dostępu do siedziby firmy.
Takie podejście do prowadzenia monitoringu w czasie rzeczywistym z wykorzystaniem wideodomofonu potwierdził Wojewódzki Sąd Administracyjny w Warszawie w wyroku z 12 października 2022 r. (sygn. akt II SA/Wa 153/22).

SPORTOWCY CHCĄ MIEĆ KODEKS POSTĘPOWANIA

Instytut Sportu – Państwowy Instytut Badawczy poinformował UODO o oddolnej inicjatywie polskich związków sportowych mającej na celu opracowanie Kodeksu postępowania w zakresie ochrony danych osobowych dla branży sportowej.

W odpowiedzi na prośbę Izby Gospodarczej Hotelarstwa Polskiego (IGHP) w siedzibie Urzędu Ochrony Danych Osobowych 21 lutego 2023 r. odbyło się spotkanie dotyczące projektu kodeksu postępowania dla branży hotelarskiej, nad którym pracuje IGHP.
Z przesłanego do UODO pisma wynika, że zawiązała się koalicja związków sportowych oraz środowisk okołobranżowych, która ma za zadanie wypracować projekt kodeksu postępowania w zakresie ochrony danych osobowych dla branży sportowej.

Inicjatorzy deklarują, że dokument ten powstanie we współpracy polskich związków sportowych, organizacji sektora sportowego i strony publicznej. Prace koordynować ma Instytut Sportu – Państwowy Instytut Badawczy.
W założeniu kodeks doprecyzować ma konkretne kwestie związane z przetwarzaniem danych osobowych w sektorze sportu, m.in. takie jak: licencjonowanie, rejestracja zawodników, transfery (w tym także do państw trzecich), organizacja zawodów, turniejów, zgrupowań, wykorzystanie danych biometrycznych w rozwoju sportu oraz prowadzenie stosownych rejestrów. W kodeksie zawarte mają zostać także wzory stosownych dokumentów, formularzy, umów, rejestrów, których przygotowywanie podmiotom sportowym obecnie nierzadko przysparza poważnych problemów. Zatwierdzony kodeks ma być gwarancją pewności stosowania określonych w nim rozwiązań i źródłem wiedzy na temat postępowania z danymi osobowymi w konkretnych sytuacjach, przede wszystkim dla zawodników, trenerów, instruktorów, sędziów, kibiców, wolontariuszy, działaczy, rodziców/opiekunów prawnych dzieci uprawiających sport, szeroko pojętej administracji sportowej, kadry sportowej, podmiotów medycznych czy ubezpieczeniowych, a także sponsorów i partnerów. Dodatkowo środowiska te będą mogły liczyć na podwyższony standard ochrony danych oraz właściwą realizację ich praw.

OCHRONA DANYCH OSOBOWYCH JEST ISTOTNA TAKŻE PRZY MASOWYM WYSYŁANIU E-MAILI

Jeżeli administrator wysyła korespondencję do większej liczby adresatów, powinien zadbać o to, aby każda z osób, do której skierowana jest tego typu korespondencja, nie miała możliwości zapoznawania się z danymi pozostałych odbiorców wiadomości, np. imionami, nazwiskami, ale również adresami e-mail.

Jedną z praktyk, która może prowadzić do naruszenia bezpieczeństwa danych w korespondencji elektronicznej jest nieukrywanie w wysyłkach masowych poszczególnych odbiorców. Przekonał się o tym jeden z administratorów z sektora publicznego, którego Prezes UODO upomniał za sposób prowadzenia masowej korespondencji.

Prowadzenie korespondencji seryjnej musi być zgodne z RODO

Chodzi o sprawię ze skargi na nieprawidłowości w procesie przetwarzania danych osobowych skarżącego, który domagał się zaprzestania udostępniania w korespondencji seryjnej w kopii otwartej nieupoważnionym osobom trzecim jego danych osobowych w zakresie adresu e-mail. Sprawa dotyczyła administratora reprezentującego sektor publiczny, a dane osobowe przetwarzane były w związku z realizacją zadań publicznych własnych oraz zleconych, wynikających z przepisów prawa. Jak wykazało postępowanie przed organem nadzorczym administrator ten udostępnił dane osobowe skarżącego w zakresie adresu e-mail w wiadomościach przesyłanych pocztą elektroniczną jako korespondencja seryjna w kopii otwartej. Taką praktykę stosował jeden z podległych administratorowi referatów w celu przesyłania informacji obejmujących cztery kategorie spraw:

- najczęściej zadawanych pytań nawiązujących do prowadzenia zleconego zadania,
- zmian w przepisach prawa,
- zasad obsługi wykonawców w pandemii oraz
- przypomnień o ogłoszeniach umieszczanych w BIP tego administratora.

Przetwarzanie danych tylko gdy to konieczne i w bezpiecznych warunkach

W ocenie organu udostępnienie danych osobowych w zakresie adresu e-mail nieuprawnionym osobom trzecim w ww. celach, nie było niezbędne do ich realizacji i nie znajdowało oparcia w żadnej z przesłanek legalizujących proces przetwarzania danych osobowych, spośród określonych w art. 6 ust. 1 RODO. W szczególności skarżący nie wyraził zgody na powyższe udostępnienie (art. 6 ust. 1 lit. a), udostępnienie to nie było niezbędne do wykonania umowy, której stroną był skarżący lub do podjęcia na jego żądanie działań przed zawarciem umowy (art. 6 ust. 1 lit. b). Udostępnienie to nie było także niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c), jak również do ochrony żywotnych interesów skarżącego lub innej osoby fizycznej (art. 6 ust. 1 lit. d). Nie było ponadto niezbędne

do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 6 ust. 1 lit. e), a także do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem (art. 6 ust. 1 lit. f). Ponadto opisane działania administratora nastąpiły z naruszeniem zasady minimalizacji (art. 5 ust. 1 lit. c RODO) oraz zasady poufności danych (art. 5 ust. 1 lit. f RODO).

wniosek

Na administratorze danych osobowych, którym w rozumieniu art. 4 pkt 7 RODO ciąży obowiązek prawny przetwarzania danych osobowych zgodnie z obowiązującymi przepisami, a w szczególności obowiązek zapewnienia by przetwarzanie odbywało się na podstawie co najmniej jednej z enumeratywnie wymienionych przesłanek art. 6 ust. 1 RODO. Ponadto zgodnie z zasadą minimalizacji, o której mowa w art. 5 ust. 1 lit. c RODO, przetwarzane dane powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.
Natomiast art. 5 ust. 1 lit. f RODO nakłada na administratora danych obowiązek przetwarzania danych osobowych zgodnie z zasadą integralności i poufności. Oznacza to, że administrator powinien zapewnić odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.
Zgodnie z art. 24 ust. 1 RODO zdanie pierwsze, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO i aby móc je wykazać

Zdaniem organu nadzorczego w tym przypadku udostępnienie adresu e-mail skarżącego osobom trzecim nie było niezbędne do realizacji celu udzielenia informacji dotyczących bieżącej pracy komórki organizacyjnej u tego administratora, zaś proces przetwarzania danych osobowych skarżącego nie był prowadzony przez tego administratora w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem (integralność i poufność). W rezultacie omawiane postępowanie zakończyło się tym, że Prezes UODO wydał decyzję, w której upomniał administratora jako podmiot decydujący o celach i sposobach przetwarzania danych w zakresie stwierdzonego naruszenia przepisów art. 6 ust. 1 RODO z uwagi na udostępnienie danych osobowych skarżącego na rzecz nieuprawnionych osób trzecich.

4 NARUSZENIA I KONTROLE

IM WIĘCEJ WIEMY O RODZAJACH NARUSZEŃ, TYM ŁATWIEJ PRZECIWDZIAŁAĆ IM W PRZYSZŁOŚCI

W dobie cyfryzacji i rosnącej liczby incydentów skutkujących naruszeniami ochrony danych osobowych zarówno administratorzy danych, jak i organy odpowiedzialne za ich ochronę muszą być dobrze przygotowane do rozpoznawania i przeciwdziałania takim zagrożeniom. Zrozumienie charakteru poszczególnych rodzajów naruszeń stanowi klucz do skutecznej reakcji na tego typu zdarzenia oraz pozwala na lepsze zabezpieczenie interesów osób, których dane dotyczą.

Poniżej omówione zostaną trzy podstawowe rodzaje naruszeń: poufności, integralności i dostępności danych. Podział ten pochodzi ze znanego w teorii bezpieczeństwa informacji modelu zwanego „triadą CIA" (ang. Confidentiality, Integrity, Availability), pierwotnie zaproponowanego w odniesieniu do naruszeń ochrony danych osobowych przez Grupę Roboczą Art. 29 w opinii 03/2014 na temat powiadamiania o przypadkach naruszeń danych osobowych oraz przedstawionego przez EROD w ramach najnowszych Wytycznych 9/2022 w sprawie zgłaszania naruszeń ochrony danych osobowych zgodnie z RODO – wersja 2.0 (Guidelines 9/2022 on personal data breach notification under GDPR – version 2.0).

Naruszenia poufności danych

Naruszenie poufności ma miejsce w przypadku nieuprawnionego lub przypadkowego ujawnienia lub dostępu do danych osobowych, czyli wtedy, gdy dane osobowe trafiają w niepowołane ręce. Konsekwencją naruszenia poufności może być m.in. nielegalne wykorzystanie danych (np. w celach marketingowych) czy kradzież tożsamości. Przykładem takiego naruszenia jest sytuacja, w której pracownik przez pomyłkę wysyła e-mail z załącznikiem zawierającym dane osobowe klienta do niewłaściwego odbiorcy. Wdrożenie odpowiedniej polityki bezpieczeństwa informacji, uwzględniającej m.in. obowiązek szyfrowania przesyłanych danych, a także monitorowanie

aktywności pracowników oraz ich regularne szkolenie to istotne elementy sprawnego systemu ochrony danych osobowych, które mogą skutecznie zmniejszyć ryzyko wystąpienia podobnych zdarzeń.

Naruszenia integralności danych

Naruszenie integralności występuje, gdy dane osobowe ulegają nieautoryzowanej lub przypadkowej modyfikacji, która skutkować może m.in. podjęciem przez administratora niewłaściwych działań opartych na nieprawdziwych informacjach. Przykładowo do naruszenia o takim charakterze dochodzi, kiedy skrypt złośliwego oprogramowania zmienia dane klientów zgromadzone w systemie informatycznym. W celu zminimalizowania ryzyka wystąpienia naruszeń integralności danych warto zastosować środki bezpieczeństwa w postaci restrykcyjnej kontroli dostępu do poszczególnych systemów oraz mechanizmów weryfikacji przetwarzanych danych, śledzenia wszelkich zmian i identyfikacji osób, które je wprowadzają.

Naruszenia dostępności danych

O naruszeniu dostępności mówimy, gdy autoryzowany dostęp do informacji zostaje utrudniony lub uniemożliwiony, co doprowadzić może m.in. do zakłócenia działania organizacji oraz nieosiągalności niektórych świadczonych przez nią usług. Za przykład takiego naruszenia może posłużyć zdarzenie, w ramach którego placówka medyczna pada ofiarą ataku hakerskiego typu ransomware, skutkującego zablokowaniem dostępu do danych pacjentów i przeszkodzeniem w udzieleniu im niezbędnej pomocy medycznej. Aby ochronić dane osobowe przed naruszeniem dostępności administratorzy powinni rozważyć wdrożenie adekwatnych rozwiązań prewencyjnych, wśród których warto wskazać m.in. regularne tworzenie i testowanie kopii zapasowych, czuwanie nad aktualnością software'u oraz stosowanie zabezpieczeń chroniących przed złośliwym oprogramowaniem. Ważnym elementem dbania o dostępność danych jest również przygotowanie procedur skutecznego ich odtwarzania, pozwalających szybko przywrócić normalne funkcjonowanie organizacji w razie wystąpienia naruszenia.

wniosek

Świadomość istnienia różnych rodzajów naruszeń ochrony danych osobowych oraz zrozumienie konsekwencji, jakie mogą one za sobą pociągać, jest kluczowe dla zapewnienia skutecznej ochrony danych w każdej organizacji. Inwestowanie w rozwój kompetencji pracowników, staranne uwzględnianie aspektów poufności, integralności i dostępności danych w procesie opracowywania i wdrażania polityk bezpieczeństwa informacji oraz stosowanie odpowiednich technologii zabezpieczających to fundamenty skutecznej ochrony danych osobowych, pozwalające przygotować się na ewentualne incydenty oraz umożliwiające szybką i efektywną reakcję na występujące naruszenia.

4 NARUSZENIA I KONTROLE

Jeden incydent, wiele naruszeń

Zdarzają się sytuacje, gdy w wyniku jednego incydentu dochodzi do naruszenia dwóch lub wszystkich trzech atrybutów bezpieczeństwa informacji, co świadczy o wadze kompleksowego podejścia do ochrony danych.

Przykładowo organizacja może stać się celem ataku cyberprzestępców, którzy włamują się do systemu informatycznego, kradną dane osobowe, modyfikują je według własnych potrzeb, a następnie blokują do nich dostęp.
Takie wydarzenia pokazują, jak istotne jest wdrożenie środków ochrony danych osobowych, które uwzględniają wszystkie trzy rodzaje naruszeń, a także podkreślają potrzebę nieustannej weryfikacji i aktualizacji polityk bezpieczeństwa informacji w celu sprostania dynamicznemu i wciąż zmieniającemu się środowisku zagrożeń.

Dzień Dziecka z UODO!

Z Rodusiem chronimy dane osobowe

1 czerwca 2023, godz. 10:00-10:45

Zapraszamy na e-lekcję uczniów kl. 1-3 szkół podstawowych

Szczegóły na www.uodo.gov.pl

GDY SYSTEM SI WYKORZYSTUJE DANE OSOBOWE, ADMINISTRATOR MUSI PAMIĘTAĆ O RODO

Niezwykle istotne jest, aby algorytmy i systemy sztucznej inteligencji (SI) zapewniały wysoki poziom bezpieczeństwa użytkowników, przetwarzając ich dane na podstawie przepisów prawa oraz zgodnie z zasadami określonymi w ogólnym rozporządzeniu o ochronie danych (RODO).

Sztuczna inteligencja coraz śmielej wkracza w różne obszary życia, a jej rozwój bazuje na ogromnej liczbie danych, w tym danych osobowych. Ponadto skutki rozwoju tej technologii mają zarówno wymiar prawny, społeczny, jak i etyczny. Sztuczna inteligencja może być różnie rozumiana.

Warto zapamiętać!

Dostrzegając duże zainteresowanie tą tematyką, Urząd Ochrony Danych Osobowych od lat stara się zwiększać świadomość społeczną w obszarze cyfryzacji na temat zagrożeń, możliwości oraz praw przysługujących każdej osobie w związku z przetwarzaniem jej danych osobowych i przywiązuje dużą wagę do regulacji prawnych w tym zakresie. Kwestia projektowania systemów sztucznej inteligencji (SI) zgodnych z RODO została poruszona m.in. podczas webinarium pt. „Projektowanie systemów SI zgodnych z RODO", zorganizowanym przez UODO w listopadzie 2022 roku. Eksperci omówili wówczas kluczowe zasady wynikające z unijnego projektu ws. sztucznej inteligencji w odniesieniu do RODO m.in. w kontekście podejścia opartego na ryzyku czy zasad etycznych dotyczących SI zgodnych z zasadami przetwarzania danych osobowych.

Podejmowane są próby wypracowania normatywnej definicji tego pojęcia. W projekcie rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji i zmieniające niektóre akty ustawodawcze Unii (dalej: akt o sztucznej inteligencji) systemy SI definiowane są jako oprogramowanie opracowane przy wykorzystaniu określonych technik i podejść, które może dla danego zestawu celów określonych przez człowieka generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję. Z kolei według rekomendacji OECD dotyczącej sztucznej inteligencji z 2019 roku są to systemy oparte na koncepcji maszyny, która może przewidywać, rekomendować i podejmować decyzje mające wpływ na środowisko rzeczywiste lub wirtualne.

Przetwarzania danych osobowych a SI

Ważne jest, aby jej rozwój z wykorzystaniem SI odbywał się z poszanowaniem prawa do prywatności i ochrony danych. Sztuczna inteligencja ma bardzo szerokie zastosowanie. SI jest wykorzystywana m.in. w medycynie, transporcie, przemyśle, czy w sektorze finansowym, np. do oceny zdolności

kredytowej (więcej w opracowaniu pt. „Sztuczna inteligencja w kontekście ochrony danych osobowych – materiały pokonferencyjne" dostępnym na www.archiwum.uodo.gov.pl).

Przedstawiciel Departamentu Nowych Technologii w swoim wystąpieniu podkreślał wówczas jak ważne jest podejście oparte na ryzyku i przeprowadzenie oceny skutków dla ochrony danych w systemach sztucznej inteligencji. W jego opinii „administratorzy chcąc użytkować dane rozwiązanie techniczne np. ChatGPT, Bing, Google Bard, Chatsonic i inne, powinni przeprowadzić ochronę skutków przed rozpoczęciem procesu przetwarzania w systemach sztucznej inteligencji. Pomocne w jej dokonaniu mogą być w szczególności normy międzynarodowe PN ISO/IEC 29134 – ocena skutków dla prywatności/Information technology — Security techniques – Guidelines for privacy impact assessment, ISO/IEC27001, ISO/IEC 27002, czy ISO/IEC 27701 na potrzeby zarządzania systemem bezpieczeństwa informacjami w zakresie prywatności".

Jeżeli przetwarzanie danych osobowych z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, konieczne będzie przeprowadzenie oceny skutków w kontekście ochrony danych osobowych.

Zagrożenia dla ochrony danych związane z SI

Postęp technologiczny z wykorzystaniem sztucznej inteligencji stwarza bardzo dużo możliwości i korzyści, jednak może pociągać za sobą również zagrożenia dla podstawowych praw, wolności i praworządności, dlatego dla lepszego wykorzystania możliwości SI Komisja Europejska zaproponowała przepisy regulujące funkcjonowanie sztucznej inteligencji, które będą ukierunkowane na człowieka (akt o sztucznej inteligencji). Ponadto w celu zapewnienia odpowiedniego stopnia ochrony praw człowieka w dobie rozwoju narzędzi opartych o systemy sztucznej inteligencji Komitet Rady Europy do spraw Sztucznej Inteligencji opublikował „zerowy" projekt Konwencji w sprawie sztucznej inteligencji, praw człowieka, demokracji i praworządności.

6 SPRAWY MIĘDZYNARODOWE

TSUE: LEKCJE ONLINE PODLEGAJĄ RODO

Jak orzekł 30 marca 2023 r. Trybunał Sprawiedliwości UE transmitowanie na żywo w formie wideokonferencji publicznego nauczania szkolnego podlega RODO.

Dwoma aktami przyjętymi w 2020 roku minister edukacji kraju związkowego Hesja (Niemcy) określił ramy prawne i organizacyjne kształcenia szkolnego w okresie pandemii COVID-19, przewidując w szczególności możliwość, by uczniowie, którzy nie mogli być obecni w klasie, mogli uczestniczyć w lekcjach na żywo za pośrednictwem wideokonferencji. W celu ochrony praw uczniów w zakresie danych osobowych ustalono, że połączenie z usługą wideokonferencji będzie dozwolone wyłącznie za zgodą samych uczniów lub – w przypadku osób niepełnoletnich – za zgodą ich rodziców. Nie przewidziano natomiast możliwości wyrażenia zgody przez zainteresowanych nauczycieli na ich udział w tej usłudze.

Sprzeciw nauczycieli

Rada główna nauczycielstwa przy ministerstwie edukacji kraju związkowego Hesja wniosła skargę przeciwko ministrowi odpowiedzialnemu za te kwestie, powołując się na fakt, że transmitowanie na żywo lekcji w formie wideokonferencji, tak jak przewidziano w uregulowaniu krajowym, nie zostało poddane warunkowi uzyskania zgody zainteresowanych nauczycieli. Minister podniósł, że przetwarzanie danych osobowych, jakim jest transmitowanie lekcji na żywo w formie wideokonferencji, jest objęte uregulowaniem krajowym, w związku z czym może być dokonywane bez uzyskania zgody zainteresowanych nauczycieli.
Sąd administracyjny rozpatrujący sprawę wskazał, że zgodnie z wolą ustawodawcy kraju związkowego Hesja uregulowanie krajowe, na podstawie którego odbywa się przetwarzanie danych osobowych nauczycieli, należy do kategorii „bardziej szczegółowych przepisów", które państwa członkowskie mogą przewidzieć zgodnie z art. 88 ust. 1 ogólnego rozporządzenia o ochronie danych [1] w celu zapewnienia ochrony praw i wolności pracowników w zakresie przetwarzania ich danych osobowych w związku z zatrudnieniem [2]. Sąd ten powziął jednak wątpliwości co do zgodności tego uregulowania z warunkami ustanowionymi w art. 88 ust. 2 RODO [3]. W związku z tym zwrócił się do Trybunału z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym.

Zdaniem TSUE e-lekcje muszą podlegać RODO

W swoim wyroku Trybunał orzekł, że uregulowanie krajowe nie może stanowić „bardziej szczegółowego przepisu" w rozumieniu art. 88 ust. 1 RODO, w przypadku gdy nie spełnia ono warunków określonych w ust. 2 tego artykułu. Ponadto Trybunał wyjaśnił, że należy odstąpić od stosowania przepisów krajowych przyjętych w celu zapewnienia ochrony praw i wolności pracowników w zakresie przetwarzania ich danych osobowych w związku z zatrudnieniem,

jeżeli przepisy te nie spełniają warunków i ograniczeń określonych w art. 88 ust. 1 i 2 RODO, chyba że rozpatrywane przepisy stanowią podstawę prawną przetwarzania, o której mowa w innym artykule RODO [4], spełniającą przewidziane w tym przepisie wymogi.

TSUE wypowiedział się nt. zgodności zdalnego nauczania z RODO

Na wstępie Trybunał uznał, że przetwarzanie danych osobowych nauczycieli przy transmitowaniu na żywo prowadzonych przez nich lekcji nauczania publicznego w formie wideokonferencji jest objęte materialnym zakresem stosowania RODO. Wyjaśnił następnie, że to przetwarzanie danych osobowych nauczycieli, którzy jako pracownicy lub urzędnicy należą do służby publicznej kraju związkowego Hesja, wchodzi w podmiotowy zakres stosowania art. 88 RODO, który dotyczy przetwarzania danych osobowych pracowników w związku z zatrudnieniem.

Uzasadnienie stanowiska TSUE

W pierwszej kolejności Trybunał zajął się kwestią, czy „bardziej szczegółowy przepis" w rozumieniu art. 88 ust. 1 RODO powinien spełniać warunki określone w ust. 2 tego artykułu. Zdaniem Trybunału, z użycia w treści art. 88 ust. 1 RODO wyrażenia „bardziej szczegółowe" wynika, że uregulowania, o których mowa w tym przepisie, powinny mieć treść normatywną właściwą dla regulowanej dziedziny i odrębną od przepisów ogólnych tego rozporządzenia. Z brzmienia art. 88 RODO wynika również, że ust. 2 tego artykułu ogranicza zakres uznania państw członkowskich, które zamierzają przyjąć „bardziej szczegółowe przepisy" na podstawie ust. 1 tego artykułu. Trybunał uznał z jednej strony, że przepisy te nie mogą ograniczać się do powtórzenia przepisów tego rozporządzenia przewidujących warunki legalności przetwarzania danych osobowych oraz zasady tego przetwarzania [5] czy też do odesłania do tych warunków i zasad. Przepisy te powinny mieć na celu ochronę praw i wolności pracowników w związku z przetwarzaniem ich danych oraz zawierać odpowiednie i konkretne środki służące ochronie godności, prawnie uzasadnionych interesów i praw podstawowych osób, których dane dotyczą. Z drugiej strony, szczególną uwagę należy zwrócić na przejrzystość przetwarzania, przekazywanie danych osobowych w ramach grupy przedsiębiorstw lub grupy przedsiębiorstw prowadzących wspólną działalność gospodarczą, a także na systemy monitorujące w miejscu pracy. W konsekwencji, aby przepis prawny można było zakwalifikować jako „bardziej szczegółowy przepis" w rozumieniu art. 88 ust. 1 RODO, musi on spełniać warunki określone w ust. 2 tego artykułu. W drugiej kolejności Trybunał wyjaśnił konsekwencje, jakie należy wyciągnąć ze stwierdzenia niezgodności rozpatrywanych przepisów krajowych z warunkami i ograniczeniami przewidzianymi w art. 88 ust. 1 i 2 RODO. Trybunał przypomniał, że do sądu odsyłającego, który jako jedyny jest właściwy do dokonywania wykładni prawa krajowego, należy ocena, czy rozpatrywane przepisy krajowe spełniają warunki i ograniczenia określone w art. 88 RODO.

Trybunał zauważył jednak, że przepisy krajowe, które uzależniają przetwarzanie danych osobowych pracowników od warunku, by przetwarzanie to było niezbędne do określonych celów związanych z wykonywaniem stosunku pracy, wydają się powtarzać ustanowiony już w RODO [6] ogólny warunek zgodności z prawem, bez dodawania bardziej szczegółowego przepisu w rozumieniu art. 88 ust. 1 tego rozporządzenia. W przypadku gdyby sąd odsyłający doszedł do wniosku, że te przepisy krajowe nie spełniają warunków i ograniczeń określonych w art. 88 RODO, powinien on co do zasady odstąpić od ich stosowania. Zgodnie bowiem z zasadą pierwszeństwa prawa Unii, w braku bardziej szczegółowych przepisów zgodnych z warunkami i ograniczeniami określonymi w art. 88 RODO, przetwarzanie danych osobowych w związku z zatrudnieniem, zarówno w sektorze prywatnym, jak i publicznym, podlega bezpośrednio przepisom tego rozporządzenia.
W tym względzie Trybunał zauważył, że do przetwarzania danych osobowych, takiego jak w niniejszej sprawie, mogą mieć zastosowanie inne przepisy RODO [7], na mocy których przetwarzanie danych osobowych jest zgodne z prawem, jeżeli jest ono konieczne, odpowiednio, do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi lub do wypełnienia obowiązku prawnego ciążącego na administratorze. W odniesieniu do tych dwóch przypadków zgodności z prawem RODO [8] z jednej strony przewiduje, że przetwarzanie musi opierać się na prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator, a z drugiej strony dodaje, że cele przetwarzania są określone w tej podstawie prawnej lub są niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. W związku z tym, gdy sąd odsyłający dojdzie do wniosku, że przepisy krajowe dotyczące przetwarzania danych osobowych w związku z zatrudnieniem nie spełniają warunków i ograniczeń określonych w art. 88 ust. 1 i 2 RODO, powinien jeszcze sprawdzić, czy przepisy te stanowią podstawę prawną przetwarzania, o której mowa w innym artykule RODO [9], spełniającą wymogi przewidziane w tym rozporządzeniu. Jeżeli tak jest, nie można odstąpić od stosowania tych przepisów krajowych.

Wyrok TSUE z 30 marca 2023 r. w sprawie C-34/21

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. 2016, L 119, s. 1, zwane dalej „RODO").
[2] Zgodnie z art. 88 ust. 1 RODO, który stanowi klauzulę upoważniającą, państwa członkowskie mogą zawrzeć w swoich przepisach lub w porozumieniach zbiorowych bardziej szczegółowe przepisy mające zapewnić ochronę praw i wolności w przypadku przetwarzania danych osobowych pracowników w związku z zatrudnieniem, w szczególności do celów wykonania umowy o pracę, zarządzania, planowania i organizacji pracy.
[3] Artykuł 88 ust. 2 RODO stanowi, że przepisy te muszą obejmować odpowiednie i szczegółowe środki zapewniające osobie, której dane dotyczą, poszanowanie jej godności, prawnie uzasadnionych interesów i praw podstawowych, w szczególności pod względem przejrzystości przetwarzania, przekazywania danych osobowych oraz systemów monitorujących w miejscu pracy
[4] Artykuł 6 ust. 3 RODO.
[5] Określone odpowiednio w art. 6 i 5 RODO.
[6] Artykuł 6 ust. 2 akapit pierwszy lit. b) RODO
[7] Artykuł 6 ust. 1 akapit pierwszy lit. c) i e) RODO.
[8] Artykuł 6 ust. 3 RODO.
[9] Przewidziana w art. 6 ust. 3 RODO w związku z jego motywem 45.

FRANCJA: GEOLOKALIZACJA WYPOŻYCZANYCH SKUTERÓW NIE MOŻE NARUSZAĆ PRYWATNOŚCI UŻYTKOWNIKÓW

CNIL (francuski organ ochrony danych) w marcu tego roku ukarał firmę CITYSCOOT administracyjną karą pieniężną w wysokości 125 tys. euro m.in. za naruszenie prywatności swoich klientów poprzez śledzenie ich lokalizacji.

CNIL przeprowadził kontrolę dotyczącą przedsiębiorstwa CITYSCOOT, które wynajmuje skutery na krótki okres. Organ skupił się na sprawdzeniu gromadzonych przez firmę danych, zweryfikował, jakie informacje i zgody uzyskuje od użytkowników, zanim przystąpi do przetworzenia informacji technicznych na ich telefonie komórkowym lub komputerze.
CNIL ustalił, że podczas wypożyczania skutera przez osobę prywatną, firma zbierała co 30 sekund dane dotyczące geolokalizacji pojazdu. Ponadto firma prowadziła rejestr tych przejazdów.
CNIL stwierdził m.in. niedopełnienie obowiązku zapewnienia minimalizacji danych (art. 5 ust.1 c RODO). Ponadto po przeanalizowaniu wykorzystania danych geolokalizacyjnych dla każdego z celów (przetwarzanie skarg klientów, wykroczeń drogowych, wsparcie użytkowników w przypadku konieczności wezwania pomocy oraz zarządzanie roszczeniami) organ wykazał, że żaden z nich nie uzasadniał gromadzenia danych w tak szczegółowy sposób, w jaki to robił CITYSCOOT.
Decyzja o nałożeniu kary w wysokości 125 tys. euro została podjęta we współpracy z hiszpańskimi i włoskimi organami ochrony danych, ponieważ CITYSCOOT oferuje te usługi również w tych krajach.

Źródło: **decyzja organu nadzorczego**

7 EDUKACJA

MŁODZI LUDZIE POTRZEBUJĄ WSKAZÓWEK, JAK DBAĆ O SIEBIE I SWOJE DANE W INTERNECIE

Im bardziej jesteśmy aktywni w sieci, tym bardziej powinniśmy zwracać uwagę na ochronę danych osobowych – wynika z informacji zaprezentowanych podczas webinarium pt. „Na jaką przynętę dasz się złapać?". Wydarzenie zorganizowali wspólnie Urząd Ochrony Danych Osobowych i Urząd Komunikacji Elektronicznej.

Adresatami wydarzenia byli uczniowie klas 7–8 szkół podstawowych oraz szkół ponadpodstawowych. Spotkanie online odbyło się 13 kwietnia 2023 r. w ramach trwającej XIII edycji programu edukacyjnego „Twoje dane – Twoja sprawa".

Zanim klikniesz, zastanów się, jakie dane chcesz udostępnić na swój temat…

Aktywność młodzieży w sieci powoduje, że udostępniają oni ogromną liczbę informacji na swój temat, w tym dane osobowe. Celem webinarium było uświadomienie uczniom, że ochrona danych osobowych wiąże się nie tylko z poznaniem regulacji prawnych oraz możliwości technologicznych urządzeń oraz z identyfikacją zagrożeń, jakie mogą pojawić się podczas korzystania z Internetu, ale przede wszystkim z umiejętnym zarządzaniem swoją obecnością w sieci. Podczas spotkania ekspertka UODO uświadomiła młodzież, jakie dane najczęściej wyłudzają oszuści. W kręgu zainteresowania oszustów są wszystkie możliwe dane osobowe: imię i nazwisko, PESEL, dane rodziny, miejsce urodzenia, adres zamieszkania, numer i seria dowodu osobistego, numery kont bankowych, dane karty płatniczej, loginy i hasła oraz PIN-y czy informacje z serwisów społecznościowych. Uczestnicy spotkania otrzymali także wskazówki, jak postąpić, gdy dane osobowe zostaną wykradzione lub wyłudzone. Wśród rekomendowanych reakcji znalazły się m.in.: rozmowa z rodzicami, zgłoszenie sprawy na policję, poinformowanie banku, przekazanie zgłoszenia do dowolnego urzędu gminy w celu unieważnienia dowodu osobistego, a także zmiana hasła do logowania i ustawień uwierzytelniania (najlepiej na dwuskładnikowe). Dodatkowo zalecane jest monitorowanie aktywności na kontach oraz sprawdzanie, czy ktoś nie posłużył się danymi.

7 EDUKACJA

… bo współczesny świat nie sprzyja anonimowości

Historia wyszukiwania oraz odwiedzanych stron, wykorzystywane urządzenia, dzielenie się informacjami osobistymi (takimi jak miejsce zameldowania czy pobytu, data urodzin, informacje o relacjach i związkach z innymi osobami, uczestnictwo w wydarzeniach) – jak podkreśliły ekspertki UKE każda z tych aktywności może dostarczyć cyberprzestępcom cennych danych na temat internauty. Prowadzące spotkanie zwróciły szczególną uwagę na phishing, vishing oraz smishing. Uczestnicy poznali definicje tych pojęć. Nauczyli się rozpoznawać te zjawiska w codziennych sytuacjach. Specjalistki wytłumaczyły uczniom na wybranych przykładach, jakie sytuacje szczególnie sprzyjają działalności cyberoszustów. Podkreśliły rolę silnych haseł, ich budowy i zasad tworzenia w powstanie skutecznej zapory przed cyberprzestępcami. Zachęcały także do systematycznej aktualizacji oprogramowania, co może pomóc internaucie zapewnić dodatkową ochronę.

Młodzi Polacy są przekonani, że trudno ich oszukać

O tym, jak bardzo młodzież potrzebuje wskazówek, jak dbać o siebie i swoje dane w Internecie, świadczą chociażby wyniki badań przeprowadzonych w 2022 roku przez serwis ChronPESEL.pl oraz Krajowy Rejestr Długów pod patronatem Urzędu Ochrony Danych Osobowych.
Okazało się, że prawie 90% badanych stwierdziło, że wie, jak zadbać o bezpieczeństwo swoich danych. 88% jest przekonanych, że z łatwością rozpozna próbę oszustwa przez telefon, SMS czy e-maila. Aż 63% deklaruje, że wie, co należy zrobić w przypadku wyłudzenia danych osobowych, takich jak: imię, nazwisko, adres lub PESEL. Jednak pomimo przekonania o swojej wiedzy i wysokim poczuciu własnego bezpieczeństwa, to właśnie młodzi Polacy są grupą, która najczęściej popełnia błędy w postaci publikacji zdjęć swoich dokumentów w sieci, udostępniania osobom trzecim loginów i haseł do logowania oraz zostawiania danych osobowych w internetowych ankietach, które nie są konieczne do wypełnienia.

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl