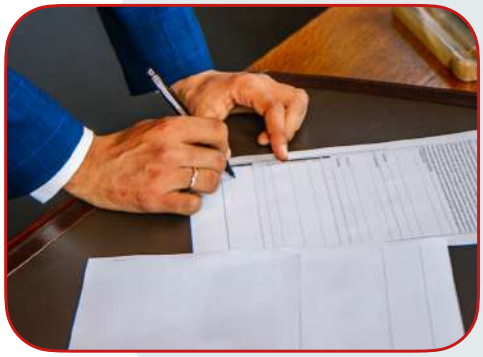
Nr 8-9/2022 (41/42)
Sierpień-wrzesień 2022

URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

NIEKTÓRE Z PRZEPISÓW USTAWY IMPLEMENTUJĄCEJ DYREKTYWĘ POLICYJNĄ DOTYCZĄCE IOD WYMAGAJĄ ZMIAN



Z wnioskiem w tej sprawie Prezes UODO zwrócił się do Ministra Spraw Wewnętrznych i Administracji, wskazując, że jest to istotne dla zapewnienia odpowiedniego statusu inspektora ochrony danych.

W wystąpieniu w tej sprawie organ nadzorczy wskazał, że ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (wdrażająca do polskiego porządku prawnego tzw. dyrektywę policyjną, czyli dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 209/977/WSiSW) wymaga zmian w zakresie przepisów dotyczących inspektora ochrony danych.

Błędne przypisanie zadań

W ocenie UODO zmiany wymagają art. 37 ust. 3 i art. 38 ust. 6 powołanej ustawy z dnia 14 grudnia 2018 r., gdyż są one sprzeczne z przepisami tzw. dyrektywy policyjnej. Z przepisów tych wynika, że zarówno przeprowadzenie oceny skutków dla ochrony danych, jak i uprzednich konsultacji administrator może powierzyć inspektorowi ochrony danych. Tymczasem przeprowadzenie oceny skutków dla ochrony danych i wystąpienie z wnioskiem o uprzednie konsultacje do organu nadzorczego to zadania administratora i to właśnie jemu są one przypisane w dyrektywie. Ich realizacja przez IOD prowadziłaby zaś do powstania konfliktu interesów.

Błędna i wymagająca zmiany jest również redakcja art. 38 ust. 6. Artykuł ten stanowi, że realizację obowiązków, o których mowa w ust. 1– 4 tego artykułu, administrator lub podmiot przetwarzający może powierzyć inspektorowi ochrony danych. Tymczasem ust. 2 i 4 tego przepisu odnoszą się do zadań Prezesa UODO, wobec tego przypisanie ich IOD oznacza błędne sformułowanie przepisu.

Braki w przepisach regulujących dokonywanie zawiadomień dotyczących IOD

Brakuje też precyzyjnych przepisów określających, jakie dane administratora powinny być przekazane przez niego do Prezesa UODO w związku z dokonywaniem zawiadomienia dotyczącego inspektora ochrony danych (wyznaczenia, odwołania, zmiany danych IOD). Ponadto potrzebne są regulacje, na mocy których administrator byłby zobowiązany do powiadomienia Prezesa UODO o każdej zmianie danych odnoszących się do administratora. Tymczasem ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych takie przepisy zawiera.

Kontrola stosowania przepisów dotyczących IOD

Skorygowanie dostrzeżonych braków i nieprawidłowego brzmienia wskazanych przepisów ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości ma istotne znaczenie nie tylko z punktu widzenia zapewnienia właściwej implementacji tzw. dyrektywy policyjnej i zapewnienia odpowiedniego statusu inspektora ochrony danych. To ważne również w kontekście prowadzonej przez organ nadzorczy weryfikacji przestrzegania przepisów dotyczących IOD, o rozpoczęciu której informowaliśmy w Newsletterze UODO dla IOD z kwietnia br. (nr 4/2022) w tekście „Ocena przestrzegania przepisów dotyczących funkcjonowania IOD". W dalszych etapach obejmie ona bowiem również wykonywanie przepisów ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

JAK STAROSTOWIE POWINNI POSTĘPOWAĆ ZE ZNALEZIONYMI NOŚNIKAMI DANYCH OSOBOWYCH?

Starostowie, realizując zadania określone w ustawie o rzeczach znalezionych, muszą pamiętać, że w sytuacji, w której mają do czynienia z nośnikami mogącymi zawierać dane osobowe, muszą przestrzegać przepisów RODO.

Do UODO wciąż wpływają sygnały świadczące o problemach ze stosowaniem przez starostów przepisów ustawy z dnia 20 lutego 2015 r. o rzeczach znalezionych. Zobowiązują ich one do zabezpieczenia znalezionych rzeczy, jednak nie wynika z nich, w jakim zakresie ponoszą oni odpowiedzialność za dane osobowe utrwalone na znalezionych nośnikach, takich jak np. laptopy, telefony komórkowe, pendrive'y, dyski, aparaty fotograficzne czy tablety, ani jak powinni z nimi postępować. W odpowiedzi na wystąpienie organu nadzorczego udzielonej przez resort spraw wewnętrznych i administracji wskazano, że przedstawione zagadnienie znajduje się poza zakresem kompetencji Ministra Spraw Wewnętrznych i Administracji. Jak jednocześnie zaznaczono, ponieważ problematyka rzeczy znalezionych mieści się w szeroko rozumianym pojęciu prawa cywilnego, a projekt obowiązującej ustawy o rzeczach znalezionych został przygotowany przez resort sprawiedliwości, to niniejsze zagadnienie powinno zostać poddane ocenie tego resortu. Z kolei w odpowiedziach udzielonych organowi nadzorczemu przez Ministerstwo Sprawiedliwości podano w wątpliwość konieczność dokonywania zmian przepisów ustawy o rzeczach znalezionych, odsyłając jednocześnie do MSWiA i resortu cyfryzacji jako właściwych w zakresie kształtowania zakresu i sposobu realizacji zadań zleconych z zakresu administracji rządowej przez starostów. **W ocenie organu nadzorczego kwestie te wymagają doprecyzowania. Jednak podjęte w tej sprawie działania (o których UODO informuje na stronie internetowej w materiale „Potrzebne przepisy dotyczące postępowania z danymi osobowymi utrwalonymi na zagubionych nośnikach") nie doprowadziły** do przygotowania przez projektodawcę stosownych zmian w obowiązujących przepisach prawa. W tej sytuacji zasadne jest, by starostowie problemy z praktycznym stosowaniem przepisów ustawy o rzeczach znalezionych sygnalizowali odpowiednim resortom, wskazując jednocześnie na potrzebę podjęcia prac legislacyjnych w tym zakresie.

Podkreślić należy, że w sytuacji, w której starostowie mają do czynienia ze znalezionymi nośnikami mogącymi zawierać dane osobowe, muszą przestrzegać przepisów RODO.
Zgodnie bowiem z definicją wyrażoną w art. 4 pkt 2 RODO przetwarzanie danych osobowych obejmuje m.in. takie operacje, jak: przechowywanie, przeglądanie, usuwanie lub niszczenie (art. 4 pkt 2 RODO).
Co istotne, to na administratorze spoczywa obowiązek przetwarzania danych zgodnie z zasadami określonymi w art. 5 RODO, w tym wyrażoną w art. 5 ust. 1 lit. f RODO zasadą poufności. Zgodnie zaś z motywem 39 RODO dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu. Zatem starostowie, realizując obowiązki nałożone na nich przepisami ustawy o rzeczach znalezionych, powinni zadbać, aby dane osobowe nie zostały udostępnione osobom nieuprawnionym.

ZALECENIA DOTYCZĄCE PRACY Z UCZNIEM NIE DO DZIENNIKA LEKCYJNEGO

W obecnym stanie prawnym brak jest podstaw, by w dzienniku lekcyjnym zamieszczać informacje o zaleceniu pracy z uczniem wynikającym z orzeczenia lub opinii poradni psychologiczno-pedagogicznej. Informacje o uczniu dotyczące kształcenia specjalnego, zajęć rewalidacyjno wychowawczych lub pomocy psychologiczno-pedagogicznej powinny być zamieszczane w indywidualnej teczce ucznia.

Zakres danych zamieszczanych w dzienniku lekcyjnym został szczegółowo określony w przepisach rozporządzenia Ministra Edukacji Narodowej z dnia 25 sierpnia 2017 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (§ 8). Jednocześnie rozporządzenie to stanowi (§ 19), że „Przedszkole, szkoła i placówka gromadzi, w indywidualnej teczce, dla każdego dziecka, ucznia, uczestnika zajęć rewalidacyjno-wychowawczych, słuchacza lub wychowanka objętego odpowiednio kształceniem specjalnym, zajęciami rewalidacyjno-wychowawczymi lub pomocą psychologiczną dokumentację badań i czynności uzupełniających prowadzonych w szczególności przez pedagoga,

psychologa, logopedę, doradcę zawodowego, terapeutę pedagogicznego, lekarza oraz innego specjalistę, a także indywidualne programy edukacyjno-terapeutyczne, o których mowa w art. 127 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe, oraz indywidualne programy zajęć, o których mowa w § 12 ust. 2 i 3”. Brak jest więc podstaw, aby w dzienniku lekcyjnym zamieszczać informacje o zaleceniu pracy z uczniem wynikającym z orzeczenia lub opinii poradni psychologiczno-pedagogicznej.

Jednocześnie szkoła, podobnie jak każdy administrator, powinna dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą. Przede wszystkim jest obowiązana zapewnić, aby przetwarzane przez nią dane osobowe były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane (zgodnie z zasadami ograniczenia celu i minimalizacji określonymi w art. 5 RODO). Jest też zobowiązana do zapewnienia, by były prawidłowo zabezpieczone i nieudostępniane osobom do tego nieuprawnionym.

UDOSTĘPNIANE DANYCH OSOBOWYCH PRZEDSTAWICIELOWI PORADNI PSYCHOLOGICZNO-PEDAGOGICZNEJ UCZESTNICZĄCEMU W PRACACH ZESPOŁU DS. OPRACOWANIA IPET

Nie ma potrzeby uzyskiwania zgody rodziców na udostępnienie danych osobowych ucznia pracownikowi poradni psychologiczno-pedagogicznej biorącemu udziału w pracach zespołu ds. opracowania indywidualnego programu edukacyjno-terapeutycznego (IPET), gdyż podstawą tego udostępnienia są przepisy prawa.

Zgodnie z § 6 ust. 8 pkt 1 rozporządzenia Ministra Edukacji Narodowej z dnia 9 sierpnia 2017 r. w sprawie warunków organizowania kształcenia, wychowania i opieki dla dzieci i młodzieży niepełnosprawnych, niedostosowanych społecznie i zagrożonych niedostosowaniem społecznym do kompetencji dyrektora szkoły należy wnioskowanie o udział w posiedzeniach zespołu ds. opracowania IPET m.in. przedstawiciela poradni psychologiczno-pedagogicznej. Stosownie do § 6 ust. 9 tego rozporządzenia zespół, co najmniej dwa razy w roku szkolnym, dokonuje okresowej wielospecjalistycznej oceny poziomu funkcjonowania

ucznia, uwzględniając ocenę efektywności programu oraz, w miarę potrzeb, dokonuje modyfikacji programu. Okresowej wielospecjalistycznej oceny poziomu funkcjonowania ucznia i modyfikacji programu dokonuje się, w zależności od potrzeb, we współpracy z poradnią psychologiczno-pedagogiczną, w tym poradnią specjalistyczną, a także – za zgodą rodziców ucznia – z innymi podmiotami.
Zatem nie ma potrzeby uzyskiwania zgody rodziców na udostępnienie danych osobowych ucznia przedstawicielowi poradni psychologiczno-pedagogicznej biorącemu udział w pracach tego zespołu, gdyż podstawą tego udostępnienia są powyższe przepisy prawa.
Jednocześnie warto przypomnieć, że obszerny materiał dotyczący podstaw przetwarzania danych osobowych przez poradnie psychologiczno-pedagogiczne jest dostępny na stronie internetowej UODO („**Jaka jest podstawa do przetwarzania przez poradnie psychologiczne szczególnych kategorii danych?**”).
Z kolei w Newsletterze UODO dla IOD ze stycznia br. (nr 1/2022) w tekście pt. „Będzie właściwa podstawa przetwarzania danych osobowych w poradniach psychologiczno-pedagogicznych” informowaliśmy o zmianach w przepisach dotyczących poradni psychologiczno-pedagogicznych.

MNIEJ DANYCH O KANDYDATACH NA ŁAWNIKÓW

Projektodawca uwzględnił uwagi UODO i zweryfikował zakres danych, jaki ma być pozyskiwany o kandydatach na ławników.

Organ nadzorczy, opiniując projekt rozporządzenia Ministra Sprawiedliwości zmieniającego rozporządzenie w sprawie sposobu postępowania z dokumentami złożonymi radom gmin przy zgłaszaniu kandydatów na ławników oraz wzoru karty zgłoszenia, zgłosił zastrzeżenia do załącznika zawierającego wzór karty zgłoszenia kandydata na ławnika. Zakwestionował zakres danych, jakie miałyby być pozyskiwane o kandydatach na ławnika. UODO podniósł, że wzgląd na określone w RODO zasady minimalizacji danych i ograniczenia celu przemawia za rezygnacją ze zbierania takich danych, jak imiona rodziców i miejsca urodzenia kandydata na ławnika. W przedstawionej opinii organ nadzorczy wskazał, że imiona rodziców uznać należy za dane osobowe osób trzecich, które pozostają z kandydatem na ławnika w stosunku stricte osobistym, i których dane osobowe nie powinny być wykorzystywane dla realizacji celu związanego z ubieganiem się o stanowisko ławnika. Poza tym niezrozumiałe jest pozyskiwanie tych danych dla (jak się wydaje) celu jednoznacznej identyfikacji osoby fizycznej w sytuacji, gdy od wielu lat na te

potrzeby wykorzystywany jest numer PESEL, którego pozyskiwanie projektowane rozporządzenie przewiduje. UODO za nadmiarowe uznał również pozyskiwanie informacji o miejscu urodzenia ławnika. W związku z tym wniósł o weryfikację projektowanego wzoru karty zgłoszenia kandydata na ławnika i usunięcie z jego treści kwestionowanych danych. Zgłoszone uwagi zostały przez projektodawcę uwzględnione w całości.

UPOMNIENIE ZA BRAK PRAWIDŁOWEGO ZAWIADOMIENIA O NARUSZENIU OSÓB, KTÓRYCH DANE DOTYCZĄ

Gdy dochodzi do naruszenia ochrony danych osobowych, które może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki powinien zawiadomić osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie należy sporządzić jasnym i prostym językiem, z podaniem wszystkich informacji wymaganych przepisami prawa art. 34. ust.2 RODO.

W czerwcu 2022 roku organ nadzorczy wydał decyzję upominającą jednego z administratorów w sprawie sposobu zawiadomienia o naruszeniu ochrony danych osobowych osób, których te dane dotyczą.

Chodzi o sprawę, w której administrator dokonał zgłoszenia naruszenia ochrony danych osobowych polegającego na uzyskaniu nieuprawnionego dostępu do służbowego konta poczty elektronicznej pracownika spółki. Administrator ustalił w szczególności, że dane osób, których dotyczyło zgłoszone naruszenie obejmowały m.in.: imię, nazwisko, adres zamieszkania/adres korespondencyjny, numer PESEL oraz numer dokumentu tożsamości (dowód osobisty/paszport).

W zgłoszeniu administrator poinformował, że dokonał zawiadomienia osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych, a także przedstawił zanonimizowaną treść zawiadomienia, które skierował do tych osób.

W wyniku analizy treści zawiadomienia UODO uznał, że pierwotne zawiadomienie osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych nie zawierało wymaganych stosownie do art. 34 ust.2 RODO informacji:

- opisu charakteru naruszenia ochrony danych osobowych,
- imienia i nazwiska oraz danych kontaktowych inspektora ochrony danych lub oznaczenia innego punktu kontaktowego, od którego można uzyskać więcej informacji,
- opisu możliwych konsekwencji naruszenia ochrony danych osobowych oraz
- opisu środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

W związku z tym organ nadzorczy zwrócił się do administratora o podjęcie stosownych działań mających na celu niezwłoczne, ponowne i prawidłowe, tj. obejmujące wszystkie ww. i wymagane prawem elementy.

Analiza kolejnego zawiadomienia wykazała, że administrator nadal nie zawarł wszystkich wymaganych elementów, stosownie do art. 34 ust. 2 RODO. Pominięto opis charakteru naruszenia ochrony danych osobowych uwzględniającego kategorie danych osobowych objęte naruszeniem, czy opis możliwych konsekwencji naruszenia ochrony danych osobowych. Spółka poprzestała jedynie na ogólnych sformułowaniach.

Wskazanie wymaganych przepisami prawa informacji nastąpiło dopiero po wszczęciu przez Prezesa UODO postępowania administracyjnego.

Pełna treść decyzji DKN.5131.14.2022

IM WIĘCEJ INTERNETU, TYM BARDZIEJ WARTO ZADBAĆ O PRYWATNOŚĆ

O wpływie Internetu i nowych technologii na kształtowanie bezpiecznych zachowań w sieci z dr. Sylwestrem Bębasem rozmawia Ewelina Janczylik-Foryś

Sylwester Bębas - doktor nauk społecznych, nauczyciel akademicki, psychoterapeuta, pedagog, profilaktyk specjalizujący się w uzależnieniach od świata wirtualnego i bezpiecznych zachowaniach w sieci, trener kompetencji medialnych, wychowawczych i interpersonalnych

Nowoczesne technologie informacyjne, których symbolem stał się komputer i Internet, budzą zainteresowanie wszystkich grup wiekowych. Z przeprowadzonego badania „Ochrona danych osobowych w 2022 r". wynika, iż młodzi ludzie uważają, że wszystko wiedzą o nowych technologiach, a osoby nieco starsze już niekoniecznie. Czy Pana zdaniem raport prawidłowo ocenia zachowania i świadomość grup wiekowych?

– Żyjemy w świecie, w którym ludzie powszechnie korzystają z Internetu. I nic w tym dziwnego, bowiem Internet służy do różnych celów do pracy, nauki, rozrywki, komunikacji itp. Używany jest przez osoby w różnym wieku, z różnym wykształceniem. Oprócz zalet niesie ze sobą wiele zagrożeń. Codziennie wykradanych jest wiele milionów rekordów, pojawia się też wiele prób instalowania złośliwego oprogramowania. Dane użytkowników sieci stały się cennym towarem na rynku cyberprzestępczym. Zakupem takich informacji zainteresowani są także tzw. brokerzy danych. Skupują oni informacje o ludziach, aby później sprzedać je zainteresowanym firmom. Raport jest spójnym wartościowym dokumentem podnoszącym świadomość na temat bezpieczeństwa danych osobowych w Polsce przeprowadzonym na reprezentatywnej grupie badanych. Raport ukazuje najważniejsze zagrożenia, niebezpieczne zachowania, konsekwencje utraty danych osobowych, działania profilaktyczne, zachowania Polaków w tym zakresie, ma wartość diagnostyczną, edukacyjna i profilaktyczną. Przekonanie młodych ludzi o tym, że wszystko wiedzą o nowych technologiach jest złudne, dlatego potrzebna jest edukacja medialna wszystkich grup wiekowych.

Bardzo ważną rolę w zapewnieniu bezpieczeństwa swoim dzieciom odgrywają rodzice, którzy powinni mieć świadomość zagrożeń, z którymi może spotkać się dziecko w sieci, oraz dysponować wystarczającą wiedzą i umiejętnościami, aby zadbać o to bezpieczeństwo. Rodzice powinni: ograniczać czas spędzany przez dzieci w sieci, rozmawiać z dzieckiem na temat bezpiecznego korzystania z Internetu, kontrolować i nadzorować aktywność dziecka w sieci, sprawdzać strony, na które zagląda dziecko, ustalić reguły, zasady i ograniczenia związane z dostępem do Internetu. Podniesienie poziomu bezpieczeństwa dzieci on-line zależy również od dostawców usług internetowych i producentów sprzętu elektronicznego oraz oprogramowania. Rozwiązania technologiczne w dużym stopniu mogą wpływać na poziom bezpieczeństwa dzieci on-line i mogą stanowić dla opiekunów młodych internautów pomoc w czuwaniu nad ich bezpieczeństwem.

90 procent Polaków deklaruje, że wie, jak zadbać o bezpieczeństwo swoich danych osobowych. Najpewniej czują się ludzie młodzi. Pomimo przekonania o swojej wiedzy, to oni są jednak grupą, która najczęściej popełnia błędy w postaci publikacji zdjęć swoich dokumentów w sieci lub udostępnia osobom trzecim loginy i hasła. Jednak młodzi ludzie nie są tacy uświadomieni jak im się wydaje…

– Dlatego potrzebna jest stała edukacja zwłaszcza na temat podstawowych zasad bezpieczeństwa. Po pierwsze, nie powinno używać się tego samego loginu i hasła do wielu usług i serwisów. Po drugie, myśleć o tym, komu i w jakim celu udostępniamy nasze dane. Nie każdy serwis musi wiedzieć o nas wszystko. Już w momencie podawania rozmaitych danych podczas rejestracji niekiedy powinno zapalić się nam w głowie czerwone światło ostrzegawcze. Po trzecie, jeżeli mamy taką możliwość, zawsze powinniśmy korzystać z uwierzytelniania dwuetapowego (np. potwierdzenie logowania kodem SMS, odciskiem palca czy korzystać z systemu rozpoznawania twarzy). Warto też uświadamiać jakie dane te zwykłe i te wrażliwe chronić. Należy zwrócić uwagę na: imię i nazwisko, numer identyfikacyjny (np. PESEL, NIP, numer dowodu osobistego), adres zamieszkania, adres mailowy, datę urodzin, płeć, kolor oczu, waga, wzrost, dane ujawniające pochodzenie rasowe lub etniczne, dane ujawniające poglądy polityczne, dane ujawniające przekonania religijne lub światopoglądowe, dane ujawniające przynależność do związków zawodowych, dane genetyczne, dane biometryczne (wykorzystywane w celu jednoznacznego zidentyfikowania osoby fizycznej), dane dotyczące zdrowia itp.

Czy Polacy są w stanie sami zadbać o swoje dane osobowe? Zawsze utrata kontroli nas danymi osobowymi to efekt ataków socjotechnicznych. Jedyne co może różnić to sposób działania.

– Dlatego należy edukować, zachęcać do czytania regulaminów. Dość często sami wyrażamy zgodę na to, aby nasze dane, które przesyłamy w jakieś miejsce w sieci lub udostępniamy określonej aplikacji lub serwisowi internetowemu, były udostępniane lub odsprzedawane innym osobom lub firmom. Informacje o tym znajdują się właśnie w regulaminach. Warto czytać na co zgadzamy się, akceptując zgodę na działanie ciasteczek. Są one w zasadzie niezbędne do prawidłowego funkcjonowania stron internetowych.

Poprawiają nasz komfort użytkowania różnych portali i serwisów. Informują też nadawców, jakie treści cieszą się większym, a jakie mniejszym zainteresowaniem. Zresztą zazwyczaj jesteśmy o nich informowani po wejściu pod konkretny adres w sieci. Nie ma w nich nic złego. Zanim na kolejnej stronie zaakceptujecie jednym kliknięciem wszystkie zgody na działanie „ciasteczek", wczytajcie się dokładnie, czego one dotyczą. Pewnie warto poświęcić kilka sekund więcej i dostosować stosowne zgody do własnych potrzeb. Za każdym razem, gdy instalujemy nową aplikację na telefonie lub tablecie, rejestrujemy się do nowego serwisu czy usługi, należy uważnie przeczytać regulamin i zastanowić się, na co właściwie się zgadzamy.

W jaki sposób zachęcić Polaków, w tym zwłaszcza osoby starsze, którym technologie cyfrowe nie są aż tak bliskie, do tego, aby jeszcze większą uwagę zwrócili na potrzebę bezpiecznego posługiwania się własnymi danymi osobowymi w codziennych sytuacjach?

– Przede wszystkim uświadamiać, że w sieci użytkownik Internetu narażony jest na różnego rodzaju oszustwa, które mają na celu np. okradzenie, oszukanie lub wykorzystanie danej osoby. Jedną z metod cyberoszustwa jest tzw. phishing – przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji np. danych logowania czy danych karty kredytowej, następuje zainfekowanie urządzenia szkodliwym oprogramowaniem i nakłonienie ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej. Jeszcze inną formą oszustwa jest spear phishing, czyli cyberpolowanie z harpunem na wybraną osobą. O ile w przypadku phishingu zarzucana najczęściej jest sieć, z nadzieją, że złapią się na nią jakieś ofiary, tak w przypadku spear phishingu cyberprzestępca poluje na jedną, konkretną ofiarę. Z kolei clone phishing jest typem phishingu, w którym prawdziwy e-mail posiadający załącznik lub link zostaje użyty przez przestępcę jako wzór przy tworzeniu wiadomości na potrzeby oszustwa. Załączniki lub linki zostają zastąpione złośliwymi wersjami, a następnie wysłane z adresu e-mail sfałszowanego tak, aby wyglądał jak ten należący do nadawcy. Whaling jest z kolei oszustwem, gdzie część ataków phishingowych zostaje skierowana w szczególności do kierownictwa wyższego szczebla lub jest ukierunkowana na pozyskanie informacji z branży biznesowej objętych tajemnicą. W przypadku ataków tego typu, sfałszowana witryna lub wiadomość jest tworzona z uwzględnieniem np. stanowiska jakie zajmują ofiary ataków w firmie. Treść e-maili często przypomina pisma pochodzące z kancelarii prawnych lub urzędów państwowych. Taka wiadomość może zawierać załącznik w postaci złośliwego oprogramowania i nakłaniać ofiarę do jego instalacji np. w celu uzyskania dostępu do ważnego dokumentu. Cyberoszuści mogą proponować także fałszywą pomoc techniczną, w której przestępca próbuje zastraszyć ofiarę i skłonić ją do zapłacenia za zbędną pomoc techniczną. Metoda ta wykorzystuje brak wiedzy informatycznej ofiary. Pharming jest bardziej niebezpieczną dla użytkownika oraz trudniejszą do wykrycia formą phishingu. Charakterystyczne dla pharmingu jest to, że nawet po wpisaniu prawidłowego adresu strony WWW, ofiara zostanie przekierowana na fałszywą, choć mogącą wyglądać tak samo, witrynę internetową. Ma to na celu przejęcie haseł, numerów kart kredytowych i innych poufnych danych

wpisywanych przez użytkownika do zaufanych witryn. Z pharmingiem związany jest drive-by pharming, który jest formą zagrożenia internetowego, będącą połączeniem ataku typu pharming, jak i socjotechniki. Celem agresora jest skłonienie ofiary do odwiedzenia przygotowanej wcześniej strony internetowej, zawierającej szkodliwy kod, który ma za zadanie zmianę ustawień na routerze osoby odwiedzającej w taki sposób, że adresy wpisywane przez użytkownika, będą przekierowywane na strony spreparowane przez atakującego. Jeszcze inne oszustwo typu scam polega na wzbudzeniu u kogoś zaufania, a następnie wykorzystanie tego zaufania do wyłudzenia pieniędzy lub innych składników majątku. Osoba wzbudzająca fałszywe zaufanie zwykle działa na jedną z ludzkich cech charakteru, zarówno negatywnych, jak i pozytywnych, takich jak: pycha i chciwość, ale też empatia i altruizm. Jest jeszcze SMS phishing, czyli atak socjotechniczny podobny do phishingu, polegający na rozsyłaniu SMS-ów, które mają skłonić ofiarę do podjęcia określonego działania.

Bardzo często podkreślamy, jak ważna jest edukacja i budowanie odpowiednich postaw wśród użytkowników nowych technologii. Często jednak korzystając z nowoczesnych rozwiązań, nie wiemy jak one działają. Co prawda, co jakiś czas aktualizujemy oprogramowanie w telefonie, ale nie wiemy dlaczego – pewnie dla poprawy funkcjonowania.

– Niestety często nie wiemy, jak działają nowe technologie, dlatego zasady bezpieczeństwa są tu kluczowe. Bardzo ważne jest, aby stosować zasady bezpieczeństwa podczas komunikowania się przez Internet. Nie powinno się rozmawiać z nieznajomymi, poza przypadkami uzasadnionymi np. sprzedawcą w sklepie internetowym, lekarzem itd. Wszystkie osoby, z którymi nawiązywany jest kontakt w sieci nie powinny być anonimowe, tzn. nieznane z imienia i nazwiska. W żadnym wypadku nie powinno się wysyłać nieznajomym plików, w tym zdjęć i filmów, przesyłać spamu, w tym tzw. łańcuszków szczęścia czy otwierać wiadomości z podejrzanymi linkami, które mogą zawierać wirusy i posłużyć do okradzenia danej osoby. Bardzo ważne jest, aby korzystając z Internetu stosować zasady netykiety, która jest rodzajem niepisanych, ale przyjętych i przestrzeganych przez internautów zasad korzystania z sieci m.in. zasad komunikowania się w sieci, jest to rodzaj internetowego savoir-vivre'u. W sieci, tak jak w każdej społeczności, istnieją reguły zachowania się, których należy przestrzegać. Nieprzestrzeganie ich może skutkować uwagami ze strony administratora i innych użytkowników, wykluczeniem z grupy, a nawet całkowitym zablokowaniem dostępu do usług. Bardzo ważne jest korzystanie z Internetu stosować szyfrowanie, które służy do zachowania poufności danych. Plik lub przesyłane dane są zniekształcane tak, że tylko właściwe osoby posiadające tajny „klucz" mogą odtworzyć oryginalny tekst. Gdy ktoś korzysta z urządzeń cyfrowych, cały czas używa systemów opartych na szyfrowaniu: kiedy korzysta z bankowości internetowej, łączy się z siecią Wi-Fi, płaci kartą płatniczą. Wokół prawie każdej czynności w sieci pojawia się szyfrowanie. Dlatego korzystając z poczty, banku lub sklepu internetowego oraz wszystkich stron, na których podaje się swoje dane (login i hasło), należy sprawdzać, czy połączenie jest szyfrowane. Połączenie szyfrowane jest wtedy gdy, w pasku adresu

znajduje się kłódka i napis: „https", gdzie „S" oznacza secure, czyli bezpieczny. Ważne jest, aby urządzenia elektroniczne, z których korzystamy chronić odpowiednim oprogramowaniem, które ułatwia identyfikację zagrożenia wirusowego i pozwala te wirusy skutecznie zwalczać. Wirusy infekują urządzenie gdy ktoś otwiera pocztę od nieznajomych. Najczęściej są to załączniki, które wcale mogą nie wyglądać groźnie. Cyberprzestępcy podszywają się także pod różne instytucje i organizacje. Niebezpieczne jest pobieranie plików z nielegalnie rozpowszechnionymi filmami, grami, programami, aplikacjami, książkami, a niekiedy także z muzyką. Instalując oprogramowanie nie należy klikać w link w wyskakującym okienku z informacją, aby pilnie coś zainstalować. Takie wyskakujące okienka często są pułapką. Linki, które są w nich zawarte, uaktywniają na urządzenie pliku ze złośliwym oprogramowaniem.

Czy powinniśmy się z tym pogodzić, że nie jesteśmy w stanie nadążyć za nowymi rozwiązaniami i po prostu polegać na ogólnych rekomendacjach?

– Internet doprowadził nie tylko do implozji przestrzeni i czasu, ale także znaczeń. Praktycznie wszystko w nim jest akceptowalne i prawie nic nie jest trwałe. Sprzyja to relatywistycznemu sposobowi myślenia. Wzmacnia to niewątpliwie coraz powszechniejszą tendencję do unikania odpowiedzialności osobistej i zaangażowania. Wzrastająca liczba użytkowników Internetu oraz rozwój on-line różnych aspektów ludzkiej działalności dotyczącej wszystkich niemalże sfer życia ludzkiego powoduje, że coraz trudniej wyznaczyć linię demarkacyjną, dzielącą życie wirtualne od życia realnego. Jesteśmy świadkami niebywałego rozwoju technik i technologii teleinformatycznych. Patologie w cyberświecie to nie tylko wyłącznie uzależnienia, ale także inne niebezpieczeństwa i zagrożenia w tym cyberoszustwa i manipulacje. Wraz z rozwojem informatyzacji pojawiły się nowe problemy związane z niewłaściwym zastosowaniem osiągnięć elektronicznego przetwarzania danych. Od pewnego czasu rejestruje się olbrzymie zainteresowanie grup przestępczych wykorzystywaniem infrastruktury sieciowej, jako nowego instrumentu nielegalnej działalności. Obecnie do podstawowych obszarów obejmujących nadużycia w Internecie należą przede wszystkim: ukrywanie tożsamości, nawiązywanie nielegalnych konwersacji/komunikacji, dystrybuowanie nielegalnych materiałów, gry hazardowe, pranie (brudnych) pieniędzy oraz wszelkie działania mające na celu przyniesienie korzyści. Rozszerza się zjawisko kradzieży i wyłudzania danych, a także cyberoszustw i manipulacji. Dlatego powinniśmy systematycznie podnosić nasze kompetencje medialne, być świadomymi i odpowiedzialnymi użytkownikami nowych technologii.

Język wypowiedzi, w jakim są kierowane do użytkowników komunikaty, jest dość trudny. Czy ludzie w ogóle rozumieją język nie tylko RODO, ale wszystkich wiadomości, jakie kierują do na nich administratorzy, deweloperzy aplikacji mobilnych? Jak informować użytkowników o przysługujących im prawach czy o możliwych zagrożeniach?

– Przede wszystkim edukować, uczyć o tych prawach i o możliwych zagrożeniach. Tego, że korzystając

z Internetu nie powinno się używać się tego samego loginu i hasła do wielu usług i serwisów. Należy myśleć o tym, komu i w jakim celu udostępnia się dane. Nie każdy serwis musi wiedzieć wszystko o jego użytkowniku. Jeżeli jest taka możliwość, zawsze powinno się korzystać z uwierzytelniania dwuetapowego np. potwierdzenia logowania kodem SMS, odciskiem palca czy korzystać z systemu rozpoznawania twarzy. Należy być ostrożnym z publikowaniem zdjęć. Nie powinno się publikować w sieci zdjęć, na których ktoś jest niekompletnie ubrany, zdjęć wnętrz mieszkań, zdjęć drogich przedmiotów, zdjęć z wakacji czy zdjęć z prywatnych spotkań. Korzystając z sieci, należy czytać regulaminy. Dość często ludzie sami wyrażają zgodę na to, aby ich dane, które przesyłają w jakieś miejsce w sieci lub udostępniają określonej aplikacji lub serwisowi internetowemu, były udostępniane lub odsprzedawane innym osobom lub firmom. Informacje o tym znajdują się właśnie w regulaminach. Za każdym razem, gdy ktoś instaluje nową aplikację na telefonie lub tablecie, rejestruje się do nowego serwisu czy usługi, powinien uważnie przeczytać regulamin i zastanowić się, na co właściwie się zgadza. Korzystając z sieci należy tworzyć bezpieczne hasła. W dzisiejszym świecie Internetu haseł używamy w zasadzie bez przerwy, przy logowaniu do poczty elektronicznej, bankowości online, dokonując zakupów lub uzyskując dostęp do rozmaitych urządzeń itp. Użytkownicy Internetu, aby łatwiej zapamiętać hasła, używają haseł krótkich, łatwo kojarzących się np. z imieniem swoich zwierząt, bohaterów z filmów, z datą swoich urodzin itp. Takie hasło niestety możne być złamane w kilka sekund. Tymczasem silne hasło nie powinno być słownikowym wyrazem, ale powinno zawierać długi ciąg dużych i małych liter, cyfr i znaków specjalnych. Bardzo dobrym rozwiązaniem podczas korzystania z Internetu jest tzw. uwierzytelnianie wielopoziomowe czyli sposób zabezpieczenia oraz autoryzacji podczas logowania przed skorzystaniem z konta użytkownika przez niepowołane osoby poprzez zdobycie przez nią identyfikatora użytkownika i hasła uwierzytelniającego. Oprócz podania tych danych logowania, użytkownik musi: podać uzyskany kod lub frazę np. ze swojego przenośnego urządzenia internetowego, poprzez przepisanie go z e-maila wysłanego przez serwis, na którym użytkownik próbuje się zalogować, czy też za pomocą specjalnej karty, linii papilarnych palca itp.

Pandemia COVID-19 narzuciła nam konieczność zastosowania e-rozwiązań. Czego się nauczyliśmy przy korzystaniu z e-usług?

– Internet w pandemii okazał się ogromnym dobrodziejstwem dla ludzi, a także dla firm działających on-line. Pierwszą zmianą jest wzrost w obszarze komunikacji – wirtualne kontakty – wideokonferencje, media społecznościowe - niemal zastąpiły komunikację bezpośrednią. Problem mają jednak osoby, które są cyfrowo wykluczone, a jest ich w Polsce około kilkanaście procent. Internet wpłynął znacząco na edukację – np. wprowadzono platformy edukacyjne dzięki, którym możliwe było nauczanie na odległość. W czasach pandemii coraz większą rolę zaczęły odgrywać zakupy on-line, nawet w takich branżach jak spożywcza, do tej pory zarezerwowana do zakupów stacjonarnych.

Wzrosty notowały także branże związane ze zdrowiem i urodą, książkami i multimediami, ubraniami, zabawkami. Warto zwrócić uwagę na rozwój bankowości elektronicznej: osoby starsze uczyły się dokonywania płatności, robienia przelewów czy korzystania z aplikacji mobilnych. Sprawy urzędowe – coraz więcej osób korzysta z platformy e-Polak potrafi!, by załatwić różne sprawy urzędowe, np. złożyć wniosek o dowód. Rozwiązanie takie jak e-PIT daje nam z kolei możliwość rozliczenia się z fiskusem przez Internet. Aplikacje mObywatel, Profil Zaufany czy Internetowe Konto Pacjenta to internetowe aplikacje, dzięki którym w łatwy, szybki i bezpieczny sposób odnajdziesz informacje o swoich danych medycznych, e-skierowania, e-recepty. System eWUŚ - umożliwia łatwe potwierdzenie prawa do leczenia w ramach ubezpieczenia w NFZ. Serwis Zintegrowany Informator Pacjenta – udostępnia zarejestrowanym użytkownikom historyczne dane o ich leczeniu i finansowaniu leczenia, gromadzone od 2008 roku przez NFZ. Portal kolejkowy – umożliwia sprawdzenie najszybszego wolnego terminu wizyty u lekarza lub w szpitalu. Mamy do czynienia z przyspieszeniem transformacji cyfrowej. Szacuje się, że proces, który trwałby kilka lat, dzięki pandemii dokonał się w ciągu kilku miesięcy.

Jakie Pana zdaniem są trendy na najbliższe lata? Czy społeczeństwo będzie dążyło do ochrony prywatności, do stosowania odpowiednich zabezpieczeń, aby chronić informacje o sobie? Czy może wręcz przeciwnie? Będziemy dążyć do ułatwień i odejdziemy od podawania haseł do kont czy wieloskładnikowego uwierzytelniania? A może wiele metod weryfikacji naszej tożsamości zastąpi biometria?

– Moim zdaniem Internet będzie coraz szerzej wykorzystywany i to będzie wymuszało coraz większą ochronę prywatności, coraz więcej metod weryfikacji zastąpi biometria i pewnie pojawią się nowe formy zabezpieczeń, których w tej chwili jeszcze nie znamy.

KARY

Norwegia: wadliwe zabezpieczenie informacji powodem ukarania administratora

Gmina Østre Toten była celem poważnego cyberataku w styczniu 2021 r. Wówczas pracownicy utracili dostęp do większości systemów informatycznych gminy, dane gminy zostały zaszyfrowane, a kopie zapasowe zostały usunięte. W wielu miejscach zlokalizowano wiadomości z żądaniem okupu.

W marcu 2021 r. ustalono, że części danych zostały opublikowane w dark webie. Szacuje się, że około 30 tys. dokumentów zostało dotkniętych atakiem. Część dokumentów zawierała wysoce wrażliwe informacje o mieszkańcach i pracownikach gminy.

Jak stwierdził norweski organ nadzorczy zabezpieczenie danych osobowych przez gminę było wadliwe. Wady te obejmują logi i analitykę logów, ochronę kopii zapasowych i brak uwierzytelniania dwuetapowego lub podobnych środków bezpieczeństwa. Zapora Firewall była niedokładnie skonfigurowana pod względem zabezpieczeń logowania, a duża część ruchu wewnętrznego nigdy nie była rejestrowana. Serwery nie były odpowiednio skonfigurowane do wysyłania logów do centralnej bazy logów, a także nie rejestrowały istotnych zdarzeń. Ponadto gmina nie zabezpieczyła kopii zapasowych przed celowym i przypadkowym usunięciem, zmianą lub odczytaniem.

Źródło: decyzja organu nadzorczego

Dania: organ nadzorczy zakazał korzystania z Google Workspace

Duński organ nadzorczy we wrześniu 2021 roku wydał decyzję, w której zobowiązał gminę Elsinore do dokonania oceny ryzyka przetwarzania danych osobowych za pomocą Google Chromebooks i Workspace, przetwarzanych przez gminę w szkole podstawowej.

Na podstawie dokumentacji i oceny ryzyka dla osób, których dane dotyczą, przygotowanej przez gminę Elsinore, duński organ ochrony danych stwierdził wówczas, że przetwarzanie nie spełnia wymogów RODO pod kilkoma względami. Jego zdaniem, gmina, jako administrator, nie oceniła pewnych szczególnych zagrożeń związanych z konstrukcją podmiotu przetwarzającego dane w odniesieniu do czynności przetwarzania, które administrator może wykonywać jako organ publiczny. Ponadto umowa przetwarzania

stanowi, że informacje mogą być przekazywane do państw trzecich w sytuacjach wymagających wsparcia technicznego bez zapewnienia wymaganego stopnia bezpieczeństwa i ochrony.

W świetle decyzji z września 2021 r. duński organ ochrony danych podjął na początku lipca tego roku nową decyzję, obejmującą między innymi:

- Zawieszenie przetwarzania danych przez gminę Elsinore w przypadku przekazywania informacji do państw trzecich bez niezbędnego stopnia ochrony.
- Ogólny zakaz przetwarzania danych osobowych w Google Workspace do czasu przeprowadzenia odpowiedniej dokumentacji i oceny skutków oraz do czasu dostosowania operacji przetwarzania do RODO.
- Poważną krytykę przetwarzania danych osobowych przez gminę.
- Duński organ nadzorczy zauważa, że wiele konkretnych wniosków zawartych w tej decyzji prawdopodobnie będzie miało zastosowanie do innych duńskich gmin, które korzystają z tej samej konstrukcji podmiotu przetwarzającego dane, co gmina Elsinore.

Źródło: decyzja duńskiego organu

Grecja: 20 mln euro kary dla Clearview AI

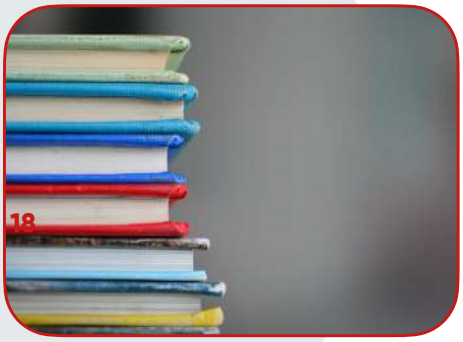
Grecki organ rozpatrzył skargę przeciwko Clearview AI Inc, złożoną przez organizację obywatelską non-profit „Homo Digitalis", w imieniu skarżącego, który twierdził, że nie był zadowolony z realizacji prawa dostępu, z którego skorzystał we wspomnianej wyżej spółce. W przedmiotowej skardze zażądano również zbadania praktyk spółki w całości z punktu widzenia ochrony danych osobowych.

Organ stwierdził, że spółka, która oferuje usługi rozpoznawania twarzy, naruszyła zasady zgodności z prawem i przejrzystości (art. 5 ust. 1 lit. a, art. 5 ust. 2, art. 6 i art. 9 RODO) oraz swoje obowiązki wynikające z art. 12, 14, 15 i 27 RODO.

Ponadto organ nakazał spółce zastosowanie się do żądania skarżącego dostępu do danych osobowych, nakładając jednocześnie (na tę samą spółkę) zakaz zbierania i przetwarzania danych osobowych podmiotów znajdujących się na terytorium Grecji, przy użyciu metod zawartych w usłudze rozpoznawania twarzy.

Wreszcie, na mocy niniejszej decyzji, organ nakazał Clearview AI Inc. usunięcie danych osobowych podmiotów mających siedzibę w Grecji, które spółka zbiera i przetwarza przy użyciu wyżej wymienionych metod.

Źródło: decyzja greckiego organu



EDUKACJA

W wrześniu br. Urząd Ochrony Danych Osobowych organizuje dwa wydarzenia, których tematyka ma służyć pogłębieniu wiedzy na temat ochrony danych osobowych oraz współczesnych wyzwań w procesie przetwarzania danych.

Zabezpieczenia techniczne przetwarzanych danych osobowych - webinarium

Urząd Ochrony Danych Osobowych planuje przeprowadzić we wrześniu br. webinarium na temat zabezpieczeń technicznych przetwarzanych danych osobowych. Podczas wydarzenia zostaną przedstawione środki techniczne i organizacyjne, zapewniające bezpieczeństwo przetwarzanych danych i zgodność ich przetwarzania z przepisami rozporządzenia. Ponadto eksperci UODO udzielą odpowiedzi na przesłane już przez administratorów pytania.

Dokładny termin webinarium oraz link do konferencji zostanie opublikowany w oddzielnym komunikacie.

Człowiek w postkwantowej rzeczywistości - konferencja naukowa

Dynamiczny rozwój procesów przetwarzania danych wymaga coraz szybszych superkomputerów oferujących niespotykaną dotąd moc obliczeniową. Czy takie rozwiązanie stanowi duże zagrożenie dla cyberbezpieczeństwa i podstawowych praw człowieka?

Na to i inne pytania odpowiemy podczas konferencji naukowej „Człowiek w postkwantowej rzeczywistości" organizowanej przez UODO już 28 września 2022 r.

Podczas spotkania organizowanego przez Urząd Ochrony Danych Osobowych zostaną podjęte tematy związane z technologią postkwantową oraz jej wpływem na życie człowieka.

XIII edycja programu „Twoje dane – Twoja sprawa"

1 września rozpoczęliśmy nabór. Więcej informacji pod linkiem **https://uodo.gov.pl/pl/p/tdts**