Nr 12/2022 (45)
Grudzień 2022

URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

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

MNIEJ DANYCH W PUBLICZNYCH OBWIESZCZENIACH KOMORNICZYCH O TERMINIE OPISU I OSZACOWANIA ZAJĘTEJ NIERUCHOMOŚCI

Ministerstwo Sprawiedliwości podzieliło opinię UODO i zapowiada ograniczenie zakresu danych osobowych ujawnianych w obwieszczeniach komorniczych o terminie opisu i oszacowania nieruchomości w rozumieniu art. 945 § 2 Kodeksu postępowania cywilnego (kpc).

W związku z docierającymi do UODO sygnałami dotyczącymi nadmiarowego zakresu danych osobowych ujawnianych w obwieszczeniach komorniczych o terminie opisu i oszacowania nieruchomości w rozumieniu art. 945 § 2 kpc, organ nadzorczy wystąpił do Ministra Sprawiedliwości z wnioskiem o rozważenie zmiany przepisów ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego i określeniu w nich: niezbędnego zakresu informacji, w tym danych osobowych, które powinny być zamieszczane w powołanych obwieszczeniach, okresu publikacji tych obwieszczeń, a także podmiotów odpowiedzialnych za ich usunięcie. W ocenie UODO przepisy dotyczące opisu i oszacowania nieruchomości, w tym zwłaszcza art. 945 § 2 kpc, są zbyt ogólnie sformułowane. Nie określają m.in. niezbędnych elementów, które powinny znaleźć się w treści publicznego obwieszczenia komorniczego o terminie opisu i oszacowania nieruchomości, w tym sposobu oznaczenia dłużnika ze wskazaniem zakresu jego danych osobowych.
Taki stan prawny prowadzi do upubliczniania przez niektórych komorników nadmiarowych danych osobowych, dodatkowo przez nieokreślony czas, co jest sprzeczne z zasadami przetwarzania danych osobowych określonymi w art. 5 ust. 1 RODO.
Opinię UODO podziela Minister Sprawiedliwości, który w odpowiedzi na powyższe wystąpienie zauważył jednocześnie, że dla zachowania spójności regulacji zasadne byłoby odpowiednie ukształtowanie art. 953 § 1 kpc dotyczącego publicznego obwieszczenia o licytacji nieruchomości (m.in. poprzez określenie czasu jego upubliczniania oraz podmiotu odpowiedzialnego za jego zdjęcie/usunięcie).
Poinformował również, że „odpowiednie działania legislacyjne, zmierzające do zmiany tego stanu rzeczy, mogą zostać podjęte w trakcie prac parlamentarnych nad projektem ustawy o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (druk sejmowy nr 2560)”.

USPRAWIEDLIWIANIE NIEOBECNOŚCI UCZNIA

Nie ma podstaw, by szkoła, na potrzeby usprawiedliwienia nieobecności ucznia, żądała podania przyczyny absencji.

Stosownie do art. 99 ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe w statucie szkoły określa się obowiązki ucznia dotyczące m.in. usprawiedliwiania, w określonym terminie i formie, nieobecności na zajęciach edukacyjnych, w tym formy usprawiedliwiania nieobecności przez osoby pełnoletnie.
Jednak prawo do określenia obowiązków ucznia w tym zakresie nie oznacza całkowitej swobody w ustaleniu zakresu danych osobowych ucznia potrzebnych do usprawiedliwienia jego nieobecności, tym bardziej że w ten sposób może dochodzić także do pozyskiwania danych szczególnych kategorii, dla których określone zostały szczególne warunki przetwarzania.
Organy szkoły regulujące wskazaną kwestię w statucie szkoły muszą wziąć pod uwagę zasady wynikające m.in. z RODO. Zgodnie zaś z zasadą minimalizacji danych, dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.
Zatem rodzic (opiekun prawny), usprawiedliwiając nieobecność swojego dziecka może, gdy uzna to za stosowne, podać przyczynę jego nieobecności, nie może zostać jednak do tego zobowiązany przez regulacje określone w statucie szkoły. Brak jest bowiem przepisów prawa, które nakazywałyby podawanie przez opiekuna prawnego ucznia przyczyny nieobecności dziecka w szkole.
W przypadku zaobserwowania przez nauczyciela systematycznej, usprawiedliwianej nieobecności ucznia, może on skontaktować się z rodzicami (opiekunami prawnymi) dziecka lub pełnoletnim uczniem i poinformować o swoich spostrzeżeniach lub zrobić to za pośrednictwem dyrektora szkoły. W przypadku dalszego, systematycznego usprawiedliwiania nieobecności ucznia, szkoła może zgłosić swoje podejrzenie co do braku realizowania obowiązku szkolnego do sądu rodzinnego. Niemniej brak możliwości nakazania rodzicom (opiekunom prawnym) dziecka podania przyczyny jego nieobecności na zajęciach nie wyklucza dobrowolnego przekazania przez nich takich informacji.

RUSZYŁY PRACE NAD STWORZENIEM KODEKSU POSTĘPOWANIA DLA JEDNOSTEK SAMORZĄDU TERYTORIALNEGO

Zawiązała się inicjatywa mająca na celu przygotowanie kodeksu postępowania dla jednostek samorządu terytorialnego. O rozpoczęciu prac w tym zakresie UODO został poinformowany przez Związek Województw RP.

Organ nadzorczy z zadowoleniem przyjął tę inicjatywę. Jednocześnie w odpowiedzi na korespondencję w tej sprawie wskazał, jaka procedura i tryb postępowania obowiązują przy pracach nad tego typu regulacją.

Praca środowiska

Podkreślił, że to środowisko tworzące kodeks ma najpierw zidentyfikować swoje potrzeby, skonsultować je wewnętrznie, a następnie przygotować projekt kodeksu i przeprowadzić dotyczące go publiczne konsultacje oraz ustalić sposób jego monitorowania.

Organ nadzorczy nie uczestniczy w pracach nad tworzeniem takiego dokumentu. Możliwe jest natomiast zorganizowanie spotkania z przedstawicielami UODO w celu omówienia zasad i procedur związanych z tworzeniem kodeksów. Jednocześnie w ten sposób organ nadzorczy realizuje jedno ze swoich zadań, jakim jest zachęcanie do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu RODO.

Ocena UODO

Dopiero w następnym etapie projekt kodeksu może być przedstawiony organowi nadzorczemu do oceny. Ocena merytoryczna treści projektu kodeksu postępowania w rozumieniu art. 40 RODO może odbyć się dopiero po złożeniu formalnego wniosku o jego zatwierdzenie i po wstępnej weryfikacji, czy przedłożony projekt spełnia wymogi formalne oraz kryteria dopuszczalności, o których mowa w Wytycznych nr 1/2019 Europejskiej Rady Ochrony Danych dotyczących kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/6792. Po stwierdzeniu, że wniosek o zatwierdzenie kodeksu postępowania spełnia wymogi formalne oraz kryteria dopuszczalności, do wnioskodawcy kierowane jest pismo zawierające informację w powyższym zakresie i o tym, że organ nadzorczy przystępuje do oceny

merytorycznej kodeksu. Jeżeli natomiast wniosek o zatwierdzenie kodeksu nie spełnia warunków, o których mowa powyżej, w piśmie skierowanym do wnioskodawców zawarte jest uzasadnienie takiej oceny.

Pomocne materiały

Jednocześnie warto przypomnieć, że w pomocne w pracach nad kodeksem postępowania mogą być materiały zamieszczone na stronie internetowej UODO:

- **Jak efektywnie prowadzić prace nad kodeksem postępowania – rekomendacje UODO**
- **Najczęściej popełniane błędy przez środowiska pracujące nad projektami kodeksów postępowania**
- **Monitorowanie kodeksów. Jak stworzyć odpowiedni mechanizm? Na co zwrócić uwagę, a czego unikać**

oraz tekst opublikowany w „Newsletterze UODO dla IOD" z listopada ub.r. (nr 11/2021) pt. „Konsultacje kodeksu postępowania powinny być szerokie, lecz podsumowanie syntetyczne".

CZAS NA AKTUALIZACJĘ STANDARDOWYCH KLAUZUL UMOWNYCH DOTYCZĄCYCH PRZEKAZYWANIA DANYCH DO PAŃSTW TRZECICH

Czas na aktualizację standardowych klauzul umownych dotyczących przekazywania danych do państw trzecich. UODO przypomina, że podmioty, które przekazują dane osobowe do krajów spoza Europejskiego Obszaru Gospodarczego (EOG) lub do organizacji międzynarodowych na podstawie nieobowiązujących już standardowych klauzul umownych (a transfer ten rozpoczął się przed 27 września 2021 r.), powinny do 27 grudnia 2022 r. zawrzeć umowy bazujące na nowych klauzulach.

Nowe standardowe klauzule umowne, na podstawie których może odbywać się przesyłanie danych z UE do krajów spoza EOG, zaczęły obowiązywać w czerwcu 2021 r. Są one dostosowane do RODO i do bardziej złożonego transferu danych, w którym często uczestniczą nie dwa, lecz kilka różnych podmiotów.

Odnoszą się do różnych scenariuszy przekazywania danych, tj. do:

- przekazywania danych między administratorami,
- przekazywania danych przez administratora podmiotowi przetwarzającemu w państwie trzecim,
- przekazywania między podmiotami przetwarzającymi,
- przekazywania danych przez podmiot przetwarzający administratorowi w państwie trzecim.

Jak informowaliśmy na naszej stronie internetowej w materiale **„Transfer danych do państw trzecich zgodny z RODO”**, od 27 września 2021 r. nie jest już możliwe zawieranie umów wykorzystujących wcześniej obowiązujące klauzule.

Natomiast dla umów zawartych przed 27 września 2021 r. przewidziano okres przejściowy, który właśnie dobiega końca. Umowy zawarte przed 27 września 2021 r. na podstawie wcześniejszych klauzul zapewniają odpowiednie gwarancje w rozumieniu art. 46 ust. 1 RODO do 27 grudnia 2022 r., pod warunkiem że operacje przetwarzania stanowiące przedmiot umowy pozostaną niezmienione oraz że stosowanie tych klauzul zapewnia, aby przekazywanie danych osobowych odbywało się z zastrzeżeniem odpowiednich zabezpieczeń.

Po 27 grudnia 2022 r. umowy muszą być zgodne z nowymi klauzulami.

Jednocześnie zaznaczyć należy, że zastosowanie nowych standardowych klauzul umownych nie wyłącza konieczności oceny planowanego transferu pod kątem zapewnienia zgodności z wyrokiem TSUE w sprawie Schrems II i ewentualnego wdrożenia środków uzupełniających standardowe klauzule umowne, o czym również można **przeczytać** na naszej stronie internetowej.
Warto też przypomnieć, że **Komisja Europejska opublikowała pytania i odpowiedzi**, stanowiące praktyczne wytyczne dotyczące stosowania standardowych klauzul umownych i pomagające zainteresowanym stronom w ich wysiłkach na rzecz zapewnienia zgodności z ogólnym rozporządzeniem o ochronie danych (RODO).
Zawarcie umów zgodnych z nowymi standardowymi klauzulami umownymi to jednocześnie doskonała okazja do przeglądu dokonywanych transferów i zweryfikowania, czy są one w ogóle dopuszczalne, czy odbywają się na właściwej podstawie, czy są opisane w sposób aktualny i czy są zapewnione odpowiednie zabezpieczenia.

PRZECHOWYWANIE NAGRANIA ROZMOWY TELEFONICZNEJ Z KLIENTEM OZNACZA PRZETWARZANIE DANYCH TEJ OSOBY

Jeśli administrator w czasie rozmowy telefonicznej z klientem rejestruje dźwięk tej rozmowy, to przechowując nagranie, przetwarza jego dane osobowe. W związku z tym, już podczas realizacji wobec klienta obowiązku informacyjnego powinien wskazać na taki zakres przetwarzania danych, jak rejestracja głosu. Ponadto gdy klient zażąda udostępnienia kopii danych osobowych, administrator powinien je wydać.

Takie stanowisko wyraził Prezes UODO w jednej z decyzji, w której nakazał administratorowi spełnienie wobec osoby, której dane dotyczą, obowiązku informacyjnego poprzez dostarczenie kopii jego danych osobowych utrwalonych w nagraniu rozmowy audio z konsultantem. Wspomniana decyzja została wydana

w następstwie złożonej do UODO skargi na nieprawidłowości w procesie przetwarzania danych osobowych przez administratora polegające na niespełnieniu wobec skarżącego obowiązku informacyjnego.

Jak ustalono skarżący kilkakrotnie zwracał się do administratora z żądaniem udostępnienia kopii danych osobowych w postaci zapisu rozmowy audio z konsultantem. Ponadto skarżący wskazał, że odmówiono mu realizacji jego żądania i oczekuje od Urzędu nakazania administratorowi wydania kopii jego danych osobowych zawartych w nagraniu będącym w dyspozycji tego administratora. Administrator zaś wskazał, że pozyskał dane skarżącego bezpośrednio od niego w związku z korzystaniem z produktów. Administrator poinformował skarżącego, że może on skorzystać z wniosku dostępu do danych zgodnie z RODO, natomiast odpowiedź na tę dyspozycję nie będzie zawierała nagrań głosowych.

Materiał dowodowy zgromadzony w niniejszej sprawie wykazał, że skarżący zwracał się do administratora o wydanie kopii nagrania rozmów, powołując się na art. 15 RODO. Konkretnie skarżący powołał się na art. 15 ust. 3 RODO, żądając przesłania kopii jego danych osobowych przetwarzanych przez administratora, wskazując jednocześnie, że zakres danych osobowych obejmować powinien kopię nagrania rozmowy z konsultantem, w którym zawarte są jego dane osobowe w zakresie głosu.

Prawo do uzyskania kopii danych

Wskazać należy, że zgodnie z art. 15 ust. 3 RODO administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu.

Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się w powszechnie stosowanej formie elektronicznej.

Zgodnie z art. 12 ust. 3 RODO administrator bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15–22. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań albo odmówić podjęcia działań w związku z żądaniem. Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

Brak realizacji obowiązku informacyjnego

W omawianej sprawie administrator ustosunkował się do złożonego przez skarżącego wniosku, przesyłając drogą elektroniczną w formie tekstowej treść danych osobowych skarżącego, które przetwarzał. Jednak sposób realizacji obowiązku informacyjnego przez tego administratora, wynikającego z art. 15 ust. 3 RODO, nie uwzględnił okoliczności, że przetwarza on dane osobowe w zakresie głosu skarżącego w wyniku przechowywania nagrania rozmowy telefonicznej.

Administrator, realizując powyższy obowiązek, nie uwzględnił danych osobowych skarżącego przetwarzanych w związku z rozmową telefoniczną, w szczególności w postaci głosu skarżącego. Administrator nie spełnił więc wobec skarżącego w sposób prawidłowy obowiązku informacyjnego (art. 15 ust. 3 RODO), a dodatkowo odmówił skarżącemu dostarczenia kopii jego danych osobowych.

Podkreślenia również wymaga, że w przypadku zwrócenia się do administratora o kopię przetwarzanych danych osobowych, administrator każdorazowo podejmuje decyzję, w jaki sposób zrealizuje to uprawnienie. W przypadku danych osobowych utrwalonych na nagraniu, administrator może dokonać wyboru, czy udostępni kopię nagrania, czy też udostępni kopię danych zawartych w tym nagraniu.

Na podstawie przepisów prawa

W opisanej sprawie, udzielając odpowiedzi skarżącemu, administrator nie wskazał również podstawy prawnej, która zwalniałaby go z obowiązku spełnienia obowiązku informacyjnego. Co istotne, w zakresie danych osobowych zawartych w nagraniu rozmowy telefonicznej administrator powołał się jedynie na regulamin świadczenia usługi bez wskazania na jakikolwiek przepis krajowego lub prawa Unii Europejskiej, który zwalniałby go z realizacji obowiązku informacyjnego wynikającego z art. 15 ust. 3 RODO w zakresie danych osobowych pozyskanych i przetwarzanych w związku z przechowywaniem zapisu rozmowy telefonicznej.

W ocenie UODO, w tej sprawie sposób realizacji obowiązku informacyjnego z art. 15 ust. 3 RODO przez administratora nie uwzględnił kopii wszystkich przetwarzanych danych osobowych skarżącego. UODOstosując uprawnienia naprawcze, nakazał administratorowi spełnienie obowiązku informacyjnego z art. 15 ust. 3 RODO względem skarżącego, poprzez dostarczenie kopii jego danych osobowych utrwalonych w nagraniu rozmowy audio z konsultantem, uwzględniającej głos skarżącego. Co istotne, spełnienie tego obowiązku przez administratora powinno nastąpić z poszanowaniem praw innych osób niż skarżący, w tym prawa do ochrony danych osobowych tych osób, tj. w sposób nie przekraczający ram obowiązku informacyjnego z art. 15 ust. 3 RODO.

DZIAŁANIA EDUKACYJNE SĄ KLUCZOWE DLA BUDOWANIA ŚWIADOMOŚCI SPOŁECZEŃSTWA

Bartłomiej Drozd, ekspert serwisu ChronPESEL.pl w rozmowie z Eweliną Janczylik-Foryś

Bartłomiej Drozd - od wielu lat zajmuje się propagowaniem wiedzy na temat bezpieczeństwa danych osobowych. Autor licznych wystąpień medialnych, w których tłumaczy aktualne sposoby działania oszustów i cyberprzestępców oraz radzi, co zrobić, żeby uniknąć negatywnych konsekwencji ich działania. Razem z serwisem ChronPESEL.pl promuje właściwe zachowania i przestrzeganie zasad bezpieczeństwa poprzez przygotowanie materiałów edukacyjnych opartych na cyklicznie realizowanych badań.

W tym roku, UODO po raz kolejny udzieliło patronatu nad badaniami „Ochrona danych osobowych w 2022 r." przeprowadzonymi na zlecenie serwisu ChronPESEL.pl i Krajowego Rejestru Długów. Czy widzi Pani jakieś szczególne różnice w porównaniu z zeszłorocznymi wynikami?

Pierwsze wnioski są umiarkowanie pozytywne. Przede wszystkim należy zwrócić uwagę na to, że w porównaniu z 2021 roku, kiedy przeprowadziliśmy pierwsze badanie pod patronatem UODO, zwiększyła się grupa respondentów, którzy deklarują, że wiedzą, jak rozpoznać próbę oszustwa, które ma na celu wyłudzenie danych osobowych. Na pewno wpływ na to mają szerokie działania edukacyjne podejmowane przez wiele instytucji oraz to, że także w związku z aktualną sytuacją międzynarodową temat cyberbezpieczeństwa na stałe zagościł w mediach. Drugim pozytywnym zjawiskiem jest rosnąca grupa osób, które twierdzą, że potrafią zadbać o bezpieczeństwo danych osobowych. Z drugiej strony, na podstawie przeprowadzonego w tym roku badania, zauważyliśmy także, że zwiększyła się grupa ankietowanych, którzy deklarują, że nie wiedzieliby, jak zareagować w sytuacji wyłudzenia. Widać zatem, że nasze przekonania i wstępne zapewnienie nie zawsze przekładają się potem na właściwe zachowania. To także sygnał, że działania edukacyjne, które od lat prowadzimy, a od roku wspólnie z Urzędem Ochrony Danych Osobowych, powinny być kontynuowane.

Tegoroczna edycja badań także poruszyła temat obowiązków jakie spoczywają na administratorze oraz inspektorze ochrony danych. Ponadto w przeprowadzonych badaniach znalazły się także pytania dotyczące przetwarzania danych w miejscu pracy. Dlaczego?

Temat ochrony danych osobowych jest bardzo szeroki i wpływ na ich bezpieczeństwo ma wiele czynników. Dlatego jednym z założeń naszych cyklicznych raportów jest to, żeby oprócz badania zmian w postawach i przekonaniach konsumentów, co roku dodawać coś nowego. Trudno dyskutować o procesie przetwarzania danych bez rozmowy o obowiązkach administratorów i inspektorów ochrony danych. Z kolei wiedza o tym, jak dane osobowe przetwarzają pracodawcy jest istotna dla wielu pracowników. Włączenie tych tematów do naszych badań wydało nam się zatem naturalne.

W 2022 roku, w porównaniu do roku ubiegłego, nadal tak samo definiujemy zagrożenia dla naszych danych. Tegoroczna edycja raportu „Wiedza na temat bezpieczeństwa danych osobowych w Polsce" przedstawiła wyniki badań w tej dziedzinie. Co trzeci badany uważa, że najbardziej musimy się obawiać wycieków z baz instytucji lub firm. Dlaczego tak bardzo boimy się wycieków danych?

Myślę, że powodem jest to, że wycieki danych są czymś na co nie mamy wpływu. Niezależnie od tego, jak bardzo byśmy się nie zabezpieczyli i jak dużo uwagi poświęcilibyśmy zachowaniu ostrożności, do wycieku danych i tak może dojść. Powodów może być wiele: nieaktualne oprogramowanie, przewaga technologiczna cyberprzestępców lub błąd osób lub podmiotów odpowiedzialnych za zabezpieczenie bazy danych. Nikt z nas nie ma na to wpływu. Możemy jedynie reagować na to, co się wydarzy.

Co trzeba wskazać, to boimy się wycieków danych, ale niemal połowa respondentów nie wiedziałaby, jak należy zareagować w przypadku wycieku danych osobowych?

Przede wszystkim powinniśmy jak najszybciej ustalić zakres tego wycieku, czyli dowiedzieć się, jakie dokładnie dane wpadły w ręce cyberprzestępców. Od tego zależą kolejne kroki. Przykładowo, jeśli wśród informacji, które wyciekły znalazły się także dane osobowe, np. numer PESEL, należy jak najszybciej sprawdzić, czy ktoś nie próbował ich już wykorzystać. Warto pomyśleć także nad uruchomieniem monitoringu aktywności kredytowej naszego numeru PESEL w biurze informacji gospodarczej, dzięki temu dowiemy, jeśli w przyszłości ktoś będzie chciał wyłudzić na niego pożyczkę lub inne zobowiązanie finansowe.

Według badań blisko 2/3 ankietowanych wie, z czym może się wiązać wyciek danych osobowych. Bazując na Państwa doświadczeniu, proszę wskazać najbardziej dotkliwe konsekwencje utraty swoich danych osobowych.

Przestępcy, którzy wyłudzili dane, mogą próbować wykorzystać je do zaciągnięcia różnych zobowiązań finansowych, np. pożyczki, umowy leasingowej lub zakupu na raty droższego sprzętu elektronicznego. Oczywiście obowiązek spłaty spoczywać będzie na tych, których dane zostały wykorzystane. Z naszych doświadczeń wynika, że często nie są to bardzo wysokie kwoty. Przestępcy nie chcąc wzbudzać podejrzeń,

zamiast jednej dużej pożyczki, próbują wziąć kilka mniejszych w różnych miejscach. Jeśli im się uda, wtedy taka kwota może być już wysoka.

Ponieważ do naruszeń ochrony danych osobowych dochodzi także z winy pracowników, czy możemy wskazać zachowania, które powinny wzbudzić wśród administratora niepokój.

Przede wszystkim powinniśmy dochować wszelkiej staranności, żeby dane, które gromadzimy, np. klientów lub pacjentów, przetwarzane były zgodnie z ich przeznaczeniem. Nadużycia w tej sprawie mogą prowadzić do zagrożenia w postaci wycieku danych. Należy także zwracać uwagę na wszelkie incydenty, nawet te najmniejsze, które niezgłoszone w porę również mogą przynieść przykre konsekwencja. Ostatnią rzeczą jest przykładanie szczególnej uwagi do wszystkich technicznych aspektów naszych zabezpieczeń.

Jak pokazały badania tylko niewiele ponad połowa badanych wie, jak pracodawca zabezpiecza ich dane osobowe. Jakie dobre praktyki możemy wskazać pracownikom, aby zachęcić ich do większej uważności na tym polu?

Bardzo ważne jest, żeby organizować regularne szkolenia na ten temat. Przepisy się zmieniają i warto zadbać o to, by wszyscy pracownicy byli z tym na bieżąco. Zachęcam także do tego, by temat był obecny w komunikacji wewnętrznej. Dobrym rozwiązaniem jest na przykład cykliczny mailing lub inna forma newslettera, z którego pracownicy dowiedzą się nie tylko o zmianach w przepisach, ale także o aktualnych zagrożeniach oraz nowych sposobach działania cyberprzestępców. Zalecam permanentną edukację z wykorzystaniem wielu form.

Od 2021 r. serwis ChronPESEL.pl wspólnie z Urzędem Ochrony Danych Osobowych i Krajowym Rejestrem Długów BIG SA przygotowuje obszerne raporty dotyczące wiedzy Polaków na temat ochrony danych osobowych

WIELKA BRYTANIA ZAKTUALIZOWAŁA ZASADY PRZEKAZYWANIA DANYCH DO PAŃSTW TRZECICH

Organ nadzorczy Zjednoczonego Królestwa (Information Commissioner's Office, ICO) opublikował aktualizację swoich wytycznych dotyczących przekazywania danych do państw trzecich. Zawierają one nową sekcję dotyczącą oceny ryzyka związanego z przekazywaniem danych do państw trzecich oraz narzędzie służące do przeprowadzania tej oceny.

Nowe wytyczne w Zjednoczonym Królestwie są alternatywą dla wytycznych opublikowanych przez Europejską Radę Ochrony Danych (EROD).

Opcjonalne narzędzie ICO do oceny ryzyka związanego z przekazaniem danych do państwa trzeciego zawiera sześć pytań. Dwa pierwsze z nich to:

1. Jakie są szczególne okoliczności ograniczonego przekazywania danych do państwa trzeciego?
2. Jaki jest poziom ryzyka dla osób w odniesieniu do przekazywanych danych osobowych?

Nowe wytyczne wyjaśniają różnice między podejściami ICO i EROD . W wytycznych przedstawiono osiem podstaw prawnych dla przekazywania danych osobowych do państw trzecich, na przykład wiążące reguły korporacyjne i standardowe klauzule ochrony danych, wraz z pomocnymi scenariuszami. Istnieje również osiem wyjątków wraz z pomocnymi scenariuszami.

Szczegółowe informacje:

Oceny ryzyka związanego z przekazywaniem danych do państw trzecich

Narzędzie służące do oceny ryzyka związanego z przekazywaniem danych do państw trzecich

KARY

Francja: Clearview AI ukarane administracyjną karę pieniężną w wysokości 20 mln euro

Od maja 2020 roku francuski organ nadzorczy otrzymał skargi od osób fizycznych na oprogramowanie Clearview AI dotyczące rozpoznawania twarzy i z tego powodu wszczął postępowanie.
W maju 2021 roku stowarzyszenie *Privacy International* również ostrzegło francuski organ nadzorczy o takim działaniu.

W listopadzie ub.r. francuski organ nadzorczy wezwał Clearview AI do zaprzestania zbierania i wykorzystywania danych osób na terytorium Francji w przypadku braku podstawy prawnej, w celu ułatwienia osobom fizycznym korzystania z ich praw oraz zastosowania się do ich wniosków o usunięcie danych. Jednak odpowiedź na to wezwanie nie została udzielona.

Ostatecznie sprawę skierowano do składu orzekającego, który jest odpowiedzialny za wydawanie sankcji, a ten na podstawie przedstawionych informacji postanowił nałożyć maksymalną karę pieniężną w wysokości 20 mln euro, zgodnie z art. 83 RODO.

W odniesieniu do bardzo poważnego ryzyka naruszenia praw lub wolności osób, których dane dotyczą, wynikającego z przetwarzania danych przez administratora, skład orzekający postanowił nakazać Clearview AI zaprzestanie zbierania i przetwarzania bez podstawy prawnej danych osób zamieszkałych we Francji oraz usunięcie w terminie dwóch miesięcy zebranych danych tych osób. Skład orzekający dodał do tego nakazu administracyjną karę pieniężną w wysokości 100 tys. euro za każdy dzień zwłoki przekraczający czas wskazanych dwóch miesięcy.

Źródło: decyzja organu nadzorczego

Słowenia: bezpieczeństwo mienia może stanowić uzasadniony interes dla śledzenia GPS, ale środek musi być odpowiedni i niezbędny

Słoweński organ nadzorczy uznał, że administrator nie wykazał prawnie uzasadnionych interesów zgodnie z art. 6 ust. 1 lit. f) oraz że śledzenie GPS nie było zgodne z zasadą minimalizacji danych (art. 5 ust. 1 lit. c) RODO). Organ nadzorczy nakazał administratorowi zaprzestanie przetwarzania danych pracowników, które były zbierane poprzez ciągłe, systematyczne i automatyczne śledzenie GPS.

Podstawą do wydania takiej decyzji była sprawa, w której administrator wprowadził śledzenie GPS w siedmiu pojazdach służbowych w 2009 roku, po kradzieży, która miała miejsce w jego zakładzie pracy. Pojazdy były wykorzystywane do transportu w terenie i montażu urządzeń u klienta. Celem śledzenia GPS było ubezpieczenie pojazdów, drogiego sprzętu i dokumentów, które znajdują się w pojeździe, na wypadek kradzieży.

Administrator stwierdził, że śledzenie GPS nie stanowi przetwarzania danych i że osoby fizyczne mogą być identyfikowane tylko w wyjątkowych przypadkach (przestępstwa, ochrona osób i mienia, wypadki drogowe, zdarzenie związane z roszczeniami itp.). Zastosowanie GPS nie powodowało dostępu do danych osobowych pracodawców, którzy korzystali z pojazdu, ponieważ były one przechowywane w oddzielnym zbiorze. Dane były przetwarzane przez aplikację i monitorowane przez zewnętrznego wykonawcę.

Słoweński organ nadzorczy ustalił, że administrator prowadził śledzenie GPS ośmiu pojazdów służbowych. Pojazdy te były wykorzystywane przez pracowników jako samochody dostawcze i do przewozu osób. Śledzenie odbywało się za pomocą specjalnego nadajnika w pojeździe i było monitorowane przez aplikację, która na bieżąco rejestrowała przebytą odległość. Poszczególne osoby były możliwe do zidentyfikowania.

Tworzono specjalny zbiór zawierający dużą ilość danych o lokalizacji pracowników. Dane były przetwarzane w sposób ciągły, systematyczny i automatyczny, dzięki czemu pracodawca mógł w każdej chwili ustalić, gdzie znajduje się osoba podróżująca jednym z pojazdów. Dostęp do danych był możliwy również w trybie retrospektywnym. Pracodawca mógł z łatwością zidentyfikować pracownika, który korzystał z pojazdu służbowego i któremu można przypisać dane o lokalizacji.

Słoweński urząd ds. ochrony danych badał, czy istniała podstawa prawna do przetwarzania danych osobowych zgodnie z art. 6 RODO. Organ nadzorczy oceniał, czy przetwarzanie danych było zgodne z prawem na podstawie art. 6 ust. 1 lit. f) RODO – prawnie uzasadnione interesy.

Słoweński organ potwierdził, że zapewnienie bezpieczeństwa mienia może leżeć w prawnie uzasadnionym interesie administratora danych, ale administrator nie wykazał, że sposób wykonania środka był odpowiedni i niezbędny. Ustalono, że śledzenie GPS odbywało się również w czasie, gdy pojazd i znajdujące się w nim mienie znajdowało się pod stałym i bezpośrednim nadzorem pracownika.

Zdaniem ekspertów słoweńskiego organu nadzorczego, w konkretnym przypadku śledzenie GPS mogło być stosowane tylko w ten sposób, że kierowca mógł włączyć GPS w miejscu, w którym pojazd, sprzęt i dokumenty mogły być zagrożone i wyłączyć go po powrocie do pojazdu, gdy chronione dobra były ponownie pod bezpośrednim nadzorem pracownika.

W kwestii bezpieczeństwa osób w przypadku wypadków drogowych słoweński organ nadzorczy uznał, że stałe śledzenie GPS jest nieproporcjonalne. Miejsce wypadku jest zazwyczaj znane, lokalizację wypadku mógł również zgłosić sam kierowca. Administrator powinien zastosować mniej inwazyjny środek w stosunku do prywatności informacji dotyczącej określonej osoby fizycznej.

Źródło: **decyzja organu nadzorczego**