Obserwuj nas na:

Nr 6/2021 (27)
Czerwiec 2021

URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

ŚWIADECTWO PRACY DLA CUDZOZIEMCA

Gdy przekazanie danych osobowych do państwa trzeciego jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń, możliwe jest skorzystanie z wyjątku, o którym mowa w art. 49 ust. 1 lit. e RODO.

W ostatnim czasie do jednej z polskich firm Konsulat Królestwa Tajlandii zwrócił się o przekazanie świadectw pracy czterech byłych pracowników tej firmy będących obywatelami Królestwa Tajlandii.

Firma, mając wątpliwości, czy udostępnienie tych zawierających dane osobowe dokumentów jest dopuszczalne, o zajęcie stanowiska wystąpiła do Prezesa UODO.

Wykonywanie funkcji konsularnych

W udzielonych wyjaśnieniach organ nadzorczy wskazał, że Konwencja wiedeńska o stosunkach konsularnych, sporządzona w Wiedniu dnia 24 kwietnia 1963 r., której stronami są m.in. Rzeczpospolita Polska i Królestwo Tajlandii, i której postanowienia stosuje się odpowiednio w razie wykonywania funkcji konsularnych przez przedstawicielstwo dyplomatyczne (art. 70 ust. 1 Konwencji wiedeńskiej), wśród funkcji konsularnych wymienia m.in.:
1) ochronę w państwie przyjmującym interesów państwa wysyłającego oraz jego obywateli, zarówno osób fizycznych, jak i prawnych, w granicach dozwolonych przez prawo międzynarodowe (art. 5 lit. a),
2) udzielanie pomocy i opieki obywatelom państwa wysyłającego, zarówno osobom fizycznym, jak i prawnym (art. 5 lit. e),
3) przesyłanie sądowych i pozasądowych dokumentów [...] zgodnie z obowiązującymi umowami międzynarodowymi lub, w braku takich umów, w sposób zgodny z ustawami i innymi przepisami państwa przyjmującego (art. 5 lit. j).

Jednocześnie z udostępnionej Prezesowi UODO korespondencji pełnomocników firmy z Konsulatem Królestwa Tajlandii wynika, iż to byli pracownicy tej firmy będący obywatelami Królestwa Tajlandii wystąpili do Departamentu Konsularnego Ministerstwa Spraw Zagranicznych Królestwa Tajlandii ze skargą na niewystawienie im przez byłego pracodawcę świadectw pracy i polecenia wykonywania pracy poza miejscem oraz godzinami pracy ustalonymi w umowach o pracę (co, zdaniem skarżących, powodowało brak bezpieczeństwa wykonywania przez nich obowiązków służbowych).

Przy tak ustalonym stanie faktycznym, w opinii organu nadzorczego, Konsulat Królestwa Tajlandii (Wydział Konsularny Ambasady Królestwa Tajlandii) jako podmiot uprawniony do ochrony interesów obywateli Królestwa Tajlandii w Rzeczypospolitej Polskiej i zobowiązany do udzielania pomocy i opieki tym obywatelom jest umocowany do pozyskania od firmy świadectw pracy (duplikatów świadectw pracy) czterech byłych jej pracowników będących obywatelami Królestwa Tajlandii celem ich przesłania tym obywatelom (przebywającym obecnie w kraju ojczystym). Jednocześnie Konsulat Królestwa Tajlandii należy w tym przypadku uznać za osobę upoważnioną przez pracownika do odbioru świadectwa pracy (co przewiduje § 3 rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej z dnia 30 grudnia 2016 r. w sprawie świadectwa pracy).

Co więcej – zgodnie z informacją zawartą w wiadomości e-mail Wydziału Konsularnego Ambasady Królestwa Tajlandii – wnioskowane świadectwa pracy oraz wyjaśnienia spółki mają stać się przedmiotem prowadzonego przez organy tajlandzkie postępowania dotyczącego legalizacji umów o pracę.

Możliwe zastosowanie wyjątku

Jednocześnie w opinii Prezesa UODO, przepisy RODO dotyczące przekazywania danych osobowych do państw trzecich nie stoją na przeszkodzie przekazaniu Wydziałowi Konsularnemu Ambasady Królestwa Tajlandii świadectw pracy (duplikatów świadectw pracy) czterech byłych pracowników spółki będących obywatelami Królestwa Tajlandii.

Choć bowiem Królestwo Tajlandii jest państwem trzecim niezapewniającym na swoim terytorium odpowiedniego stopnia ochrony danych osobowych w rozumieniu art. 45 ust. 1 i 3 RODO i nie będzie mógł być do opisanego przekazania zastosowany art. 46 ust. 1 i 3 RODO, to – w ocenie organu właściwego w sprawie ochrony danych osobowych – można rozważyć wyjątek z art. 49 ust. 1 lit. e RODO. Przepis ten dopuszcza przekazanie danych osobowych do państwa trzeciego, gdy przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń. W myśl motywu 111 RODO, postępowanie oraz organ, przed którym takie postępowanie może się toczyć, są rozumiane szeroko, tj. rodzaj postępowania nie ma znaczenia: może to być postępowanie sądowe lub administracyjne lub jakiekolwiek inne postępowanie pozasądowe, w tym postępowanie przed organami regulacyjnymi (wskazuje się na to również w literaturze, np. Piotr Drobek [w:] Witold Chomiczewski, Michał Czerniawski, Piotr Drobek, Urszula Góral, Magdalena Kuba, Joanna Łuczak, Paweł Makowski, Katarzyna Witkowska, Natalia Zawadzka, Edyta Bielak-Jomaa (red.), Dominik Lubasz (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, Wydawnictwo Wolters Kluwer Polska SA, Warszawa 2017, komentarz do art. 49 rozporządzenia 2016/679 w prawniczym programie komputerowym LEX Omega, teza 11).

W opinii Prezesa UODO, skoro po przekazaniu świadectw pracy (duplikatów świadectw pracy) czterech byłych pracowników spółki do Królestwa Tajlandii przez organy tajlandzkie ma zostać przeprowadzone postępowanie dotyczące złożonych przez nich skarg, to wydaje się, iż art. 49 ust. 1 lit. e RODO znajduje w takiej sytuacji zastosowanie.

Ocena skarg i roszczeń poza właściwością Prezesa UODO

Prezes UODO podkreślił jednocześnie, że ocena zasadności skarg na spółkę i – ewentualnych – roszczeń byłych pracowników spółki pozostaje poza zakresem właściwości organu ds. ochrony danych osobowych.

GDY ORGAN PODATKOWY ŻĄDA UDOSTĘPNIENIA INDYWIDUALNEGO PROGRAMU REHABILITACJI PRACOWNIKA NIEPEŁNOSPRAWNEGO

Organy podatkowe są uprawnione do żądania udostępnienia określonych dokumentów i informacji, ale powinny przetwarzać dane adekwatne do określonego celu. W każdym przypadku należy analizować, czy żądany zakres informacji, w tym danych osobowych, jest niezbędny w celu wyjaśnienia danej sprawy.

Do Prezesa UODO wpłynęła prośba o wskazanie, czy organ podatkowy może żądać od pracodawcy przedstawienia indywidualnego programu rehabilitacji opracowanego dla pracownika niepełnosprawnego.

Ogólne wskazówki

Odnosząc się do tej prośby, organ nadzorczy wskazał, że każdą sprawę należy oceniać indywidualnie, kierując się zarówno ogólnymi zasadami określonymi w RODO, jak i przepisami szczególnymi regulującymi działalność konkretnych sektorów czy podmiotów.

Pomoc de minimis

Znaczenie dla oceny sprawy mają m.in. przepisy rozporządzenia Ministra Pracy i Polityki Społecznej z dnia 19 grudnia 2007 r. w sprawie zakładowego funduszu rehabilitacji osób niepełnosprawnych, które stanowią, że jeżeli wydatki w ramach indywidualnych programów rehabilitacji są dokonywane ze środków pochodzących ze zwolnienia podatkowego i stanowią przysporzenie dla pracodawcy, są pomocą de minimis (§ 2 ust. 2). Warunkiem uznania pomocy jako pomocy de minimis jest uzyskanie zaświadczenia wydanego przedsiębiorcy przez organ podatkowy, podmiot uprawniony do pobierania opłat na podstawie odrębnych przepisów lub inny podmiot

udzielający pomocy (§ 9 ust. 1). W celu uzyskania zaświadczenia przedsiębiorca przedstawia informację o dokonaniu wydatku ze środków funduszu rehabilitacji w ciągu 30 dni od dnia jego dokonania (§ 9 ust. 2), a występując o wydanie zaświadczenia, przedsiębiorca przedstawia uzyskane zaświadczenia o pomocy de minimis otrzymanej w okresie obejmującym bieżący rok kalendarzowy oraz dwa poprzedzające go lata kalendarzowe albo oświadczenie o wielkości pomocy de minimis otrzymanej w tym okresie, albo oświadczenie o nieskorzystaniu z pomocy de minimis w tym okresie oraz informacje o każdej pomocy innej niż de minimis, jaką otrzymał w odniesieniu do tych samych kosztów kwalifikujących się oraz na dany projekt inwestycyjny, z którym związana jest pomoc de minimis (§ 9 ust. 3).

Uprawnienia organów podatkowych

Pod uwagę należy wziąć również uprawnienia organów podatkowych do wezwania strony lub innych osób do złożenia wyjaśnień, zeznań, przedłożenia dokumentów lub dokonania określonej czynności osobiście, przez pełnomocnika lub na piśmie, w tym także w formie dokumentu elektronicznego, jeżeli jest to niezbędne dla wyjaśnienia stanu faktycznego lub rozstrzygnięcia sprawy – zgodnie z art. 155 ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa. Oznacza to, że organ podatkowy w toku prowadzonych czynności w konkretnej sprawie ma prawo wezwać stronę postępowania podatkowego do przedłożenia określonych dokumentów, jeżeli jest to niezbędne dla wyjaśnienia stanu faktycznego lub rozstrzygnięcia sprawy, tak aby nie doszło do naruszenia przepisów postępowania administracyjnego.

Zgodnie z wyrokiem Wojewódzkiego Sądu Administracyjnego w Kielcach z 30 marca 2016 r. (sygn. akt II SA/Ke 117/16), „poprzez instytucję wezwania strony, czy innej osoby do określonego zachowania na podstawie art. 155 Ordynacji podatkowej, realizowany jest przez organ obowiązek podjęcia wszelkich niezbędnych działań w celu dokładnego wyjaśnienia stanu faktycznego sprawy. (...) Ocena bowiem, czy złożenie przez stronę dowodu jest niezbędne pozostaje w gestii organu, przed którym toczy się postępowanie".

Kwestię dotyczącą przetwarzania danych osobowych w toku postępowania podatkowego WSA w Kielcach rozstrzygnął również w wyroku z 23 marca 2017 r. (sygn. akt II SA/Ke 107/17), wskazując, że: „chociaż przepisy O.p. [Ordynacji podatkowej] wprawdzie wprost nie mówią o przetwarzaniu danych osobowych, to zarówno w doktrynie, jak i w orzecznictwie nie budzi wątpliwości, że w takim postępowaniu dochodzi do przetwarzania danych osobowych. Na czynności te składa się: przetwarzanie danych osobowych stron postępowania, przeprowadzanie dowodów zwłaszcza osobowych, prowadzenie akt sprawy, sporządzanie protokołów, dokonywanie doręczeń i wezwań, udostępnianie akt sprawy, a wreszcie wydanie rozstrzygnięcia. Mimo braku w przepisach O.p. upoważnienia do przetwarzania danych osobowych, noszącego cechy upoważnienia o charakterze generalnym, należy przyjąć, że przetwarzanie danych osobowych przez organ administracji dla celów prowadzonego postępowania jest niezbędne dla wykonania uprawnień i obowiązków przyznanych organowi w przepisach art. 122 i 187 § 1 O.p.".

Przestrzeganie RODO

Podkreślić przy tym należy, że organ podatkowy przetwarzający dane osobowe powinien kierować się również zasadami wynikającymi z art. 5 RODO, przede wszystkim zasadami zgodności z prawem, celowości i minimalizacji danych, a zatem przetwarzać dane zgodnie z obowiązującymi przepisami prawa, w konkretnych, wyraźnych i prawnie uzasadnionych celach i w sposób adekwatny do tych celów.

Z kolei pracodawca, który jest administratorem danych osobowych swoich pracowników, aby udostępniać te dane, musi legitymować się również podstawą prawną do takiego działania. Zatem, aby było ono legalne, konieczne jest spełnienie przynajmniej jednej przesłanki wymienionej w art. 6 ust. 1 RODO. Wśród nich należy wskazać m.in. na zgodę osoby, której dane dotyczą (lit. a), niezbędność przetwarzania w związku z wypełnieniem obowiązku prawnego ciążącego na administratorze (lit. c), czy realizację celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią (lit. f).

Warto przy tym pamiętać, że indywidualny program rehabilitacji może zawierać informacje dotyczące zdrowia (np. o niepełnosprawności), a więc dane wskazane w art. 9 ust. 1 RODO, które – ze względu na swój sensytywny charakter – powinny zostać objęte większą ochroną. Żeby ich przetwarzanie było zgodne z prawem, musi zostać spełniony jeden z warunków określonych w art. 9 ust. 2 RODO.

Indywidualna analiza

W tym stanie prawnym, w ocenie organu nadzorczego, w toku postępowania podatkowego organy podatkowe mają uprawnienie do żądania udostępniania określonych dokumentów i informacji, niemniej w każdym przypadku należy przeanalizować, czy żądany zakres informacji, w tym danych osobowych, jest niezbędny w celu wyjaśnienia danej sprawy. Nie jest bowiem konieczne przetwarzanie danych na wszelki wypadek i w celach niezwiązanych z konkretnym postępowaniem. Oznacza to, że organy podatkowe nie mogą nadużywać swojego prawa do wzywania stron w toku prowadzonego postępowania i w każdym przypadku powinny przetwarzać dane adekwatne do określonego celu, a tym samym czynić zadość zasadom przetwarzania danych określonych w art. 5 RODO.

Pomocny inspektor

W przypadku wątpliwości związanych z ochroną danych osobowych w przyjmowanych rozwiązaniach administrator, a także pracownicy, mogą zwrócić się do inspektora ochrony danych, którego zadaniem jest monitorowanie przyjmowanych rozwiązań pod kątem ich zgodności z ogólnym rozporządzeniem o ochronie danych i którego powołanie w instytucjach publicznych (zgodnie z art. 37 ust. 1 lit. a RODO) jest obligatoryjne. Inspektor, mając wiedzę nie tylko z zakresu ochrony danych osobowych, ale przede wszystkim znając specyfikę realizowanych przez administratora zadań, powinien dostosowywać podejmowane działania tak, aby działając zgodnie z prawem, nie naruszać istoty autonomii jednostki.

UPOMNIENIE ZA NARUSZENIE ZASADY MINIMALIZACJI DANYCH W POSTĘPOWANIU PODATKOWYM

Za umieszczenie w wezwaniach świadków w postępowaniu podatkowym adresu nieruchomości, której sprawa dotyczyła, Prezes UODO udzielił zarządowi związku międzygminnego upomnienia. Uznał bowiem, że w ten sposób naruszona została zasada minimalizacji danych.

Prezes UODO badał tę sprawę na skutek skargi złożonej przez właścicieli nieruchomości o charakterze letniskowym. W stosunku do nich związek międzygminny prowadził z urzędu postępowanie w sprawie określenia wysokości opłaty za gospodarowanie odpadami komunalnymi z tej nieruchomości.

Wezwania świadków

W jego toku jako świadków związek wezwał pięciu sąsiadów skarżących z miejsca ich stałego zamieszkania. W rozesłanych do nich wezwaniach wnosił o udzielenie pisemnych wyjaśnień (w trybie art. 155, art. 181 oraz art. 189 § 1 ustawy z dnia 29 sierpnia 1997 r. Ordynacja podatkowa) dotyczących tego, kto mieszkał w miejscu stałego zamieszkania skarżących. W korespondencji tej związek podał również dokładny adres ich nieruchomości letniskowej.

Wyjaśnienia związku

Związek w udzielonych Prezesowi UODO wyjaśnieniach, odnosząc się do zarzutów skarżących i powołując na orzecznictwo, podnosił, że jako organ podatkowy musiał tak postąpić. Żeby móc rzetelnie prowadzić postępowanie w danej sprawie, musi bowiem spełniać wszystkie przepisy Ordynacji podatkowej. Jednocześnie zaznaczył, że podanie dokładnego adresu nieruchomości letniskowej skarżących było niezbędne ze względu na konieczność określenia, czego dotyczy prowadzone postępowanie. Podnosił, że skoro określenie wysokości opłaty za gospodarowanie odpadami komunalnymi zależy od sposobu wykorzystania konkretnej nieruchomości, to podanie jej dokładnego adresu było niezbędne.

Niewłaściwe określenie przedmiotu sprawy

W wydanej w tej sprawie decyzji Prezes UODO wskazał, że zgodnie z art. 159 § 1 Ordynacji podatkowej, wezwanie strony lub innych osób do złożenia wyjaśnień, zeznań, przedłożenia dokumentów lub dokonania określonej czynności powinno zawierać:
1) nazwę i adres organu podatkowego;
2) imię i nazwisko osoby wzywanej;
3) w jakiej sprawie i w jakim charakterz oraz w jakim celu osoba ta zostaje wezwana;
4) czy osoba wezwana powinna stawić się osobiście lub przez pełnomocnika, czy też może złożyć wyjaśnienie lub zeznanie na piśmie lub w formie dokumentu elektronicznego;
5) czy dokumenty mogą być przedłożone w formie dokumentu elektronicznego lub na informatycznych nośnikach danych;
6) termin, do którego żądanie powinno być spełnione, albo dzień, godzinę i miesce zgłoszenia się osoby wzywanej lub jej pełnomocnika;
7) skutki prawne niezastosowania się do wezwania.

Tymczasem związek, podając w wezwaniach skierowanych do sąsiadów skarżących dokładny adres ich nieruchomości o charakterze letniskowym, w związku z którą prowadził postępowanie, ujawnił sąsiadom informację o dokładnym adresie nieruchomości należącej do skarżących, która nie była potrzebna do ustalenia okoliczności objętej wezwaniem, tj. dotyczącej zamieszkiwania osób pod adresem będącym miejscem stałego zamieszkania skarżących.

Prezes UODO podniósł, że wskazanie w wezwaniu pełnego adresu nieruchomości letniskowej należącej do skarżących nie było jedynym możliwym sposobem określenia przedmiotu sprawy. Związek pytał bowiem, kto mieszkał w miejscu ich stałego zamieszkania, a więc w zupełnie innej nieruchomości.

Artykuł 159 § 1 Ordynacji podatkowej nie nakazuje organowi podatkowemu podawania w wezwaniu pełnego zakresu prowadzonej sprawy. Związek mógł sformułować wezwanie w taki sposób, by sąsiedzi skarżących nie uzyskali wiedzy na temat pełnego adresu posiadanej przez nich nieruchomości, a jednocześnie nie utracili możliwości skorzystania z przysługujących im praw odmowy składania zeznań czy odmowy udzielenia odpowiedzi wynikających z art. 196 Ordynacji podatkowej. Również określenie stron postępowania prowadzonego przez związek nie wymagało wskazania pełnego adresu drugiej nieruchomości skarżących, pod którym, jak wskazał sam związek, nie zamieszkiwali.

Prezes UODO uznał, że wezwania skierowane do sąsiadów skarżących zawierały zbyt szeroki zakres danych, który nie może zostać usankcjonowany treścią art. 159 § 1 Ordynacji podatkowej. Tym samym zarząd związku międzygminnego naruszył zasadę minimalizacji danych wyrażoną w art. 5 ust. 1 lit. c) RODO. Jednak biorąc pod uwagę incydentalny charakter tego naruszenia oraz ograniczony zakres danych, Prezes UODO uznał upomnienie za wystarczającą reakcję.

BĘDZIE ANONIMIZACJA DECYZJI W POSTĘPOWANIU W SPRAWIE ZAWARCIA UMOWY O UDZIELANIE ŚWIADCZEŃ OPIEKI ZDROWOTNEJ

Trwają prace nad nowelizacją ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych oraz ustawy – Prawo farmaceutyczne. Jedna z projektowanych zmian dotyczy dokonywania anonimizacji decyzji dotyczących rozpatrzenia odwołania od rozstrzygnięcia postępowania w sprawie zawarcia umowy o udzielanie świadczeń opieki zdrowotnej.

Do projektowanej zmiany przepisów doszło na skutek interwencji Prezesa UODO, który w wystąpieniu z 22 czerwca 2020 r. zwrócił się do ministra zdrowia z wnioskiem o rozważenie zmiany brzmienia art. 154 ust. 3 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych jako niezgodnego z RODO i budzącego wątpliwości w praktycznym stosowaniu. Przepis ten stanowił wówczas, że po rozpatrzeniu odwołania od rozstrzygnięcia postępowania w sprawie zawarcia umowy o udzielanie świadczeń opieki zdrowotnej dyrektor oddziału wojewódzkiego

Narodowego Funduszu Zdrowia wydaje decyzję administracyjną uwzględniającą lub oddalającą odwołanie, a decyzja ta jest zamieszczana w terminie dwóch dni od dnia jej wydania, na tablicy ogłoszeń oraz na stronie internetowej właściwego oddziału wojewódzkiego Funduszu.

Prezes UODO w swoim wystąpieniu podniósł, iż w treści decyzji mogą być zamieszczone dane różnych osób (nie tylko stron postępowania, ale i osób trzecich) oraz różnych kategorii (dane zwykłe i szczególne kategorie danych), a powołany przepis nie zawiera rozwiązań zapewniających publikację decyzji z poszanowaniem prawa do prywatności osób fizycznych, których dane znajdują się w treści takiej decyzji. Wskazał, że udostępnianie wszelkich danych, w tym danych osób fizycznych zawartych w decyzjach administracyjnych, może stanowić ingerencję w konstytucyjnie gwarantowane prawo do ochrony prywatności oraz autonomii informacyjnej jednostki, jako prowadzące do udostępniania szeregu informacji nie tylko dotyczących strony czy uczestnika postępowania, ale także osób trzecich.

Jednocześnie zaznaczył, że udostępnianie w trybie dostępu do informacji publicznej dokumentów urzędowych zawierających dane osobowe podlega przepisom RODO. Zgodnie zaś z określoną w nim zasadą minimalizacji danych oraz zasadą ograniczenia celu, upublicznianie dokumentów urzędowych powinno być poprzedzone uprzednią oceną administratora, czy w określonym stanie faktycznym i prawnym dla osiągnięcia celu zachodzi niezbędność publikacji danych osobowych. W przypadku braku takich przesłanek, informacje o osobach fizycznych powinny być poddane anonimizacji.

W odpowiedzi na to wystąpienie resort zdrowia zadeklarował dokonanie zmiany wskazanych przepisów, a niedawno przesłał uwzględniający je projekt **ustawy o zmianie ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych oraz ustawy - Prawo farmaceutyczne**. Przewiduje on nowe brzmienie art. 154 ust. 3, w którym wprost wprowadza się obowiązek dokonywania anonimizacji upublicznianej zgodnie z tym przepisem decyzji administracyjnej, w zakresie danych osobowych oraz innych danych istotnych ze względu na identyfikację podmiotową osób innych niż strony postępowania.

W opinii Prezesa UODO, taka konstrukcja przepisu zapewni jego zgodność z RODO i wyeliminuje wątpliwości dotyczącego jego stosowania w praktyce.

EDUKACJA

Co czwarty Polak boi się ataku cyberprzestępców

Blisko co czwarty Polak boi się, że w czasie pandemii padnie ofiarą hakerów wyłudzających dane osobowe. Równocześnie blisko 60 proc. respondentów nie wie lub nie jest pewna, jakie działania należy podjąć w takim przypadku. Niestety, nie robimy wszystkiego, żeby zapobiec podobnym sytuacjom. 1/3 z nas nie dba o to, by hasło do logowania w banku lub serwisie internetowym było odpowiednio trudne, a ponad 20 proc. ankietowanych nigdy go nie zmieniło.

To wyniki badania przeprowadzonego przez serwis ChronPESEL.pl i Krajowy Rejestr Długów pod patronatem Urzędu Ochrony Danych Osobowych, a zaprezentowane podczas webinarium, które odbyło się 28 maja 2021 r. Raport pt. „Zagrożenia dla bezpieczeństwa i ochrony danych z zdaniem Polaków" zawiera analizę wyników badania oraz komentarze i wskazówki ekspertów na co dzień zajmujących się ochroną danych osobowych na temat wniosków wynikających ze sprawdzenia stanu wiedzy Polaków na temat zagrożeń związanych z bezpieczeństwem w cyberprzestrzeni.

Prezentacji wyników badań towarzyszyła debata z udziałem ekspertów z zakresu ochrony danych osobowych. „Zagrożenia dla bezpieczeństwa i ochrony danych zdaniem Polaków po 3 latach obowiązywania RODO – wyzwania, trendy, możliwości”- to temat dyskusji, do której zostali zaproszeni Monika Krasińska, dyrektor Departamentu Orzecznictwa i Legislacji, UODO, Bartłomiej Drozd, ekspert z serwisu ChronPESEL.pl oraz r.pr. Macieja Gawroński, Gawroński & Partners.

Podczas dyskusji zostały przedstawione zagrożenia i zasady ochrony danych osobowych. Prelegenci odnieśli się także do zaprezentowanych wyników raportów, omówili trendy i wyzwania w ochronie danych oraz nowoczesnych technologii. Dużą część dyskusji poświęcono ochronie numeru PESEL. Monika Krasińska, dyrektor Departamentu Orzecznictwa i Legislacji UODO podkreśliła, że z jednej strony numer PESEL jest niepowtarzalny, nie podlega zmianie i należy go chronić, a z drugiej strony tworzone są rejestry ujawniające numer PESEL i jednocześnie pozbawiające go jakiejkolwiek ochrony, czyniąc go powszechnie dostępnym.

Podczas rozmowy podniesiono także jak ważną rolę w każdej organizacji pełni inspektor ochrony danych.

Czas trwania pandemii COVID-19 i konieczność zastosowania rozwiązań, takich jak: świadczenie pracy w trybie zdalnym, realizacja nauczania dzieci i młodzieży metodami na odległość czy powszechne użycie e-usług w większości branż, spowodował nie tylko powszechne przyspieszenie transformacji cyfrowej, ale również wzmożoną aktywność cyberprzestępców. Jednym z bardziej pożądanych przez nich obecnie „towarów” są dane osobowe, dzięki którym mogą zyskać dostęp do wielu dóbr. Z kolei brak prawidłowych nawyków osób fizycznych, dzięki którym mogą zabezpieczyć swoje dane osobowe czy zbyt frywolne traktowanie przez administratorów zasad ochrony danych osobowych, może prowadzić do negatywnych konsekwencji. Dlatego tak ważne są działania edukacyjne, które przyczyniają się do podniesienia świadomości społecznej w obszarze ochrony danych osobowych wielu grup społecznych i zawodowych o zróżnicowanym przekroju wiekowym.

KOMENTARZE EKSPERTÓW UODO DO RAPORTU

"Zagrożenia dla bezpieczeństwa i ochrony danych zdaniem Polaków"

JACEK MŁOTKIEWICZ

Dyrektor Departamentu Kontroli i Naruszeń UODO

Zarówno ataki hakerskie, jak i wycieki danych w podmiotach prywatnych czy publicznych są to naruszenia, z którymi wiąże się też wiele obowiązków dla podmiotów, które danymi dysponują - administratorów danych.

Powinny one przede wszystkim niezwłocznie powiadomić osoby, których dane przetwarzają o zaistniałej sytuacji i to w taki sposób, aby osoby te mogły zrozumieć, co się stało z ich danymi osobowymi oraz co to dla nich oznacza. Szczególnie istotne jest, aby podmiot profesjonalnie zajmujący się danymi - administrator - wskazał możliwe konsekwencje zdarzenia oraz jakie działania po jego stronie, jak i po stronie osoby, których dane dotyczą, mogą zminimalizować ewentualne negatywne skutki naruszenia. Ważne jest też podanie kontaktu, gdzie można uzyskać więcej informacji na temat naruszenia. Wywiązywanie się przez dysponentów danych z powyższych obowiązków może znacznie wpłynąć na świadomość osób, których dane dotyczą zarówno co do istniejących zagrożeń, jak i sposobów radzenia sobie z ich skutkami.

Jak wynika z przeprowadzonego badania co czwarty Polak boi się, że w czasie pandemii padnie ofiarą hakerów wyłudzających dane osobowe. I nie jest to obawa bezzasadna. W sytuacji wprowadzenia w kraju szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych osobisty kontakt obywatela z instytucjami państwowymi, bankami, firmami jest znacznie utrudniony. Skutkuje to zwiększeniem ryzyka wyłudzenia danych m.in. poprzez oszustwa typu „phishing” lub wykorzystanie socjotechnik bazujących na niewystarczającej wiedzy czy też naiwności ludzi.

Celem ataku jest np. kradzież informacji potrzebnych do logowania, szczegółów kart kredytowych czy wrażliwych danych. Nakładają się na to również problemy z funkcjonowaniem systemów państwowych (np. system profilu zaufanego, system e-rejestracja) poprzez ich zbyt duże, chwilowe obciążenie liczbą zleconych do realizacji zadań. Co za tym często osoby chcące skontaktować się z daną instytucją mogły jedynie skorzystać z kontaktu telefonicznego, który ułatwia hakerom stosowanie socjotechnik.

BARTŁOMIEJ ŻEROMSKI

Dyrektor Departamentu Skarg UODO

Z opublikowanego raportu „Zagrożenia dla bezpieczeństwa i ochrony danych zdaniem Polaków" wynika, że blisko 2/3 dorosłych Polaków deklaruje, że wie, jakie działania należy podjąć w przypadku wyłudzenia lub kradzieży danych osobowych. Co należy wskazać, ankietowani uznali, że najmniejsze zagrożenie w postaci wyłudzenia/kradzieży danych pochodzi z instytucji państwowych.

Jak wynika z przeprowadzonych badań, najlepiej przygotowani do takich sytuacji są ludzi młodzi w wieku między 18 a 24 rokiem życia. Blisko 74 proc. z nich zadeklarowało, że poradziłoby sobie w takim przypadku. Należy jednak mieć też na uwadze, że nawet postępując, zgodne ze wszystkimi zasadami bezpieczeństwa możemy nie uchronić się przed wykorzystaniem naszych danych osobowych, gdy dojdzie do utraty kontroli nad danymi.

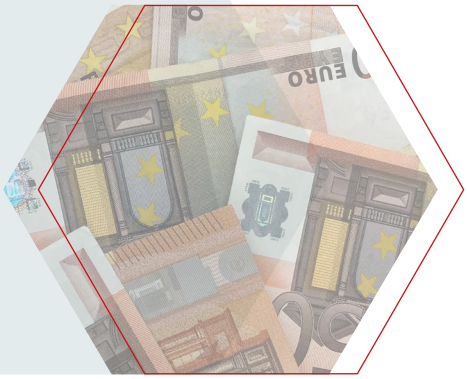
Pozyskując nasze dane osobowe, jedni wykorzystują je w celach przestępczych (jak zawieranie umów, pożyczek czy umów kredytowych na cudze dane), inni w celach marketingowych i sprzedażowych. Niezależnie od celu, w którym zostaną wykorzystane nasze dane dobrze wiedzieć jak się zabezpieczyć przed sytuacją, aby nasze dane nie wpadły w niepowołane ręce. Aby zminimalizować ryzyko utraty tożsamości warto przestrzegać kilku podstawowych zasad, jak nie podawanie w Internecie, w tym na portalach społecznościowych, zbyt wielu informacji o sobie, swoich bliskich i znajomych, nie zamieszczanie w sieci zdjęć, które mogą świadczyć o naszym stanie majątkowym. Posiadanie kilku adresów e-mail wykorzystywanych wyłącznie np. do rejestracji na portalach społecznościowych, grach, sklepów internetowych powoduje, że nawet w przypadku utraty kontroli nad pocztą jesteśmy w stanie ograniczyć wpływ tego zdarzenia na nasze życie.

Używajmy trudnych do odgadnięcia haseł i okresowo je zmieniajmy. Co prawda w przeprowadzonych badaniach blisko 2/3 deklaruje, że używa bardzo trudnych lub trudnych haseł dostępu do serwisów, ale już tylko 20 proc. ankietowanych zmienia hasło do konta bankowego raz w miesiącu lub częściej, 1/3 osób (34,6 proc.) robi to raz na pół roku. Natomiast 22 proc. nigdy tego nie zrobiło. Jeszcze rzadziej zmieniamy hasła do skrzynki mailowej i portali społecznościowych.

Raport „Zagrożenia dla bezpieczeństwa i ochrony danych zdaniem Polaków" wyraźnie pokazuje, że nieustanna edukacja społeczeństwa ma sens. Polacy są coraz bardziej świadomości i głodni wiedzy na temat ochrony danych osobowych. Wiele osób zaczęło odważniej korzystać ze swoich praw. Pytają administratorów o podstawę uprawniającą do przetwarzania ich danych. Korzystają też z prawa wniesienia skargi do Prezesa UODO.

Wielu Polaków zrozumiało bowiem, że ochrona własnych danych osobowych to przejaw dbania o własne bezpieczeństwo oraz prywatność.

Zapis spotkania jest udostępniony na stronie internetowej Urzędu: https://uodo.gov.pl/pl/138/2058



Holandia: kara dla gminy miejskiej za śledzenie sieci Wi-Fi

Holenderski organ ochrony danych nałożył karę na gminę miejską Enschede w wysokości 600 tys. euro za stosowanie śledzenia sieci Wi-Fi w centrum miasta w sposób, który jest zabroniony. Śledzenie sieci Wi-Fi umożliwiło śledzenie klientów sklepów oraz osób mieszkających lub pracujących w centrum miasta.

W 2017 roku gmina miejska Enschede postanowiła zmierzyć, jak bardzo zatłoczone było centrum miasta, wykorzystując do tego celu czujniki. Zakontraktowała firmę, która specjalizuje się w przeprowadzaniu liczenia ludzi. Na ulicach handlowych umieszczono wyposażenie z czujnikami, które wykrywały sygnały sieci Wi-Fi z telefonów komórkowych przechodniów. Każdy telefon był rejestrowany osobno i otrzymywał unikalny kod. Umożliwiło to zmierzenie jak bardzo zatłoczona jest ulica, licząc, ile telefonów znajduje się w pobliżu czujnika w danym miejscu.

Postępowanie prowadzone przez organ ochrony danych w gminie miejskiej Enschede wykazało, że liczenie ludzi zmieniło się w ich śledzenie. Prywatność ludzi nie była należycie chroniona, ponieważ można było ich śledzić bez potrzeby.

Naruszenie rozpoczęło się w maju 2018 r., a po interwencji organu ochrony danych gmina miejska zaprzestała 1 maja 2020 r. stosowania śledzenia Wi-Fi.

Gmina miejska Enschede zgłosiła sprzeciw wobec tej decyzji.

Źródło: https://edpb.europa.eu/news/national-news/2021/dutch-dpa-fines-municipality-wi-fi-tracking_pl

Islandia: InfoMentor z karą za niewłaściwą ochronę danych osobowych

Islandzki organ ochrony danych ukarał przedsiębiorstwo InfoMentor sumą 3.5 mln koron (23,1 tys. euro) za niezapewnienie odpowiedniego bezpieczeństwa danych osobowych w systemie informacyjnym „Mentor" dla szkół i innych podmiotów pracujących z dziećmi.

Ze względu na lukę w systemie, która powodowała, że sześciocyfrowy numer systemowy każdego użytkownika był widoczny w adresie URL konkretnej strony w systemie Mentor, nieupoważnione podmioty uzyskały dostęp do krajowych numerów identyfikacyjnych i awatarów ponad 400 dzieci. Incydent ten został zgłoszony jako naruszenie danych w lutym 2019 roku.

Przedsiębiorstwo InfoMentor przyznało, że wiedziało o luce w systemie i że rozwiązanie dla problemu zostało już stworzone. Z powodu błędu ludzkiego, rozwiązanie to nie zostało w pełni wdrożone do systemu aż do momentu, gdy doszło do naruszenia danych.

InfoMentor omyłkowo wysłało również krajowe numery identyfikacyjne uczniów, których dotyczyło naruszenie danych, do niewłaściwych szkół i inspektora ochrony danych.

Najistotniejszymi czynnikami przy ustalaniu wysokości administracyjnej kary pieniężnej były: liczba osób, których dane dotyczą, bezpośrednio i potencjalnie dotkniętych naruszeniem danych, fakt, że osoby, których dane dotyczą, są dziećmi oraz że główną działalnością InfoMentor jest opracowywanie i obsługa systemu informacyjnego przeznaczonego dla szkół i innych podmiotów pracujących z dziećmi. Nie było jednak dowodów na to, że osoby, których dane dotyczą, poniosły szkodę, a InfoMentor podjęło liczne kroki w celu zwiększenia bezpieczeństwa danych osobowych w systemie.

Źródło: https://edpb.europa.eu/news/national-news/2021/icelandic-dpa-issues-fine-infomentor-i-nadequate-protection-personal-data_pl

NOWE ODPOWIEDZI NA PYTANIA INSPEKTORÓW

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

Wyjaśnienia dotyczą takich kwestii, jak:

Czy administrator jest zobowiązany na podstawie RODO do zapewnienia inspektorowi zespołu IOD?

Czy z zewnętrznym IOD należy zawrzeć umowę powierzenia?

Jaka powinna być podstawa prawna przetwarzania danych osobowych osób wystawiających referencje?

URZĄD OCHRONY DANYCH OSOBOWYCH