Nr 10/2022 (43)
Październik 2022

URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

WEBINARIUM O ZADANIACH ADMINISTRATORA I INSPEKTORA OCHRONY DANYCH

Podczas organizowanego przez UODO webinarium **„Zadania administratorów i IOD w kontekście bezpiecznego przetwarzania danych osobowych”** została zaprezentowana trzecia część raportu, którą opracowano na podstawie wyników badania „Ochrona danych osobowych w 2022 r.”. W czasie dyskusji przedstawiono zadania administratora oraz inspektora ochrony danych. Prelegenci skomentowali jak w praktyce powinny wyglądać zabezpieczenia danych osobowych oraz co należy rozumieć poprzez środki organizacyjne czy środki techniczne.

Pełna treść wyników z przeprowadzonego badania została zaprezentowana w materiale **„Ofiary wycieków danych osobowych chcą wiedzieć, jak poradzić sobie z ich skutkami”**, w którym także udostępniono pełen zapis wideo z przeprowadzonego na ten temat webinarium.

Poniżej przedstawiamy odpowiedzi na wybrane pytania, które zostały zadane podczas spotkania.

Na czym polega „spear pshishing”?

Tomasz Ochmiński, Departament Kontroli i Naruszeń UODO: Spear phishing jest to taki rodzaj phishingu, czyli socjotechniki, która jest nakierowana na dany podmiot. Cyberprzestępca robi wszystko, żeby zdobyć jak najwięcej informacji o podmiocie, który będzie atakowany. Używa technik OSINT-owych, robi skany różnego typu, czyli środowiska, w którym znajduje się, kolokwialnie nazywając, „ofiara” i zdobywa wszystkie informacje, żeby spróbować jak najsprytniej i jak najprecyzyjniej dotrzeć do organizacji/podmiotu, który będzie atakował.

Czy inspektor ochrony danych powinien mieć wiedzę, stanowiącą tajemnicę przedsiębiorstwa, w celu efektywnej realizacji swoich zadań?

Łukasz Kołodziejczyk, ClickMeeting: Zgodnie z zasadą wiedzy koniecznej, jeżeli taka wiedza w tym zakresie nie jest niezbędna do realizacji zadań inspektora, to oczywiście nie. Szczerze mówiąc, nie wyobrażam sobie

żeby inspektor mógł współpracować z administratorem, z zespołem pracowników, nie mając w ogóle dostępu do informacji stanowiących tajemnicę przedsiębiorstwa, bo na samym końcu opis procesów wewnętrznych też będzie stanowił tajemnicę przedsiębiorstwa. Inspektor nie musi mieć dostępu do jakiegoś szczególnego typu informacji, np. do wynagrodzeń, bo nie jest to do niczego potrzebne. W zależności od tego, ile tych informacji jest potrzebnych inspektorowi, taki dostęp powinien mieć. Jeżeli to są informacje objęte tajemnicą przedsiębiorstwa, to trzeba to odpowiednio zabezpieczyć.

Jaka częstotliwość wykonywania kopii zapasowych może być uznana za odpowiednią?

Tomasz Ochmiński, Departament Kontroli i Naruszeń UODO: To zależy od tego, jak dużo tych danych posiadamy, jaki to jest w ogóle rodzaj tych danych. Inaczej będziemy traktowali firmę, która przetwarza dane osobowe, dla przykładu na pięciu komputerach, gdzie przetwarzanych danych nie jest dużo i te kopie mogą być robione rzadziej. Z inną sytuacją mamy do czynienia, kiedy administratorem jest organizacja, która posiada 1000 serwerów wirtualnych i ten proces nie może być w żaden sposób zakłócony. Czasami te kopie po prostu muszą być praktycznie robione na bieżąco. Wszystko zależy od skali danej organizacji.

Bartosz Biderman, Departament Cyberbezpieczeństwa UKNF: Zgodzę się z przedmówcą, że faktycznie w przypadkach osób fizycznych, takie kopie bezpieczeństwa wszystkich posiadanych przez siebie danych można wykonywać i aktualizować w zależności od potrzeby, przyjmując interwał czasu odpowiedni dla przyrostu danych, które powinny być w ocenie użytkownika backupowane. Backup, w zależności od wykorzystywanego rozwiązania, można przechowywać lokalnie na dodatkowym nośniku typu dysk HD, SSD lub na zasobach zdalnych typu NAS. Natomiast w przypadku instytucji większych, na przykład instytucji finansowych, takie kopie zapasowe wykonuje się częściej, w sposób automatyczny, zgodnie z przyjętym wewnątrz harmonogramem. Pracownicy dywersyfikują rodzaje nośników ze względu na trwałość – zapisywanie backupów na macierzach dyskowych, taśmach. Sposób wykonywania backupu, jego częstotliwość, a także nośnik, na który jest zapisywany, jak również okres jego przechowywania, regulowany jest przez wewnętrzne procedury organizacji, ale też regulacje prawne.

Łukasz Kołodziejczyk, ClickmMeting: Dodam słowo z punktu widzenia podmiotu, który robi takie kopie i ma do tego infrastrukturę. To wszystko zależy także od tego, jakie biznes ma oczekiwania oraz od systemu -od tego jak został zdefiniowany system przetwarzania danych. Możemy mieć do czynienia z taką sytuacją, że rzeczywiście kopie codzienne będą wymagane, ale może być i tak, że wykonywanie kopii zapasowych będzie wymagane co godzinę. Tu wiadomo, to wszystko zależy również od tego, do czego służy dany system, z którego dane mają być backupowane.

Przez kogo i w jakim zakresie powinny być weryfikowane backupy?

Łukasz Kołodziejczyk, ClickMeeting: To zależy, jak to jest skonstruowane w organizacji. W dużych organizacjach, przy takich, które mają mocno rozwiniętą strukturę w obszarze IT, to najczęściej jest tak, że biznes definiuje wymagania co do backupu, czyli jakiś właściciel procesu. W usłudze to będzie zależało od tzw. SLA, czyli poziomu świadczenia usług. Czasami wykonanie backupu zależy od wymagań klienta i przeprowadzany jest co określony czas. Jeżeli administrator konfiguruje jakiś system backupowy lub te automatyczne procedury backupowania danych, to będzie pewnie uprawniony do tego, żeby odtwarzać ten backup... Najlepiej, żeby to nie tylko i wyłącznie jedna osoba czy jeden podmiot wykonywał zarówno backup, jak i go potem odtwarzał i testował. Te zadania przynajmniej powinny być rozdzielone.

Jakie działania powinny wchodzić w grę na etapie „privacy by design”?

Małgorzata Dulińska-Majkowska, Kaczmarski Group: Z punktu widzenia prawnika istotne jest to, żeby administrator dokładnie przedstawił cały proces przetwarzania danych, jak go sobie wyobraża, jaki powinien być zakres przetwarzanych danych. Wspólnie, w mojej ocenie, wraz z inspektorem ochrony danych powinno się przejść proces, sprawdzić czy ten zakres jest prawidłowy, czy została zachowana zasada minimalizacji danych, następnie oczywiście weryfikacja wszystkich podstaw prawnych przetwarzania tzw. miejsc, w których mamy wejście do procesu, wyjście z procesu. Tak najlepiej przedstawiają to mapy procesu. Z kolei w mniejszych organizacjach można by się skupić po prostu na takim prostym rozrysowaniu sobie, na zasadzie schematu, całego procesu, wskazania celu przetwarzania zakresu danych. Kolejnym etapem, to są te wszystkie kwestie techniczne, jak powinny być wprowadzone zabezpieczenia, które uchronią nas przed naruszeniem danych osobowych.

Tomasz Ochmiński, Departament Kontroli i Naruszeń UODO: Myślę, że tu należy w ogóle uwzględnić też proces wytwórczy. Dzisiaj jest taka sytuacja na rynku, że powstaje dużo software houseów, „zasilanych” ludźmi, którzy przekwalifikowują się z różnych innych zawodów na programistów. Te software house mają zapotrzebowanie na tworzenie głównie web aplikacji. Także tu jest duża rola inspektora ochrony danych, przede wszystkim właśnie w podmiotach, które wytwarzają to oprogramowanie, nad prawidłowym zaimplementowaniem zasad „privacy by design”, „privacy by default”.

Jeżeli wprowadzamy nowe zadania, nową czynność przetwarzania danych na podstawie przepisów prawa, ustawy, to kto powinien ustalić ryzyko?

Łukasz Kołodziejczyk, ClickMeeting: Jeśli mamy zorganizowany system zarządzania bezpieczeństwem informacji, czy system zarządzania ochroną prywatności to wszystko będzie zależało od tego, jak wygląda organizacja. Z punktu widzenia inspektora, to można powiedzieć, że inspektor na żądanie administratora dokonuje oceny skutków naruszenia. Ale ogólnie rzecz biorąc, dobrze by było, żeby właściciel procesu,

brał w tym udział i na pewno powinien posiadać odpowiedzialność. Podkreślam, to wszystko zależy od skali organizacji, od kultury i rozwoju organizacji. W niektórych organizacjach tworzy się całe zespoły do szacowania ryzyka, ponieważ one posiadając fachową wiedzę w tym zakresie i doświadczenie, potrafią posługiwać się odpowiednimi narzędziami. Na pewno osoba zarządzająca danym zasobem powinna brać w udział [w ustalaniu ryzyka]. Ważne jest również ustalenie kto w organizacji akceptuje to ryzyko. Analiza ryzyka jest istotnym procesem i najczęściej, też mogę powiedzieć z praktyki, tak jest, że nikt nie chce być „właścicielem" tego ryzyka, ponieważ on musi podjąć pewne działania, żeby je zminimalizować, co oczywiście wiąże się z czasem czy zmianami w budżecie.

Jak skutecznie przeciwdziałać metodom infiltracyjnym stosowanym przez cyberprzestępców?

Tomasz Ochmiński, Departament Kontroli i Naruszeń UODO: Przede wszystkim szkolenia. To jest podstawa. Musimy się wszyscy szkolić, mieć świadomość tych wszystkich zagrożeń, które na nas czyhają. Oczywiście także należy dodatkowo wprowadzić odpowiednie zabezpieczenia techniczne, chociażby właśnie w postaci eliminacji spamu, który tak naprawdę chyba najbardziej nas nęka. Ciężko jest w tym momencie zabezpieczyć się np. przed smishingiem, kiedy dostajemy SMS-a i nie wiemy, czy to jest podmiot wiarygodny (bo łatwo można podszyć się pod dowolny numer telefonu), chociażby jakiś dostawca energii, który nakłania nas do wejścia na formularz, gdzie musimy zweryfikować, podać dane osobowe, czy to ktoś po prostu się podszywa. I w tym momencie tylko i wyłącznie ratuje nas nasza świadomość. Także świadomość, czyli odpowiednie szkolenia wspierane pewnymi rozwiązaniami technicznymi.

OCHRONA STABILNOŚCI PEŁNIENIA FUNKCJI IOD POWINNA ZOSTAĆ WZMOCNIONA

W ocenie organu nadzorczego celowe jest rozważenie zmiany przepisów prawa krajowego pod kątem doprecyzowania w polskim porządku prawnym regulacji art. 38 ust. 3 zdanie drugie RODO, a tym samym wzmocnienia pozycji inspektora ochrony danych.

Taką opinię UODO przekazał Kancelarii Prezesa Rady Ministrów pytany przez nią o to, czy w związku z wyrokiem Trybunału Sprawiedliwości Unii Europejskiej (TSUE) z 22 czerwca 2022 r. w sprawie C-534/20 Leistritz (ochrona danych osobowych – status inspektora ochrony danych – zakaz wypowiedzenia stosunku pracy inspektora ochrony danych przez administratora będącego jego pracodawcą), **konieczna jest zmiana obowiązującego w Polsce prawa lub praktyki jego stosowania.**

Co orzekł Trybunał

TSUE w powołanym wyroku udzielił odpowiedzi na pytanie, czy art. 38 ust. 3 zdanie drugie RODO należy interpretować w ten sposób, że stoi on na przeszkodzie przepisom prawa krajowego, na mocy których niedozwolone jest wypowiedzenie w zwyczajnym trybie stosunku pracy inspektora ochrony danych (IOD) przez administratora będącego jego pracodawcą, niezależnie od tego, czy następuje ono z powodu wykonywania jego zadań.

Art. 38 ust. 3 zdanie drugie RODO

„Nie jest on [IOD] odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań.”

W art. 38 ust. 3 RODO prawodawca unijny nie definiuje terminów *odwoływany*, *karany* i *za wypełnianie swoich zadań*. Zgodnie z punktem 24 powołanego wyroku art. 38 ust. 3 zdanie drugie RODO ma zastosowanie do stosunków między inspektorem ochrony danych (IOD) a administratorem lub podmiotem przetwarzającym, niezależnie od charakteru stosunku pracy łączącego tego inspektora z administratorem lub podmiotem przetwarzającym. Ponadto w punkcie 34 wyroku TSUE odwołał się do opinii rzecznika generalnego, który jest zdania, iż każde państwo członkowskie może przy wykonywaniu pozostawionych mu kompetencji ustanowić przepisy szczególne zapewniające większą ochronę w zakresie rozwiązywania stosunku pracy z inspektorem ochrony danych, o ile przepisy te są zgodne z prawem UE, a konkretnie z przepisami RODO, m.in. z jego art. 38 ust. 3 zdanie drugie. Zgodnie zaś z punktem 36 wyroku art. 38 ust. 3 zdanie drugie RODO należy interpretować w ten sposób, że nie stoi na przeszkodzie uregulowaniu krajowemu, które przewiduje, że administrator lub podmiot przetwarzający może rozwiązać stosunek pracy z inspektorem ochrony danych, będącym członkiem jego personelu, jedynie z ważnej przyczyny, nawet jeśli rozwiązanie stosunku pracy nie jest związane z wypełnianiem przez tego inspektora jego zadań, o ile takie uregulowanie nie zagraża realizacji celów RODO. W związku z tym TSUE orzekł, że państwa członkowskie mają możliwość doprecyzowania w krajowym porządku art. 38 ust. 3 zdanie drugie RODO, poprzez przyjęcie odpowiednich legislacyjnych rozwiązań lepiej chroniących niezależność IOD, a także zapewniających wzmocnienie ich pozycji.

Stanowisko UODO

Za przyjęciem takiej interpretacji art. 38 ust. 3 zdanie drugie RODO opowiada się również organ nadzorczy. W jego opinii art. 38 ust. 3 zdanie drugie RODO nie stoi na przeszkodzie przepisowi prawa krajowego, na mocy którego inspektor ochrony danych uzyska dalej idącą ochronę prawną przed odwołaniem lub karaniem. Art. 38 ust. 3 RODO jest bowiem ogólnym wskazaniem zasady, jaką powinny kierować się państwa ze względu na bezpośredniość stosowania unijnego rozporządzenia.
Ustawodawca polski, wprowadzając do porządku prawnego nowe regulacje prawne na podstawie RODO, zwłaszcza ustawę z dnia 10 maja 2018 r. o ochronie danych, nie uregulował w żaden szczególny sposób ochrony pełnienia funkcji IOD. Dlatego regulacje szczegółowe dotyczące ochrony stabilności pełnienia tej funkcji powinny zostać doprecyzowane we właściwych przepisach obejmujących zarówno przypadki stosunku pracy, jak i umowy o świadczenie usług. TSUE w powołanym wyroku ocenił, że art. 38 ust. 3 zdanie drugie RODO ma zastosowanie zarówno do IOD będącego członkiem personelu administratora danych lub podmiotu przetwarzającego, jak i do osoby wykonującej te zadania na podstawie umowy o świadczenie usług, zgodnie z art. 37 ust. 6 RODO (pkt 23 wyroku). Pozycja inspektora ochrony danych w obu przypadkach powinna zatem zostać wzmocniona.

W odniesieniu do umów o pracę na czas określony obecnie w polskim porządku prawnym brak jest podstaw prawnych dających IOD roszczenie o przywrócenie do pracy lub odszkodowanie w przypadku, gdy wypowiedzenie nastąpiło bez naruszenia przepisów o wypowiadaniu umowy na czas określony, mimo naruszenia przez pracodawcę (administratora) zakazu wskazanego w art. 38 ust 3 zdanie 2 RODO.
W polskim porządku prawnym w art. 18 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy prawodawca ustanowił zasadę uprzywilejowania pracownika będącą normą semidyspozytywną, która pozwala na umowne ukształtowanie stosunku pracy w sposób korzystniejszy dla pracownika. W związku z tym, mając m.in. na względzie wyrok TSUE w sprawie C-534/20, uzasadnione jest dążenie do wzmocnienia pozycji IOD. Im bowiem stabilniejsza jest jego pozycja, tym większa szansa na niezależne wykonywanie przypisanych mu zadań, co wpływa na jakość jego pracy oraz zapewnianie wysokiego poziomu ochrony danych osób fizycznych.

Czas na rozpoczęcie dyskusji

W związku z powyższym o ocenie UODO zasadne byłoby rozpoczęcie przez ministrów właściwych w kwestiach ochrony danych osobowych i zatrudnienia dialogu z interesariuszami (m.in. organizacjami pracodawców, organizacjami zrzeszającymi IOD) w sprawie rozszerzenia w polskim porządku prawnym zakresu ochrony osób wykonujących funkcję inspektora ochrony danych.

BĘDĄ CZĘŚCIOWE ZMIANY ODNOSZĄCYCH SIĘ DO IOD PRZEPISÓW USTAWY IMPLEMENTUJĄCEJ DYREKTYWĘ POLICYJNĄ

Taką deklarację Ministerstwo Spraw Wewnętrznych i Administracji złożyło w odpowiedzi na wystąpienie Prezesa UODO w sprawie konieczności dokonania zmiany niektórych dotyczących IOD przepisów ustawy implementującej dyrektywę policyjną.

O przesłaniu takiego wniosku informowaliśmy w poprzednim wydaniu newslettera UODO dla IOD (nr 8-9/2022) w tekście „Niektóre z przepisów ustawy implementującej dyrektywę policyjną dot. IOD wymagają zmian". Wskazaliśmy w nim, że w ocenie UODO przepisy ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (wdrażającej 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 2008/977/WSiSW) są źle sformułowane, co skutkuje m.in. błędnym przypisaniem zadań IOD oraz brakiem precyzyjnych przepisów regulujących dokonywanie zawiadomień dotyczących IOD.

Jednak MSWiA nie w pełni podzieliło tę opinię. W ocenie resortu, nie ma potrzeby doprecyzowania przepisów odnoszących się do przesyłania do Prezesa UODO zawiadomień dotyczących IOD. Pozytywnie odniesiono się natomiast do stanowiska UODO dotyczącego konieczności zmiany art. 37 ust. 3 i art. 38 ust. 6 ustawy w zakresie możliwości powierzenia IOD przeprowadzenia oceny skutków planowanych operacji przetwarzania danych dla ochrony danych osobowych, jak również wystąpienia do organu nadzorczego z wnioskiem o przeprowadzenie uprzednich konsultacji.

W odpowiedzi na wystąpienie wskazano jednak, że „zakres i charakter postulowanych zmian nie uzasadniają podjęcia odrębnej inicjatywy legislacyjnej. Tym samym zmiany w zakresie zadań inspektora

ochrony danych mogą zostać wprowadzone w przyszłości przy okazji zamian przepisów o zbliżonym zakresie tematycznym w innych ustawach".

Odnosząc się do tych informacji i dziękując za deklarację wprowadzenia zmian, UODO wskazał jednocześnie, że w toku ewentualnych przyszłych prac legislacyjnych należy ponownie rozważyć przedstawioną przez organ nadzorczy argumentację dotyczącą dokonywania zawiadomień dotyczących IOD oraz wprowadzenia przepisów, na mocy których administrator byłby zobowiązany do powiadomienia Prezesa UODO o danych administratora oraz o każdej zmianie tych danych.

OCHRONA DANYCH OSOBOWYCH W PROGRAMIE STUDIÓW

W programie studiów podyplomowych w zakresie wyceny nieruchomości uwzględnione mają być kwestie dotyczące ochrony danych.

Tak wynika z przekazanego do zaopiniowania przez UODO projektu rozporządzenia Ministra Rozwoju i Technologii zmieniającego rozporządzenie w sprawie minimalnych wymogów programowych dla studiów podyplomowych w zakresie wyceny nieruchomości.

Organ nadzorczy z zadowoleniem przyjął uwzględnienie tej tematyki w programie studiów. Podkreślił, że działanie to z pewnością przyczyni się do odpowiedniego przygotowania absolwentów studiów do rzetelnego wykonywania zawodu rzeczoznawcy majątkowego.

W opinii UODO ochrona danych osobowych – ze względu na interdyscyplinarność tej dziedziny – powinna być ujmowana we wszystkich programach nauczania, co przyczyni się do podniesienie poziomu wiedzy w tym zakresie, a jednocześnie zwiększenia poszanowania naszego prawa do ochrony danych osobowych i prawa do prywatności.

POPRZEZ WYDAWANE DECYZJE WSKAZUJEMY KIERUNKI DZIAŁANIA

O wydawanych decyzjach mówi Jacek Młotkiewicz, dyrektor Departamentu Kontroli i Naruszeń UODO w rozmowie z Eweliną Janczylik-Foryś

Jednym z najważniejszych działań organu nadzorczego jest monitorowanie przestrzegania RODO i reagowanie w sytuacji naruszenia przepisów tego aktu prawnego. Najbardziej dobitnym przykładem takiej reakcji jest wydawanie decyzji administracyjnych nakładających administracyjną karę pieniężną. Ponadto organ nadzorczy wydaje również inne decyzje administracyjne, w tym decyzje udzielające upomnienia oraz decyzje nakładające obowiązek dostosowania operacji przetwarzania danych do wymogów wynikających z RODO.

W jakich przypadkach naruszenia danych osobowych wydawane są decyzje upomnienia a w jakich administracyjne kary pieniężne?

Upomnienia są przede wszystkim udzielane w wyniku przeprowadzonego postępowania administracyjnego w związku ze złożoną skargą i dotyczą takich kwestii jak chociażby udostępnienie danych osobowych nieuprawnionym podmiotom, brak realizacji obowiązków informacyjnych czy też uchybień w zakresie zabezpieczenia danych osobowych. Decyzje z upomnieniem wydawane są też na skutek naruszeń ochrony danych osobowych i wykazanych w toku przeprowadzonego postępowania nieprawidłowości co do bezpieczeństwa przetwarzanych danych osobowych. Można jednak zaobserwować pewne podobieństwa między decyzjami z upomnieniem a decyzjami nakładającymi administracyjną karę pieniężną za naruszenie przepisów RODO dotyczących obowiązków z zakresu bezpieczeństwa danych.

W przypadku obu rodzajów decyzji wskazywane uchybienia dotyczą zwykle nieprawidłowości w zakresie przeprowadzonej analizy ryzyka, doboru nieskutecznych środków technicznych czy organizacyjnych mających zapewnić bezpieczeństwo danych, a także braku regularnego testowania, mierzenia i oceniania skuteczności zastosowanych środków bezpieczeństwa dla ochrony przetwarzanych danych osobowych. Podstawowa różnica, od której zależy, czy zostanie wydana decyzja z administracyjną karą pieniężną, czy decyzja z upomnieniem, związana jest z tym, czy konsekwencją niewłaściwej realizacji obowiązków z zakresu prawidłowego zabezpieczenia danych osobowych jest tzw. wyciek danych, a więc utrata poufności danych, czy też „tylko” utrata ich dostępności.

W tym pierwszym przypadku, a więc w przypadku wycieku danych, konsekwencją jest najczęściej decyzja z administracyjną karą pieniężną, co jednoznacznie potwierdzają wydane w tym zakresie przez organ nadzorczy decyzje. Natomiast w sytuacji, w której utracony został atrybut dostępności danych zwykle wydawana jest decyzja z upomnieniem, w szczególności wówczas gdy administrator wykazał podjęcie szeregu działań naprawczych, które w ocenie organu nadzorczego w sposób istotny ograniczają ryzyko ponownego wystąpienia naruszenia w tym zakresie, spowodowanego najczęściej działaniem złośliwego oprogramowania typu ransomware. Nie ma jednak żadnych gwarancji, że taki podział będzie zawsze i w każdym przypadku kiedy naruszenie ochrony danych osobowych będzie związane tylko z utratą dostępności danych, to efektem będzie decyzja z upomnieniem. Każdy przypadek jest bowiem oceniany indywidualnie.

Co jest brane pod uwagę przy wydawaniu decyzji?

W kontekście kształtowania, w związku z wydawaniem decyzji administracyjnych, praktyki w zakresie właściwego zabezpieczenia danych osobowych oceniana jest przede wszystkim analiza ryzyka przeprowadzona przez administratora (w tym, czy uwzględniono w niej wszystkie zagrożenia dla przetwarzanych danych osobowych) oraz sposób i częstotliwość testowania, mierzenia i oceniania skuteczności zastosowanych środków bezpieczeństwa.

Kolejne brane pod uwagę zagadnienia dotyczą procedur związanych ze sporządzaniem kopii zapasowych danych, a także wykorzystywanych systemów informatycznych i urządzeń do przetwarzania danych osobowych. Jeżeli chodzi o kopie zapasowe, to częstym błędem jest brak jakichkolwiek procedur w tym zakresie lub ich lakoniczność, w efekcie czego sporządzane kopie zapasowe nie są poddawane jakiejkolwiek weryfikacji prawidłowości ich sporządzenia, czy też testowaniu skuteczności odtwarzania z nich danych osobowych. Oznacza to, i takie przypadki wynikają ze zgłoszeń naruszenia ochrony danych osobowych, niemożność przywrócenia danych lub niezgodność przywróconych danych z innymi danymi przetwarzanymi przez administratora.

Innym błędem jest przechowywanie takich kopii wraz z danymi eksploatowanymi na bieżąco, co skutkuje ich zaszyfrowaniem w przypadku ataku ransomwere. Takie działania zaprzeczają podstawowej funkcji kopii zapasowych, tj. szybkiego i sprawnego przywrócenia danych i zapewnienia ciągłości działania administratora w zakresie przetwarzania danych osobowych. Należy także podkreślić, że w przypadku niektórych podmiotów, np. podmiotów z sektora publicznego, może to prowadzić do powstania wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, skoro osoby te, z uwagi na zaszyfrowanie danych, nie będą mogły załatwić żadnej sprawy w urzędzie. Jeśli zaś chodzi o wykorzystywane systemy informatyczne i urządzenia do przetwarzania danych osobowych, to nadal spotykamy się z sytuacjami używania przez administratorów systemów informatycznych, które utraciły już wsparcie producenta oraz urządzeń,

na których nie ma możliwości aktualizacji oprogramowania firmware, co powoduje, że atakujący mogą stosunkowo łatwo przełamywać zabezpieczenia wykorzystując luki bezpieczeństwa istniejące w tych systemach. Te kwestie jako podnoszone w wydawanych decyzjach i jako wpływające w istotny sposób na zastosowanie określonej sankcji (tj. czy kary czy upomnienia) powinny zmienić podejście administratorów do tych zagadnień.

UODO także dużą uwagę przykłada do zawiadomienia osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych. W tym przypadku z jaką sankcją mogą się spotkać administratorzy?

To zależy od indywidualnych okoliczności sprawy. Upomnienia są bowiem także udzielane za brak prawidłowej reakcji administratora danych na skierowane do niego wystąpienie w trybie art. 52 ustawy o ochronie danych osobowych o właściwe zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony jej danych osobowych. Mówiąc o nieprawidłowej reakcji administratora mam na myśli nieprzekazanie osobie, której dane zostały naruszone, wszystkich wymaganych informacji, zgodnie z art. 34 ust. 2 RODO, a nie sytuacje, kiedy administrator w ogóle neguje konieczność skierowania takiego zawiadomienia do takiej osoby. W takim bowiem przypadku wydawane są decyzje nakładające administracyjną karę pieniężną. Decyzje w tym zakresie kształtują zatem praktykę, polegającą na tym, że administratorzy, którzy otrzymali ww. wystąpienie, kierują do osób, których dane zostały objęte naruszeniem, ponowne zawiadomienie.

Czemu służą wydawane decyzje, oprócz tego, że odnoszą się do postępowań konkretnego administratora?

Wydawane decyzje mają przede wszystkim na celu wskazanie administratorom, podmiotom przetwarzającym oraz inspektorom ochrony danych pożądanego kierunku postępowania związanego z ochroną danych osobowych, a także uświadomić istnienie określonego obowiązku i możliwego podejścia w celu jego prawidłowego wykonania.

KARY

Francja: brak przemyślanego posługiwania się danymi doprowadził do nałożenia kary.

Dane geolokalizacyjne stały się przyczyną nałożenia na UBEEQO International przez francuski organ nadzorczy administracyjnej kary pieniężnej w wysokości 175 tys. euro.

W następstwie kontroli przeprowadzonych w 2020 roku związanych z nowymi zastosowaniami danych geolokalizacyjnych w kontekście mobilności, francuski organ nadzorczy (CNIL) skontrolował spółkę UBEEQO International. Działalność tej spółki polega na wynajmie pojazdów na krótkie okresy. Dochodzenia skupiły się w szczególności na gromadzonych danych, ustalonych okresach przechowywania, informacjach przekazywanych osobom fizycznym oraz wdrożonych środkach bezpieczeństwa.

Główne ustalenia w sprawie wskazały na:

- niedopełnienie obowiązku zapewnienia minimalizacji danych (art. 5 ust. 1 lit. c RODO),
- brak określenia i przestrzegania proporcjonalnego okresu zatrzymywania danych (art. 5 ust 1. lit. e RODO),
- niepoinformowanie osób, których dane dotyczą (art. 12 RODO).

Na podstawie tych ustaleń CNIL we współpracy z innymi organami, których sprawa dotyczy (w Belgii, Danii, Hiszpanii, Włoszech i Niemczech) nałożył na UBEEQO International administracyjną karę pieniężną w wysokości 175 tys. euro.

Źródło: decyzja organu nadzorczego