URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO

Nr 11/11/23

SPIS TREŚCI

Szanowni Państwo!

Niedługo minie rok od powstania pierwszego polskiego kodeksu branżowego, stanowiącego ważny krok milowy w procesie zatwierdzania krajowych kodeksów i torującego drogę do powstania następnych tego typu dokumentów. W celu poprawy jakości procedur zapewnienia bezpieczeństwa danych medycznych w połowie grudnia 2022 roku Urząd Ochrony Danych Osobowych, wspólnie z Federacją Związków Pracodawców Ochrony Zdrowia Porozumienie Zielonogórskie, przyjął kodeks branżowy dedykowany małym placówkom medycznym. Obecnie trwają prace nad jego nowelizacją, co doskonale pokazuje, że przygotowanie tego typu przepisów to dopiero początek drogi, gdyż wymagają one stałego monitoringu i dostosowywania do dynamicznie zmieniającej się rzeczywistości. Jednocześnie jesteśmy na zaawansowanym etapie prac nad kolejnym kodeksem dla branży medycznej, tym razem specjaliści UODO zajęli się przygotowaniem przepisów dedykowanych dużym placówkom medycznym, takim jak szpitale, które wymagają innego podejścia i innych procedur ze względu na rodzaj i ilość danych. Szczegóły związane z pracami nad kodeksami świetnie wyjaśnia Dyrektor Departamentu Orzecznictwa i Legislacji UODO, Monika Krasińska w wywiadzie, którego udzieliła do tego numeru Biuletynu. Misją Urzędu Ochrony Danych Osobowych jest tworzenie praktyk i przepisów wymuszających traktowanie danych medycznych, należących do kategorii danych wrażliwych w sposób szczególny. Zagadnienia dotyczące danych w środowiskach, szeroko pojętej, ochrony zdrowia są przedmiotem ścisłego zainteresowania polskiego regulatora, a materia z nią związana ma dla nas wysoki priorytet.

Jednak temat rozłożenia nad pacjentem parasola opieki zapewniającej bezpieczeństwo jego danych medycznych nie kończy się oczywiście na ustanowieniu kodeksów. Ważna jest szeroko zakrojona współpraca UODO z innymi organami m.in. z Rzecznikiem Praw Pacjenta. Na tym polu ułatwiamy osobom fizycznym upominanie się o swoje prawa i dochodzenie ich na oficjalnej drodze. Takie możliwości z jednej strony upraszczają postępowanie w przypadku szkody już wyrządzonej na skutek dopuszczenia się naruszeń, z drugiej stanowią niejako straszak dla instytucji, które nie będą odpowiednio zabezpieczały danych.

Równolegle nasz Urząd pracuje nad zawarciem porozumienia ze środowiskiem pielęgniarskim – niezmiernie ważnym i niestety często niedocenianym elementem świata medycznego.

Sektor ochrony zdrowia to obszar, który dostarcza nam wielu wyzwań związanych z ochroną danych osobowych, z którymi przychodzi nam się zmierzyć.

Nie sposób nie wspomnieć o ujawnieniu wrażliwych danych lekarza przez Ministra Zdrowia Adama Niedzielskiego czy o jednej z sieci aptek, która rejestrowała rozmowy pracowników z klientami. Tego typu przypadki wymagają interwencji organu nadzorczego, który podjął stosowne czynności wyjaśniające, by dogłębnie zbadać powyższe sprawy.
Na koniec wszystkich zainteresowanych tematem ochrony danych medycznych zapraszam do udziału w ogólnopolskiej konferencji: „Medycyna przyszłości – zarządzanie, aspekty prawne, nowoczesne technologie w rozwoju ochrony zdrowia", którą UODO organizuje wspólnie z WSB. Wydarzenie odbędzie się w Dąbrowie Górniczej 7 grudnia 2023 r. Po szczegóły zapraszam wkrótce na stronę uodo.gov.pl.

Jakub Groszkowski
Zastępca Prezesa UODO

Drodzy Czytelnicy!

W tym miesiącu szczególne miejsce w naszym Biuletynie zajęła tematyka branżowych kodeksów postępowania. Urząd Ochrony Danych Osobowych widzi ogromny potencjał w ich wpływie na interpretację przepisów prawa, a także ograniczenie ryzyka nieadekwatnego przetwarzania danych. Kodeksy pełnią funkcję edukacyjną, a jednocześnie zawierają wiele praktycznych wskazówek, dotyczących tego jak zastosować RODO i przepisy branżowe w konkretnych sytuacjach, w których przetwarzane są dane osobowe. Więcej o kodeksach, w tym o pierwszym zatwierdzonym przez Urząd Kodeksie postępowania dla małych placówek w po roku funkcjonowania, a także o tym jak wygląda współpraca między UODO a podmiotem monitorującym przestrzeganie Kodeksu, dowiecie się Państwo z rozmowy z Moniką Krasińską, Dyrektor Departamentu Orzecznictwa i Legislacji w UODO.

Kontynuując temat publikacji ważnych z punktu widzenia ochrony danych, piszemy o przygotowanym przez EROD Przewodniku ochrony danych dla małych firm. Powstał z potrzeby udzielenia pomocy administratorom danych i podmiotom przetwarzającym, w planowaniu i wdrażaniu procesów umożliwiających wykrycie i szybkie powstrzymanie naruszenia, oceny ryzyka dla osób fizycznych, czy ustaleniu kiedy konieczne jest zgłaszanie naruszenia i zawiadomienie o nim osób fizycznych. Jak wiemy, niewłaściwa analiza ryzyka oraz brak zgłoszenia Prezesowi UODO naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później niż w terminie 72 godzin po jego stwierdzeniu, skutkują sankcjami organu nadzorczego. Niewłaściwa analiza i brak zgłoszenia to powody, które Urząd wskazał w uzasadnieniu swojej decyzji odnośnie kary w wysokości 103 752 zł, jaką nałożył na Link 4 Towarzystwo Ubezpieczeń S.A. w Warszawie. Skutkiem innej ciekawej decyzji, którą opisujemy w Biuletynie było upomnienie organu nadzorczego w związku z publikacją wpisu na Facebooku. Prezes UODO w swoim rozstrzygnięciu przypomniał, że w określonych okolicznościach korzystanie z portali społecznościowych i przypisanych im prywatnych profili może się wiązać z przetwarzaniem danych osobowych w rozumieniu rozporządzenia 2016/679 i musi spełniać określone w nim przepisy. Pozostając w temacie sankcji, francuski organ ochrony danych CNIL nałożył na SAF LOGISTICS, firmę zajmującą się transportem lotniczym administracyjną karę pieniężną w wysokości 200 000 euro za gromadzenie zbyt dużej ilości danych swoich pracowników, naruszanie ich prywatności i brak wystarczającej współpracy z organem. Szczegóły w artykule.

Zachęcamy też do zapoznania się z wynikami kontroli, jaką austriacki organ nadzorczy dokonał w przedsiębiorstwie, które korzystało z urządzeń śledzących GPS w pojazdach służbowych używanych przez pracowników. O tym, czy austriacki regulator podzielił argumenty co do podstaw prawnych monitoringu, na jakie powołała się firma, zgodnie z RODO dowiedzą się Państwo z naszego materiału.

Polecamy również lekturę przeprowadzonej przez Urząd analizy przepisów RODO i krajowych przepisów szczególnych, a także stanowisk innych unijnych organów nadzorczych co do praktyki nagrywania przez urzędy rozmów telefonicznych z interesantami. Jak wskazuje Prezes UODO w większości przypadków jest ona bezpodstawna.
Jak co miesiąc poruszamy kwestie związane z nowymi technologiami. Tym razem radzimy jak bezpiecznie korzystać z AR – rozszerzonej rzeczywistości. Liczymy, że nasze wskazówki pomogą użytkownikom cieszyć się ze zdobyczy techniki, a jednocześnie zadbać o swoje dane osobowe.
Przyjrzymy się też tematowi utworzenia, przez niderlandzkiego regulatora, rejestru algorytmów dla organizacji rządowych, by móc lepiej je kontrolować oraz nadzorować sposób, w jaki są wykorzystywane przez podmioty publiczne i organizacje prywatne. Piszemy też o tym, że hiszpański organ nadzorczy (AEPD) w swojej publikacji zaakcentował różnice ujęcia transparentności w projekcie rozporządzenia o AI oraz w RODO. Sztuczna inteligencja była również tematem 45. konferencji Global Privacy Assembly (GPA) – forum zrzeszającego ponad 130 organów regulacyjnych ds. ochrony danych i prywatności na całym świecie. W tym roku gospodarzem konferencji był komisarz ds. prywatności na Bermudach (PrivCom).
Na koniec chciałbym zachęcić studentów i naukowców do udziału w konkursie o przyznanie nagrody im. Stefano Rodoty, która honoruje innowacyjne i oryginalne akademickie projekty badawcze w dziedzinie ochrony danych. Do końca listopada UODO jako członek Komitetu T-PD, z ramienia Rzeczypospolitej Polskiej, zaprasza do wysłania formularza zgłoszeniowego. Zwycięzca dostanie możliwość zaprezentowania swojej pracy na kolejnej sesji plenarnej Komitetu T-PD – wśród renomowanych międzynarodowych ekspertów w dziedzinie ochrony danych osobowych i decydentów z około 90 krajów. Trzymamy kciuki za najlepsze prace!

Zachęcam Państwa do lektury

Adam Sanocki
Dyrektor Departamentu
Komunikacji Społecznej,
Rzecznik Prasowy UODO

1 ROZMOWA Z EKSPERTEM

KODEKSY POSTĘPOWANIA – INSTRUMENTY ZWIĘKSZAJĄCE OCHRONĘ DANYCH OSOBOWYCH.
W ROK PO PRZYJĘCIU PIERWSZEGO KODEKSU, CO DALEJ?

Z Moniką Krasińską, Dyrektor Departamentu Orzecznictwa i Legislacji w UODO rozmawia Karol Witowski Zastępca Rzecznika Prasowego UODO.

W połowie grudnia 2023 r. minie rok od momentu zatwierdzenia przez Prezesa UODO „Kodeksu postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych" opracowanego przez Federację Związków Pracodawców Ochrony Zdrowia Porozumienie Zielonogórskie. Jak branża przyjęła ten dokument?

Środowisko medyczne od chwili zainicjowania prac nad kodeksem wiązało z nim duże nadzieje i bardzo pozytywnie przyjęło jego zatwierdzenie. Dość powiedzieć, że niektóre małe i średnie placówki medyczne, by móc zostać członkiem kodeksu, specjalnie przystępują do Porozumienia Zielonogórskiego. Dokument ten powstał bowiem dla członków tej Federacji. A jego rola w osiąganiu najwyższych standardów w ochronie danych osobowych jest niezwykle istotna. Według danych z 7 listopada 129 podmiotów rozpoczęło procedurę przystąpienia do kodeksu, a 95 spośród nich uzyskało pozytywne certyfikaty potwierdzające uzyskanie członkostwa w kodeksie.

Generalnie można powiedzieć, że dla administratorów kodeks jest skutecznym narzędziem zapewniania rozliczalności, dla medyków ułatwieniem w pracy, a dla pacjentów – źródłem wiedzy na temat ich praw. Nic więc dziwnego, że został pozytywnie przyjęty.

Przed uchwaleniem RODO istniały instrumenty samoregulacyjne. Generalny Inspektor Ochrony Danych Osobowych współpracował na podstawie porozumień chociażby z sektorem bankowym czy marketingu bezpośredniego, które przygotowywały kodeksy dobrych praktyk będące narzędziami soft-law. Rozporządzenie o ochronie danych osobowych zmieniło podejście do tych rozwiązań. Kodeksy postępowania, bo obecnie taką mają nazwę, zyskały na znaczeniu i stały się wiążącymi instrumentami prawnymi. Przystępujące do nich podmioty mogą wykazać, że prowadzą swoje działania zgodnie z przepisami RODO. Ich stosowanie bierze się m.in. pod uwagę przy wymierzaniu administracyjnych kar pieniężnych.

Zakładam jednak, że do takich sytuacji nie będzie dochodzić. Kodeks pełni bowiem funkcję edukacyjną, a jednocześnie zawiera wiele praktycznych wskazówek, jak zastosować RODO i przepisy branżowe w konkretnych sytuacjach, w których przetwarzane są dane osobowe. Ponadto o wdrożenie jego postanowień w poszczególnych placówkach dba podmiot monitorujący.

Czy to prawda, że kodeks będzie nowelizowany?

To naturalne, że takie dokumenty wymagają aktualizacji. Ich nowelizacje to oczywisty proces. Kodeks musi bowiem uwzględniać zmiany przepisów i najnowsze orzecznictwo, a jednocześnie cały czas odpowiadać aktualnym potrzebom nie tylko

podmiotów medycznych, ale przede wszystkim pacjentów i innych osób, których dane podmioty medyczne przetwarzają.
Obecnie inicjatorzy powstania „Kodeksu postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych" rzeczywiście rozważają nowelizację tego dokumentu. Skłaniają ich do tego m.in. zmiany w przepisach prawa oraz pierwsze doświadczenia zdobyte w czasie stosowania kodeksu. Pod koniec września odbyło się spotkanie przedstawicieli UODO oraz wnioskodawców i twórców kodeksu oraz podmiotu monitorującego (Federacja Związków Pracodawców Ochrony Zdrowia Porozumienie Zielonogórskie, Jamano sp. z o.o., RS Jamano sp. z o.o. sp. k.), w czasie którego omówiono zakres planowanych zmian. Mogą one dotyczyć takich zagadnień, jak m.in.: monitoring wizyjny, naruszenia ochrony danych, weryfikacja tożsamości, a także zapobieganie cyber-zagrożeniom. Warto pamiętać, że w branży medycznej przetwarzane są na dużą skalę szczególne kategorie danych, więc ich bezpieczeństwo jest niezmiernie istotne z punktu widzenia ochrony prywatności. Obecnie UODO czeka na oficjalne przedstawienie przez wnioskodawcę konkretnych propozycji zmian w Kodeksie.

Jak wygląda obecnie współpraca między UODO a podmiotem monitorującym przestrzeganie Kodeksu, czy taka współpraca jest konieczna?
Zakres współpracy podmiotu monitorującego z UODO wynika zarówno z przepisów prawa, jak i postanowień Kodeksu, który stanowi m.in., że podmiot monitorujący raz do roku informuje Prezesa UODO o wszelkich działaniach prowadzonych przez niego w odniesieniu do kodeksu postępowania, zwłaszcza zaś o tym, ile i które placówki przystąpiły do kodeksu; ile skarg na nie wpłynęło do podmiotu monitorującego, jakich problemów najczęściej dotyczą i w jaki sposób zostały załatwione. Ma też informować o czynnościach sprawdzających przeprowadzonych w następstwie stwierdzenia naruszenia kodeksu. Pierwszy taki raport jeszcze przed nami.
Niezależnie od tego pozostajemy z przedstawicielami podmiotu monitorującego w częstym kontakcie. Dzięki temu UODO ma niezbędne informacje dotyczące praktyki funkcjonowania kodeksu, a podmiot monitorujący - możliwość bieżącego zapoznawania się ze stanowiskami UODO odnoszącymi się m.in. do zmian w przepisach mających wpływ na postanowienia kodeksu.

W lutym 2021 r. Prezes UODO pozytywnie zaopiniował projekt Kodeksu postępowania dla sektora ochrony zdrowia złożonego przez Polską Federację Szpitali. Dlaczego branża medyczna podzieliła się na dwa segmenty? I dlaczego ten drugi Kodeks jeszcze nie został zatwierdzony?
Każdy z kodeksów medycznych był tworzony dla potrzeb różnych środowisk.
Ten już zatwierdzony jest dedykowany niedużym podmiotom. Ten, którego twórcą jest Polska Federacja Szpitali, ma być przeznaczony dla większych placówek.
Poza tym powodem podziału branży medycznej na dwa segmenty są kwestie ich statusu. Art. 41 ust. 6 RODO wyłącza możliwość monitorowania zatwierdzonych kodeksów postępowania w odniesieniu do przetwarzania prowadzonego przez organy i podmioty publiczne.

Warto pamiętać, że w branży medycznej przetwarzane są na dużą skalę szczególne kategorie danych, więc ich bezpieczeństwo jest niezmiernie istotne z punktu widzenia ochrony prywatności.

Biorąc pod uwagę ten przepis, Federacja Porozumienie Zielonogórskie podjęła decyzję o wyłączeniu placówek publicznych z możliwości przystąpienia do Kodeksu. Takie podejście ma wyraźne zalety, ponieważ mimo tego, iż małe gabinety lekarskie i duże placówki, jak szpitale, muszą stosować te same przepisy dotyczące ochrony danych, w praktyce sposób realizacji tych obowiązków znacząco się różni. Kodeks Polskiej Federacji Szpitali ma objąć podmioty publiczne, więc wymaga wpisania do niego mechanizmów monitorowania, które będą podobne do mechanizmów stosowanych przez podmioty monitorujące, a jednocześnie wynikające z krajowych przepisów. Stworzenie takich mechanizmów nie jest proste, nie tylko w warunkach prawa polskiego. W żadnym kraju stosującym RODO nie zatwierdzono jeszcze kodeksu postępowania dla podmiotów publicznych. Na szczęście jesteśmy już na końcu tej drogi, gdyż Polska Federacja Szpitali przedstawiła propozycje monitorowania satysfakcjonujące z punktu widzenia wymogów RODO.

Które środowiska czekają na swoje kodeksy branżowe? Nad którymi kodeksami prace już trwają?
Na stronie internetowej UODO w zakładce „Kodeksy i certyfikacja" na bieżąco informujemy o tym, które środowiska pracują nad opracowaniem kodeksu dla swojej branży, a które złożyły wnioski o ich zatwierdzenie.
Dotychczas do Prezesa UODO, oprócz dwóch powyższych kodeksów dla sektora medycznego, zgłoszono jeszcze siedem formalnych wniosków o zatwierdzenie kodeksów postępowania. Wiemy też, że powstało jeszcze sześć innych inicjatyw, ale dotąd nie przedłożyły one organowi nadzorczemu formalnych wniosków o zatwierdzenie projektów kodeksów.
Pierwsze wnioski o zatwierdzenie kodeksu wpłynęły do Prezesa UODO jeszcze przed początkiem stosowania RODO i nie mogły być procedowane. Po maju 2018 r. złożono wnioski dla kodeksów medycznych, sektora bankowego, spółdzielni mieszkaniowych, branży badań rynku czy marketingu bezpośredniego. Niektóre z projektów kodeksów powielały tylko RODO, inne zawierały rozwiązania, które zdaniem organu nadzorczego były niedopuszczalne. Wnioskodawca wolał czasem wycofać wniosek o zatwierdzenie kodeksu niż zrezygnować z tych rozwiązań. W innym przypadku wnioskodawca nie był w stanie wykazać, że reprezentuje administratorów czy podmioty przetwarzające z branży i postępowanie o zatwierdzenie kodeksu postępowania umorzono.
Ponadto przeprowadziliśmy dwa postępowania, które są związane z akredytacją. Mieliśmy również sześć wniosków o akredytację podmiotu monitorującego, z czego cztery sprawy zostały zakończone wobec nieuzupełnienia braków formalnych albo niespełnienia podstawowych kryteriów, które warunkują rozważenie udzielenia akredytacji, czyli dalsze procedowanie sprawy przez organ nadzorczy.
Jednocześnie UODO, w związku z uczestnictwem w pracach Europejskiej Rady Ochrony Danych, brał udział w opiniowaniu dwóch europejskich kodeksów dedykowanych przetwarzaniu danych w chmurze oraz kilku niezatwierdzonych jeszcze kodeksów krajowych.

Kodeksy powinny być konstruowane w taki sposób, aby wprowadzić jednolity standard w podejściu do kluczowych zagadnień związanych ze stosowaniem RODO, dać jednoznaczne i skuteczne wskazówki postępowania dotyczące przetwarzania danych osobowych z uwzględnieniem specyfikacji danej branży.

1 ROZMOWA Z EKSPERTEM

Dlaczego prace nad kodeksami trwają tak długo?

Kodeksy powinny być konstruowane w taki sposób, aby wprowadzić jednolity standard w podejściu do kluczowych zagadnień związanych ze stosowaniem RODO, dać jednoznaczne i skuteczne wskazówki postępowania dotyczące przetwarzania danych osobowych z uwzględnieniem specyfiki danej branży. Opracowanie dojrzałego kodeksu wymaga poważnego przedyskutowania i dokładnego zinwentaryzowania wszystkich problemów, które odnotowuje dany sektor. Mówimy tu o rzeczywistych, istniejących problemach oraz próbie znalezienia antidotum na ich rozwiązanie poprzez stosowanie konkretnych przepisów RODO czy też krajowych przepisów sektorowych. Inwentaryzacja problemów, a także zasobów administratorów jest tutaj bardzo ważna. Dzięki pracom nad kodeksem administratorzy i podmioty przetwarzające mogą na nowo przyjrzeć się funkcjonującym procedurom i rozwiązaniom technicznym czy organizacyjnym. Analiza tego, co chcielibyśmy w kodeksie przygotować i poddać później pod ocenę organu nadzorczego powinna rozpocząć się od bardzo dokładnego przyjrzenia się, jak wygląda „od środka" dana organizacja czy branża. Dlatego w przygotowaniu kodeksu tak niezmiernie ważne jest czynne uczestnictwo przedstawicieli środowiska, dla którego ten dokument powstaje. Pozyskanie pełnej wiedzy o faktycznych problemach i o stosowaniu przepisów o ochronie danych osobowych w celu ich rozwiązania powinno być okazją do standaryzacji procedur.

Od strony formalnej warunkiem przyjęcia kodeksu postępowania jest przedłożenie jego projektu organowi nadzorczemu do zatwierdzenia. Projekt taki musi spełniać wymogi określone w RODO i ustawie o ochronie danych osobowych, a także w Wytycznych EROD nr 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących. Przedłożenie wniosku o zatwierdzenie kodeksu postępowania wiąże się również z obowiązkiem uiszczenia opłaty skarbowej.

Co ważne, poprawnie złożony wniosek powinien zawierać informację o przeprowadzonych przed złożeniem wniosku konsultacjach publicznych oraz ich wyniku.

Natomiast sama procedura zatwierdzenia kodeksu postępowania składa się z kilku etapów. W pierwszym organ nadzorczy dokonuje wstępnej oceny projektu kodeksu. Bada, czy przedłożony projekt spełnia wymogi formalne oraz kryteria dopuszczalności, o których mowa w Wytycznych EROD. Drugi etap związany jest z oceną treści. Służy jej wyjaśnieniu z wnioskodawcą, umożliwiając mu wprowadzenie ewentualnych modyfikacji. Kończy się zaś wydaniem przez organ nadzorczy opinii o zgodności przedłożonego projektu z przepisami RODO. Ostatni etap obejmuje zatwierdzenie kodeksu postępowania w formie decyzji administracyjnej, o ile organ nadzorczy uzna, że stanowi on odpowiednie zabezpieczenie właściwego stosowania RODO.

Z dotychczasowych doświadczeń UODO zebranych w czasie prac na projektami kodeksów postępowania wynika, że środowiska inicjujące prace nad tymi dokumentami popełniają błędy, które często wpływają na wydłużenie procedury zatwierdzenia kodeksu, zawieszenie prac nad projektem, a nawet całkowite zaniechanie przygotowania takiego dokumentu. Żeby uniknąć takich problemów, a podmiotom zainteresowanym stworzeniem kodeksów ułatwić prace nad nimi, przygotowaliśmy specjalny materiał zawierający wiele cennych podpowiedzi w tym zakresie. Jest on dostępny na naszej stronie internetowej.

1 ROZMOWA Z EKSPERTEM

Dla której branży opracowanie kodeksu będzie najtrudniejsze?
To raczej nie problem branży, lecz braku w niej podmiotu, który można by uznać za reprezentatywny dla niej, a więc uprawniony do złożenia wniosku o zatwierdzenie kodeksu. Byliśmy już informowani o takich inicjatywach i podejmowaliśmy rozmowy z zainteresowanymi, dyskutując, jak można by rozwiązać ten problem. Przykładem może być inicjatywa stworzenia przez IOD-ów ze szkół kodeksu dla sektora oświaty.
Innym istotnym problemem jest omówione wyżej stworzenie odpowiednich mechanizmów monitorowania w przypadku kodeksów odnoszących się do podmiotów publicznych.
W tym kontekście chciałabym natomiast podkreślić, że nie ma ustalonego zakresu zagadnień, które kodeks postępowania musi regulować. Może więc powstać kodeks obejmujący niewielki wycinek spraw za to charakterystycznych i ważnych dla branży, a wskazanie praktycznych, zgodnych z RODO rozwiązań, które powinny być stosowane w konkretnych sytuacjach, może stanowić ważną wartość kodeksu.

Jak kwestie kodeksów wyglądają w innych krajach? Jak Polska wypada pod tym względem na tle innych państw członkowskich?
Całkiem nieźle. W wielu krajach nie ma zatwierdzonego żadnego kodeksu postępowania. Wiele zatwierdzonych kodeksów ma niewielki zakres przedmiotowy. Tylko w Polsce zatwierdzono kodeks dla branży medycznej (poza badaniami klinicznymi), a niedługo może zostanie zatwierdzony drugi i kolejne.
Sukcesywnie uzupełniany rejestr wszystkich zatwierdzonych kodeksów postępowania jest dostępny na stronie internetowej EROD. Są tam informacje zarówno o kodeksach obowiązujących w poszczególnych państwach członkowskich, jak i o kodeksach transgranicznych.

Czy problemem jest wybór podmiotów akredytowanych do pełnienia funkcji monitorującej stosowanie poszczególnych kodeksów?
Żeby kodeks mógł pełnić swoją funkcję, musi istnieć niezależny, sprawnie funkcjonujący podmiot monitorujący. Musi być on zaakceptowany przez organ nadzorczy w odrębnym postępowaniu akredytacyjnym. Mamy świadomość, jakie trudności mają podmioty składające wnioski o zatwierdzenie kodeksów z wyznaczaniem takiego podmiotu monitorującego, z jego funkcjonowaniem, zakresem jego działań i spełnieniem kryteriów dla funkcjonowania takiego podmiotu, wynikających i z samego rozporządzenia, i z wytycznych Europejskiej Rady Ochrony Danych.
M.in. dlatego podjęliśmy prace nad określeniem wymogów akredytacji podmiotów monitorujących kodeksy. Projekty były szeroko dyskutowane i analizowane przez wiele środowisk. Następnie wymogi te zostały przez Prezesa Urzędu Ochrony Danych Osobowych skonsultowane na podstawie przepisów rozporządzenia o ochronie danych osobowych z Europejską Radą Ochrony Danych z zastosowaniem mechanizmu spójności, a następnie po uwzględnieniu uwag EROD zostały opublikowane w sposób wynikający z obowiązujących przepisów.

1 ROZMOWA Z EKSPERTEM

Dlaczego kodeksy postępowania są tak ważne i dlaczego powinny powstawać?
Opracowanie i sprawne funkcjonowanie kodeksów leży w interesie administratorów, przetwarzających dane, a także osób, których dane dotyczą. Są one zbiorem zatwierdzonych przez Prezesa UODO zasad, które wskazują, jak zastosować RODO i przepisy branżowe w konkretnych sytuacjach i pomagają zapewnić wysoki poziom ochrony danych osobowych. Jednocześnie umożliwiają podmiotom, które do nich przystąpiły, skupienie się na podstawowej działalności.
Przykładowo firmy stosujące kodeks dla małych placówek medycznych mogą skoncentrować się na udzielaniu świadczeń zdrowotnych, a jednocześnie poza regulacjami zawartymi w Kodeksie, wskazującymi, jak mają postępować w konkretnych przypadkach, otrzymują od jego twórców wsparcie w zakresie stosowania postanowień RODO, dostęp do bazy wiedzy dedykowanej dla danej branży, a także wsparcie przy incydentach związanych z przetwarzaniem danych osobowych. Urząd Ochrony Danych Osobowych widzi w kodeksach ogromny potencjał. Także dlatego, że właściwie przygotowane pozwalają skutecznie wyeliminować ryzyko niewłaściwej interpretacji przepisów prawa, a także ryzyko nieadekwatnego przetwarzania danych czy wprowadzania zbędnych procesów przetwarzania danych. Poza tym rozwiązania kodeksowe mogą stosować także podmioty niebędące jego członkami, co będzie powodowało upowszechnianie praktyk zaakceptowanych przez organ nadzorczy również w tych podmiotach.
Dla wielu administratorów istotne może być to, że stosowanie zatwierdzonego kodeksu postępowania będzie czynnikiem branym pod uwagę przez organ nadzorczy przy ocenie poszczególnych aspektów przetwarzania danych dokonywanej w przypadku zgłoszonych naruszeń ochrony danych czy przy wydawaniu rozstrzygnięć, które będą zapadały w decyzjach administracyjnych zamykających postępowania skargowe, pokontrolne czy wszczęte z urzędu. W przypadku naruszenia przepisów RODO przestrzeganie zatwierdzonego kodeksu postępowania może mieć także wpływ na rodzaj zastosowanego środka naprawczego stosowanego przez organ nadzorczy, w tym na wysokość administracyjnej kary pieniężnej. Warto też zaznaczyć, że osoby, których dane dotyczą, skargę odnoszącą się do naruszenia postanowień kodeksu mogą złożyć do podmiotu monitorującego. To otwiera drogę do polubownego jej załatwienia, a jednocześnie przyspiesza realizację praw do ochrony danych.
Nie ma obowiązku przystępowania do grona firm stosujących branżowe kodeksy postępowania. Gorąco jednak do tego zachęcam, ponieważ wiąże się to z licznymi korzyściami.

2 UODO SYGNALIZUJE

CZY URZĄD MOŻE NAGRYWAĆ ROZMOWY Z INTERESANTAMI?

Przeprowadzona przez UODO analiza przepisów RODO i krajowych przepisów szczególnych, a także stanowisk innych unijnych organów nadzorczych prowadzi do wniosku, że urzędy muszą przemyśleć praktykę nagrywania rozmów telefonicznych z interesantami. W większości przypadków jest ona bowiem bezpodstawna.

Z prośbą o zajęcie stanowiska w tej kwestii zwrócił się do UODO jeden z inspektorów ochrony danych (IOD). Swoje wątpliwości opisał na przykładzie urzędów gmin. Jak wskazał:

Część administratorów decyduje się w imię ochrony interesów pracowników urzędu na nagrywanie rozmów przychodzących za zgodą dzwoniących petentów. Oczywiście owa zgoda polega na kontynuacji rozmowy po usłyszeniu komunikatu o takim wyborze, a nieudzielenie zgody polega na rozłączeniu się i wybraniu się osobiście do urzędu w celu załatwienia sprawy czy pozyskania informacji.

W mojej opinii nie ma żadnej, legalnej i usprawiedliwionej przesłanki do takiego procederu. Trudno uznać za dobrowolną zgodę opartą o reguły art. 6 ust. 1 lit. a RODO, jeśli alternatywą dla nagrywanej rozmowy jest „wycieczka" do czasami odległego urzędu. Sądzę, że za zgodą petenta można byłoby rozmowę nagrywać, ale dla celów służących samemu petentowi i przy zachowaniu możliwości kontynuacji rozmowy bez opcji nagrywania. Jeśli jednak administrator motywuje nagrywanie rozmów interesem własnym, tj. ograniczeniem „nieprzyjemnych rozmów", gróźb i obelg rzucanych przez interesantów w rozmowie z urzędnikiem, to uważam to za przesłankę opisaną w art. 6 ust. 1 lit. f RODO, co w wypadku relacji między urzędem a petentem jest wyraźnie zabronione w ostatnim zdaniu tego artykułu.

Uważam, że niedorzeczność wyboru opcji przetwarzania danych w oparciu o dobrowolnie wyrażoną zgodę widać jak na dłoni w hipotetycznej, ale możliwej do wyobrażenia sytuacji. Mianowicie petent może zgodzić się na nagrywanie, obrazić czy grozić urzędnikowi, następnie cofnąć zgodę na przetwarzanie danych i zażądać usunięcia danych, tj. nagrania. (…)

Kolejnym problemem, już na gruncie praw dostępu do urzędów publicznych dla obywateli, jest sam fakt ograniczania kontaktu telefonicznego z takim urzędem, często w sprawach błahych i zmuszanie obywatela – wobec niechęci do nagrywania rozmowy – do odwiedzin osobistych w urzędzie.

Proszę zatem o opinię rozstrzygającą, czy urzędy gminy i im podobne instytucje publiczne mają prawo nagrywania rozmów wg powyższego modelu, a jeśli tak, to jaka będzie przesłanka przetwarzania danych w systemach zapisu owych rozmów. (…).

W odpowiedzi UODO wskazał, że dla zajęcia wiążącego stanowiska niezbędna jest dokładna znajomość wszystkich okoliczności faktycznych danego przypadku, w którym prowadzone jest nagrywanie, w tym rodzaju przetwarzanych danych, warunków i celów ich przetwarzania. Niemniej przeprowadzona analiza przepisów RODO i krajowych przepisów szczególnych, a także stanowisk innych unijnych organów nadzorczych prowadzi do wniosku, że co do zasady praktyka ta jest bezpodstawna.

Co trzeba wziąć pod uwagę?
Żeby wskazać właściwą podstawę przetwarzania danych osobowych przez administratora w konkretnej sytuacji, należy rozpocząć od ustalenia, jakich kategorii osób przetwarzanie dotyczy i jakich kategorii są to dane.

Następnie należy ustalić cel tego przetwarzania w odniesieniu do danych osób określonej kategorii. Określenie celu jest elementem niezbędnym dla dokonania oceny, czy określone działanie jest dopuszczalne i ewentualnie na jakiej podstawie. Dane osobowe muszą być bowiem zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami – zgodnie z zasadą ograniczenia celu (art. 5 ust. 1 lit. b RODO).

W Wytycznych Grupy Roboczej Art. 29 w sprawie przejrzystości na podstawie rozporządzenia 2016/679, WP260 rev.01 str. 9 znajdują się wskazówki, jak zgodnie z zasadą przejrzystości formułować informacje kierowane do podmiotów danych, w tym jak należy przedstawiać cel przetwarzania danych osobowych: „Informacje powinny być konkretne i jednoznaczne; nie należy ich formułować przy pomocy pojęć abstrakcyjnych lub wieloznacznych ani pozostawiać dowolności interpretacji. Należy zwłaszcza jednoznacznie określić cele i podstawę prawną przetwarzania danych osobowych.” W przypadku nagrywania rozmów pracowników z interesantami telefonującymi do urzędu, dochodzić będzie do przetwarzania danych osobowych zarówno dzwoniących, jak i pracowników urzędu.

Czy jest podstawa do nagrywania dzwoniących interesantów?

Jeśli chodzi o przetwarzanie przez urząd danych osobowych interesantów, to w pierwszej kolejności należy ocenić, jakie są faktyczne cele pozyskiwania i dalszego przetwarzania tych danych. Ustalenie faktycznych celów jest kluczowe dla podjęcia decyzji o potrzebie aż tak głębokiej ingerencji w prywatność osób, jaką jest ich nagrywanie. Czy celem tym, jak wskazał IOD, może być „ochrona interesów pracowników urzędu”? To wątpliwe, tym bardziej że nie wiadomo, o ochronę jakich interesów chodzi i w jaki sposób nagrywanie rozmów miałoby się do tego przyczynić.

2 UODO SYGNALIZUJE

Trzeba mieć na uwadze, że osoby, których dane dotyczą, w większości przypadków telefonują do urzędu w celu uzyskania informacji odnoszących się do zadań realizowanych przez urząd i dane pozyskiwane poprzez nagrywanie tych rozmów będą dotyczyły tych zadań i spraw z nimi związanych. Będzie to miało wpływ zarówno na kategorie osób, których dane dotyczą, jak i zakres oraz kategorie danych pozyskiwanych w wyniku nagrywania.
W tym kontekście należy wziąć pod uwagę to, że przetwarzanie danych osobowych zwykłych jest legalne tylko wtedy, gdy odbywa się na podstawie jednej z przesłanek określonych w art. 6 RODO. W analizowanej sytuacji nie można też wykluczyć, że pozyskiwane będą dane szczególnych kategorii, których przetwarzanie – zgodnie z art. 9 ust. 1 RODO – jest co do zasady zabronione. Nie można również wykluczyć pozyskiwania w tej formie danych, o których mowa w art. 10 RODO, które jest dopuszczalne jedynie na zasadach określonych w tym przepisie.
Co do podstaw prawnych przetwarzania zwykłych danych osobowych przez podmioty publiczne przesłankami mającymi najczęściej zastosowanie są przesłanki określone w art. 6 ust. 1 lit. c i e RODO. Zatem w odniesieniu do przetwarzania danych interesantów administrator będący podmiotem publicznym powinien przede wszystkim ustalić, czy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c) lub czy przetwarzanie danych jest niezbędne do wykonywania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 6 ust. 1 lit. e). Obydwie przesłanki wskazują na niezbędność przetwarzania na ich podstawie. Ponadto zgodnie z art. 6 ust. 3 RODO podstawa przetwarzania w przypadku tych przesłanek musi być określona w prawie Unii lub w prawie krajowym. A zatem przyjęcie podstawy przetwarzania w oparciu o przesłankę z art. 6 ust. 1 lit. c lub art. 6 ust. 1 lit. e RODO może nastąpić tylko w powiązaniu z właściwym przepisem prawa unijnego lub krajowego.

Obecnie nie ma przepisu, który uprawniałby organy gminy do rejestrowania rozmów telefonicznych dla realizacji ich zadań czy też w ramach sprawowania władzy publicznej. Przepisy procedury administracyjnej przewidują, że sprawy administracyjne mogą być załatwiane ustnie, telefonicznie, za pomocą środków komunikacji elektronicznej lub innych środków łączności. Nie można tu jednak stosować automatyzmu, bo telefoniczne załatwienie sprawy – zgodnie z art. 14 § 2 kodeksu postępowania administracyjnego – możliwe jest jedynie wtedy, gdy przemawia za tym interes strony, a przepis prawny nie stoi temu na przeszkodzie. Ponadto – zgodnie ze zdaniem drugim tego paragrafu – treść oraz istotne motywy takiego załatwienia powinny być utrwalone w aktach w formie protokołu lub podpisanej przez stronę adnotacji. Przepisy kodeksu postępowania administracyjnego nie uprawniają zatem do utrwalania załatwienia sprawy w formie nagrania rozmowy telefonicznej. A to oznacza, iż urząd przy pozyskiwaniu danych osobowych w związku z nagrywaniem rozmów telefonicznych nie mógłby powołać się na art. 6 ust. 1 lit. c lub e RODO.
Organy administracji publicznej co do zasady nie powinny powoływać się również na zgodę osób, które dzwonią do urzędu gminy w sprawach odnoszących się do zadań gminy z uwagi na wyraźny brak równowagi w stosunkach między administratorem będącym władzą publiczną a osobą, której dane dotyczą. W większości przypadków nie ulega również wątpliwości, że osoba, której dane dotyczą, nie będzie miała realnej alternatywy wobec zaakceptowania (warunków) przetwarzania zaproponowanych przez tego administratora (motyw 43 RODO).

Po drugie zaś, żeby zgoda mogła stanowić podstawę przetwarzania danych, musi spełniać bardzo konkretne warunki określone w art. 4 pkt 11 oraz w art. 7 RODO. Tymczasem w analizowanej sytuacji osoba, której dane dotyczą, nie będzie miała możliwości telefonicznego załatwienia sprawy bez nagrywania jej rozmowy. Zgoda, o której mowa w RODO, nie może być obarczona jakimkolwiek elementem przymusu, presji lub braku możliwości swobodnego złożenia oświadczenia woli.
Za dobrowolne wyrażenie zgody w rozumieniu RODO − jak wskazała Europejska Rada Ochrony Danych w Wytycznych dotyczących zgody na mocy rozporządzenia 2016/679 (str. 7) − nie można uznać sytuacji, w której osobie, której dane dotyczą, nie przysługuje rzeczywista możliwość wyboru, czuje się ona zmuszona do wyrażenia zgody lub poniesie negatywne konsekwencje w przypadku jej niewyrażenia.
Dodać należy, że zgodnie z brzmieniem motywu 43 RODO, aby zapewnić dobrowolność, zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem, w szczególności gdy administrator jest organem publicznym i dlatego jest mało prawdopodobne, by w tej konkretnej sytuacji zgodę wyrażono dobrowolnie we wszystkich przypadkach.
Jeśli chodzi o stosowanie przez organy publiczne przesłanki określonej w art. 6 ust. 1 lit. f RODO, to należy podkreślić, iż w tym przepisie znajduje się zastrzeżenie, iż podstawa prawna wskazana w lit. f nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań. Prawnie uzasadniony interes administratora nie powinien mieć zastosowania jako podstawa prawna do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań, bowiem podstawę prawną przetwarzania danych osobowych powinien określić ustawodawca (motyw 47 RODO). A zatem omawiana przesłanka mogłaby być zastosowana przez podmioty publiczne, jednak nie w sytuacji, w której realizują one swoje zadania określone w przepisach jako ustawowe kompetencje.

Czy można nagrywać rozmowy telefoniczne pracowników?
Na skutek nagrywania rozmów telefonicznych z interesantami urzędu gminy dochodzi także do pozyskiwania danych osobowych pracowników, a to z kolei determinuje konieczność oceny legalności takich działań na gruncie przepisów prawa pracy, które wprowadziły dla procesów przetwarzania danych osobowych związanych z zatrudnieniem szczególne gwarancje, o których stanowi art. 88 RODO. Przede wszystkim należy wskazać, że przepisy kodeksu pracy wskazują, jakie informacje i w jakich celach pracodawca może pozyskiwać od pracownika. Przepisy te regulują też szczegółowo, kiedy i na jakich warunkach pracodawca może prowadzić monitoring pracownika, a nie ma wątpliwości, że nagrywanie rozmów pracownika stanowi inny monitoring (kontrolę) pracownika, o którym mowa w art. 22^3 § 4 kodeksu pracy. Zgodnie z tym przepisem prowadzenie monitoringu pracownika byłoby możliwe jedynie w sytuacji, jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwe użytkowanie udostępnionych pracownikowi narzędzi pracy. A zatem wskazany w piśmie IOD cel nagrywania rozmów, jakim jest „ochrona interesów pracowników”, nie jest wymieniony w powołanym przepisie, a tym samym nagrywanie rozmów pracowników w takim celu nie znajduje podstaw w przepisach kodeksu pracy.

Ani „ochrona interesów pracowników”, ani ich zgoda nie mogą stanowić podstawy uprawniającej urząd do nagrywania ich rozmów z interesantami.

W analizowanej sytuacji również zgoda pracownika nie może stanowić ważnej podstawy prawnej przetwarzania danych osobowych ze względu na wyraźny brak równowagi między osobą, której dane dotyczą a administratorem (motyw 43 RODO). Zgodnie z RODO powinna być ona dobrowolna, świadoma i pracownik ma prawo ją odwołać bez negatywnych konsekwencji dla niego (motyw 42 oraz art. 4 pkt 11 i art. 7 RODO).

Jakie obostrzenia wprowadza Prawo telekomunikacyjne?
Analiza dopuszczalności nagrywania rozmów powinna uwzględniać również przepisy ustawy z dnia 16 lipca 2004 r. -– Prawo telekomunikacyjne. Art. 159 Prawa telekomunikacyjnego wskazuje, kiedy dopuszczalne jest nagrywanie rozmów telefonicznych. Zgodnie z ustępem 2 tego artykułu zakazane jest zapoznawanie się, utrwalanie, przechowywanie, przekazywanie lub inne wykorzystywanie treści lub danych objętych tajemnicą telekomunikacyjną przez osoby inne niż nadawca i odbiorca komunikatu, chyba że:

1. będzie to przedmiotem usługi lub będzie to niezbędne do jej wykonania,
2. nastąpi za zgodą nadawcy lub odbiorcy, których dane te dotyczą,
3. dokonanie tych czynności jest niezbędne w celu rejestrowania komunikatów i związanych z nimi danych transmisyjnych, stosowanego w zgodnej z prawem praktyce handlowej dla celów zapewnienia dowodów transakcji handlowej lub celów łączności w działalności handlowej,
4. będzie to konieczne z innych powodów przewidzianych ustawą lub przepisami odrębnymi.

Jakie są wnioski?
A zatem, czy urząd może nagrywać rozmowy telefoniczne z interesantami? Biorąc pod uwagę powołane wyżej regulacje, w większości przypadków nie ma podstaw, by urzędy nagrywały rozmowy telefoniczne z interesantami. Dlatego powinny one jak najszybciej przeprowadzić kompleksową analizę swoich praktyk.

3 WYBRANE DECYZJE UODO

PUBLIKACJA POSTU NA FACEBOOKU MOŻE WIĄZAĆ SIĘ Z PRZETWARZANIEM DANYCH OSOBOWYCH

Skarżony opublikował na swoim profilu na Facebooku wpis, do którego załączył zdjęcie postanowienia sądu rejonowego. Dotyczyło ono postępowania, w którym sam występował w charakterze strony. Na postanowieniu widniały również dane osobowe w postaci imienia i nazwiska oraz daty urodzenia innych uczestników postępowania.

Osoba, której dane zostały w ten sposób upublicznione zdecydowała się wnieść skargę do Prezesa UODO na niezgodne z prawem przetwarzanie jej danych osobowych oraz małoletniej osoby, której jest przedstawicielem ustawowym. Przed wniesieniem skargi do organu nadzorczego, skarżony usunął wpis ze swojego profilu.
W swoich wyjaśnieniach skarżony, poprzez swojego pełnomocnika, wskazał m.in., że „nie udostępnił" danych osobowych skarżącej oraz małoletniej osoby i że aktualnie ich dane nie są publikowane na Facebooku. Podniósł również, że przepisy rozporządzenia 2016/679 nie mają w badanej sprawie zastosowania, ponieważ publikacja wpisu i towarzyszącego mu zdjęcia na portalu społecznościowym stanowi czynność o czysto osobistym lub domowym charakterze.
Badając sprawę, organ nadzorczy w pierwszej kolejności stwierdził, iż skarżony publikując zdjęcie odpisu postanowienia, na którym widniały imię, nazwisko oraz data urodzenia, udostępnił w ten sposób dane osobowe skarżącej i małoletniej osoby.

Publikacja postu na Facebooku – czynność o czysto osobistym lub domowym charakterze?
W następnej kolejności organ podjął się ustalenia, czy podniesiony przez skarżonego tzw. „wyjątek domowy i osobisty", o którym mowa w art. art. 2 ust. 1 pkt. c rozporządzenia 2016/679 ma miejsce w badanej sprawie. Wskazany przepis doprecyzowuje motyw 18 preambuły RODO lub rozporządzenia 2016/679, zgodnie z którym działalność osobista lub domowa może między innymi polegać na korespondencji i przechowywaniu adresów, podtrzymywaniu więzi społecznych oraz działalności internetowej podejmowanej w ramach takiej działalności.
Na pierwszy rzut oka wszystko się zgadza. Czy można bowiem uznać Facebooka za coś innego, niż internetowe narzędzie do podtrzymywania więzi społecznych? Przyglądając się jednak powyższej kwestii nieco bliżej, organ zauważył, że w piśmiennictwie nie jest ona tak oczywista i budzi pewne istotne wątpliwości. Przytoczył w tym kontekście opinię Grupy Roboczej Art.29, przyjętą jeszcze na gruncie dyrektywy 95/46/WE, która uznała, że „przetwarzanie danych przez użytkowników w portalach społecznościowych mieści się – co do zasady – w zakresie czynności osobistych lub domowych, chyba że dostęp do danych mają inne osoby niż te, które zostały wybrane samodzielnie przez użytkownika, np. poprzez dodanie do kontaktów". Sam charakter portali społecznościowych, oferujących usługi komunikatorów internetowych i przestrzeni do publikacji zdjęć i postów, może zatem sprzyjać zaklasyfikowaniu ich do kategorii „czynności o czysto osobistym lub domowym charakterze". Jak sugeruje fragment przytoczonej powyżej opinii, nie może być to jednak klasyfikacja automatyczna. Nie bez znaczenia jest bowiem co, w jakim celu i komu udostępniamy na swoim profilu społecznościowym, zwłaszcza jeżeli dotyczy to tak newralgicznych pod kątem prywatności obszarów jakim jest chociażby postępowanie sądowe.
Organ wskazał, że skarżony zamieścił swój wpis jako post publiczny, tak więc każdy użytkownik serwisu Facebook miał do niego dostęp.

Prezes UODO uznał tym samym, że jego publikacji nie można zakwalifikować jako czynności o „czysto osobistym lub domowym charakterze” i dodał, że jest to szczególnie istotne w kontekście funkcjonalności, jaką oferuje Facebook w postaci możliwości ograniczenia grona odbiorców publikowanego postu, z której skarżony jednak nie skorzystał.

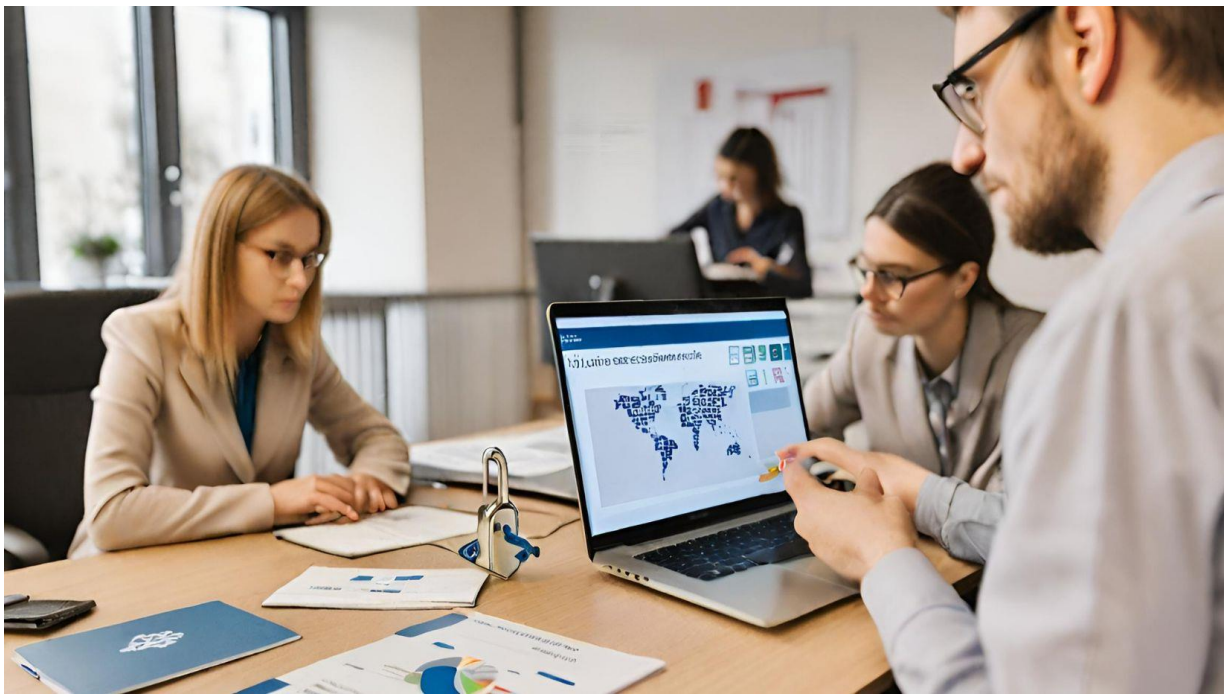
Czy publikacja postu była zgodna z przepisami rozporządzenia?
Stwierdzając, że badana sprawa wchodzi w zakres zastosowania rozporządzenia 2016/679 organ przystąpił do ustalenia, czy w sprawie zostały spełnione zasady oraz przesłanki legalności przetwarzania danych osobowych, o których mowa odpowiednio w art. 5 i 6 rozporządzenia. Skarżony w toku złożonych wyjaśnień nie wskazał, na jakiej podstawie przetwarzał dane osobowe skarżącej i małoletniej osoby. Prezes UODO również nie ustalił, aby skarżący legitymował się którąkolwiek z przesłanek, o których mowa w art. 6 rozporządzenia i która pozwalałaby na taką publikację. Odnosząc się natomiast do zasad przetwarzania danych osobowych zwrócił szczególną uwagę na zasadę minimalizacji danych (art. 5 ust. 1 list c RODO) oraz na korespondujący z nią motyw 39 preambuły, zgodnie z którym dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. A sposób w niniejszej sprawie z pewnością istniał, chociażby w postaci anonimizacji danych zamieszczonych w odpisie postanowienia. Z jednej strony skarżony umożliwiłby innym osobom zapoznanie się z okolicznościami toczącego się postępowania, z drugiej zaś prywatność skarżącej i małoletniej osoby zostałaby zachowana.

Korzystanie z portali społecznościowych może wiązać się z przetwarzaniem danych osobowych
Podsumowując swoje rozważania organ stwierdził, że skarżony poprzez publikację wpisu na swoim profilu społecznościowym, przetwarzał dane osobowe skarżącej i osoby małoletniej bez podstawy prawnej i korzystając z przysługujących mu na gruncie rozporządzenia uprawnień, udzielił mu w tej sprawie upomnienia. Prezes UODO w swojej decyzji przypomniał tym samym, że w określonych okolicznościach korzystanie z portali społecznościowych i przypisanych im prywatnych profili może się wiązać z przetwarzaniem danych osobowych w rozumieniu rozporządzenia 2016/679 i musi spełniać określone w nim przepisy.

4 NARUSZENIA I KONTROLE

EROD PRZYGOTOWAŁA PRZEWODNIK OCHRONY DANYCH DLA MAŁYCH FIRM

O szkodliwym wpływie naruszeń danych osobowych na funkcjonowanie organizacji najlepiej wiedzą te przedsiębiorstwa, które w skutek incydentów bezpieczeństwa poniosły straty finansowe bądź zostały dotknięte karami czy spadkiem zaufania klientów. Europejska Rada Ochrony Danych przygotowała Przewodnik ochrony danych dla małych przedsiębiorców, który ma pomóc małym i średnim biznesom reagować na naruszenia ochrony danych i wskazać im, kiedy należy powiadamiać o nich organy nadzorcze.



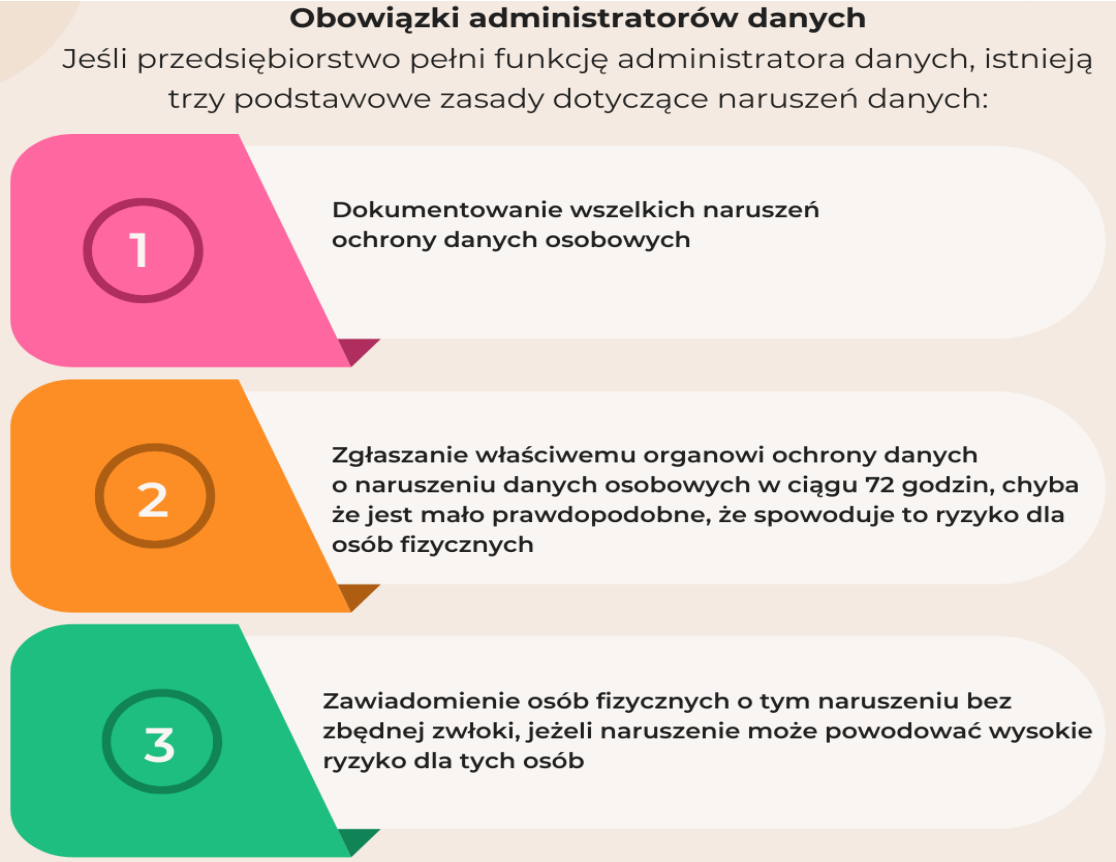
Co to jest „naruszenie ochrony danych osobowych”

Naruszenie ochrony danych osobowych oznacza „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych”.

Organizacje powinny mieć świadomość, że naruszenie ochrony danych osobowych może obejmować nie tylko „utratę” danych osobowych, ale również zdarzenia mające wpływ na poufność, integralność lub dostępność danych osobowych. Co ważne, do naruszeń danych osobowych zaliczają się zdarzenia związane z bezpieczeństwem, które są następstwem zarówno wypadków (takich jak wysłanie wiadomości e-mail do niewłaściwego odbiorcy, zgubienie klucza USB zawierającego dane klienta czy przypadkowe usunięcie danych medycznych, dla których nie ma kopii zapasowej), jak i działania celowe (takie jak ataki phishingowe mające na celu uzyskanie dostępu do danych klientów).

Innymi słowy, obejmuje to sytuacje, w których ktoś uzyskuje dostęp do danych osobowych, przekazuje je bez odpowiedniego upoważnienia lub gdy dane osobowe stają się niedostępne w wyniku szyfrowania przez oprogramowanie ransomware. Naruszeniem jest też sytuacja, w wyniku której dochodzi do przypadkowej utraty lub zniszczenia danych. Chociaż wszystkie naruszenia ochrony danych osobowych są incydentami związanymi z bezpieczeństwem, nie wszystkie zdarzenia dotyczące bezpieczeństwa są naruszeniami ochrony danych osobowych (ponieważ dane zdarzenie może nie dotyczyć żadnych danych osobowych).

4 NARUSZENIA I KONTROLE



Administratorzy danych muszą rozumieć i przestrzegać powyższych obowiązków oraz z wyprzedzeniem wdrożyć właściwe procedury, które pozwolą im w odpowiednim czasie zareagować adekwatnie do sytuacji.
W przypadku wszystkich naruszeń – nawet tych, które nie zostały zgłoszone organowi ochrony danych na podstawie oceny, że jest mało prawdopodobne, aby powodowały ryzyko dla osób, których dane dotyczą – administrator danych musi zarejestrować przynajmniej podstawowe szczegóły naruszenia, jego ocenę, skutki i podjęte działania zaradcze, zgodnie z wymogami art. 33 ust. 5 RODO.

Co robić i jakie podjąć działania?
Zgodnie z art. 33 ust. 1 RODO, wszelkie naruszenia ochrony danych, z wyjątkiem tych, które nie stwarzają żadnego ryzyka dla osób fizycznych, należy zgłaszać właściwemu organowi ochrony danych. Organy ochrony danych wdrożyły procedury lub formularze internetowe, które poprowadzą administratora krok po kroku, aby mieć pewność, że podał wszystkie wymagane informacje.
Jeżeli naruszenie ma miejsce w kontekście przetwarzania transgranicznego i wymagane jest zgłoszenie, administrator danych, jeśli ma siedzibę w Europejskim Obszarze Gospodarczym (EOG), musi powiadomić wiodący organ ochrony danych. Administrator danych opracowując plan reagowania na naruszenia, powinien dokonać oceny, który organ ochrony danych jest tym wiodącym. Jeżeli ma jakiekolwiek wątpliwości w identyfikacji wiodącego organu ochrony danych, powinien co najmniej powiadomić lokalny, dla miejsca naruszenia, organ ochrony danych.

4 NARUSZENIA I KONTROLE

Gdy wymagane jest zgłoszenie, należy go dokonać tak szybko, jak to możliwe, nie później niż w ciągu 72 godzin od uzyskania informacji o naruszeniu. Jeżeli nie będzie to możliwe, wymagane jest uzasadnienie opóźnienia oraz dokonanie zgłoszenia w kilku etapach. Po obowiązkowym wstępnym zgłoszeniu, dalsze informacje można przekazywać w kolejnych krokach. Należy uznać, że organizacja ma świadomość wystąpienia naruszenia danych, jeżeli zaistniał uzasadniony stopień pewności, że doszło do incydentu bezpieczeństwa.

Zaleca się, aby wszystkie organizacje, w ramach swoich wewnętrznych procedur dotyczących naruszeń ochrony danych, posiadały system rejestrowania, w jaki sposób i kiedy dowiedziały się o naruszeniu ochrony danych osobowych oraz oceny jego potencjalnego ryzyka. Dzięki sprawnie działającym procedurom, będą mogły przedstawić właściwemu organowi ochrony danych szczegóły wystąpienia incydentu bezpieczeństwa.

Podobnie, zgodnie z art. 33 ust. 2 RODO, jeżeli mały bądź średni przedsiębiorca (MŚP) jest podmiotem przetwarzającym dane osobowe w imieniu innej organizacji, ma on obowiązek bez zbędnej zwłoki zgłosić administratorowi danych każde naruszenie ochrony danych osobowych. Ma to kluczowe znaczenie dla umożliwienia administratorowi danych wywiązanie się z obowiązków informacyjnych w odpowiednim czasie. Wymogi dotyczące zgłaszania naruszeń powinny być również szczegółowo określone w umowie pomiędzy administratorem danych a podmiotem przetwarzającym, zgodnie z wymogami art. 28 RODO.

ZGŁOSZENIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH WŁAŚCIWEMU ORGANOWI OCHRONY DANYCH MUSI ZAWIERAĆ CO NAJMNIEJ:

1. opis charakteru naruszenia danych osobowych, w tym, jeśli to możliwe, kategorie i przybliżoną liczbę osób, których to dotyczy, oraz kategorie i przybliżoną liczbę danych osobowych, których to dotyczy
2. imię i nazwisko oraz dane kontaktowe inspektora ochrony danych (IOD) lub innego punktu kontaktowego, w którym można uzyskać więcej informacji
3. opis prawdopodobnych konsekwencji naruszenia ochrony danych osobowych
4. opis środków podjętych lub proponowanych przez MŚP w celu zaradzenia naruszeniu ochrony danych osobowych, w tym, w stosownych przypadkach, środki mające na celu złagodzenie jego ewentualnych negatywnych skutków

4 NARUSZENIA I KONTROLE

Zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych
Ponadto o niektórych naruszeniach ochrony danych należy bez zbędnej zwłoki zawiadomić osoby fizyczne, których dane dotyczą. Celem tego wymogu jest zapewnienie osobom dotkniętym naruszeniem możliwości podjęcia niezbędnych środków ostrożności w przypadku wystąpienia zdarzeń, które mogą powodować wysokie ryzyko naruszenia ich praw i wolności.
Taka komunikacja z osobami fizycznymi musi odbywać się bezzwłocznie, by zminimalizować bezpośrednie ryzyka dla dotkniętych naruszeniem osób, a w stosownych przypadkach, w ścisłej współpracy z właściwym organem ochrony danych.
Istnieją okoliczności, w których administratorzy danych nie będą zobowiązani do powiadamiania osób fizycznych, np., gdy:

- administrator danych zaszyfrował dane, a klucze szyfrujące nie zostały naruszone;
- administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
- wymagałoby to niewspółmiernie dużego wysiłku; w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

ZAWIADOMIENIE SKIEROWANE DO DANEJ OSOBY POWINNO JASNYM I PROSTYM JĘZYKIEM OPISYWAĆ CHARAKTER NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORAZ ZAWIERAĆ CO NAJMNIEJ NASTĘPUJĄCE INFORMACJE:

- imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, od którego można uzyskać więcej informacji
- opis możliwych konsekwencji naruszenia ochrony danych osobowych
- opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków
- zalecenia dla osoby fizycznej co do minimalizacji potencjalnych niekorzystnych skutków

Przewodnik ochrony danych dla małych firm, wydany przez EROD, zachęca administratorów danych i podmioty przetwarzające do planowania z wyprzedzeniem i wdrażania procesów umożliwiających wykrycie i szybkie powstrzymanie naruszenia, ocenę ryzyka dla osób fizycznych, a następnie ustalenie, czy konieczne jest zgłaszanie go właściwemu organowi ochrony danych i zawiadomienie osób fizycznych o naruszeniu.

5 KARY

ADMINISTRATOR MOŻE ODSTĄPIĆ OD OBOWIĄZKU ZGŁOSZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH, TYLKO GDY WYSTĄPIENIE RYZYKA NARUSZENIA PRAW LUB WOLNOŚCI OSÓB FIZYCZNYCH JEST MAŁO PRAWDOPODOBNE

Prezes Urzędu Ochrony Danych Osobowych nałożył na Link4 Towarzystwo Ubezpieczeń S.A. z siedzibą w Warszawie, administracyjną karę pieniężną w wysokości 103 752 zł. Powodem nałożenia kary jest niezgłoszenie Prezesowi UODO naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.

Do Urzędu Ochrony Danych Osobowych wpłynęła informacja, że osoba trzecia, jako nieuprawniony odbiorca, otrzymała w formie załącznika do wiadomości e-mail dokument potwierdzający przyznanie odszkodowania. W nadanej przez Link4 Towarzystwo Ubezpieczeń S.A. wiadomości znalazły się takie dane jak imię, nazwisko, adres do korespondencji, dane wskazujące markę, model, numer rejestracyjny samochodu, a także numer polisy, numer szkody, jej wartość oraz kwota uznanego roszczenia. O otrzymaniu wiadomości z cudzymi danymi osoba trzecia poinformowała również firmę ubezpieczeniową, na co nie otrzymała jednak żadnej odpowiedzi zwrotnej.
Biorąc pod uwagę brak widocznej reakcji po stronie administratora organ nadzorczy, korzystając z uprawnień jakie daje mu art. 58 ust. 1 lit. a) i e) RODO, zwrócił się do niego z pytaniem m.in., czy wiedział o błędnej wysyłce wiadomości e-mail oraz czy dokonał stosownej analizy zdarzenia pod kątem ryzyka naruszenia praw lub wolności osób fizycznych, niezbędnej do oceny czy doszło do naruszenia ochrony danych skutkującego koniecznością zawiadomienia Prezesa UODO oraz osób, których dotyczy naruszenie.

Administrator wiedział o zdarzeniu i przeprowadził analizę ryzyka
W odpowiedzi administrator wskazał, że wiedział o zdarzeniu i wyjaśnił, że wiadomość została wysłana do nieuprawnionego adresata oraz likwidatora szkody. Przyznał też, że wiadomość została błędnie zaadresowana „w wyniku błędu ludzkiego". Ubezpieczyciel poinformował również, że dokonał stosownej analizy ryzyka w oparciu o „rekomendowaną na stronie UODO metodologię ENISA" oraz udostępniony na stronie internetowej jednej z firm oferującej usługi z zakresu ochrony danych osobowych i bezpieczeństwa informacji darmowy kalkulator do oceny wagi naruszenia. W oparciu o wymienione narzędzia uzyskał wynik wskazujący na niskie ryzyko dla praw i wolności osoby, której dane dotyczą. Wyniki analizy zostały przekazane do dalszej weryfikacji w zespole Inspektora Ochrony Danych LINK4. Jej efektem było uznanie niskiego ryzyka dla praw i wolności osoby, której dane dotyczą i poprzestanie na odnotowaniu incydentu w wewnętrznym rejestrze administratora.
Ze względu na brak zgłoszenia naruszenia ochrony danych osobowych, organ nadzorczy wszczął z urzędu postępowanie administracyjne wobec spółki. Administrator podtrzymał określone we wcześniejszej korespondencji ustalenia. W oparciu o wskazany sposób szacowania ryzyka, spółka jako główne kryteria oceny przyjęła trzy elementy: kontekst przetwarzania danych, łatwość identyfikacji osoby, której dane dotyczą i okoliczności naruszenia mające dodatkowy wpływ na powagę/dotkliwość naruszenia.

W oparciu o wymienione kryteria spółka stwierdziła m.in., że udostępniony osobie trzeciej dokument nie zawierał żadnych danych szczególnej kategorii. Zdaniem Link4 były to dane zwykłe, w stosunkowo wąskim zakresie, których nie można również uznać za dane finansowe. Przyznanie bowiem odszkodowania we wskazanej wysokości nie pozwala na określenie stanu finansowego osoby, której dane dotyczą. Ryzyka związane z wystąpieniem strat w postaci zaciągnięcia kredytów lub zobowiązań cywilnoprawnych, posługiwania się danymi do celów przestępczych typu fałszerstwa lub wyłudzenia, czy wreszcie ryzyko związane z naruszeniem dobrego imienia, również są zdaniem administratora, przy tak wąskim zakresie i charakterze danych, wykluczone.
Spółka stwierdziła również, że dane osoby dotkniętej naruszeniem trafiły do wąskiego grona odbiorców, a okoliczności sprawy nie wskazują, aby mogły im przyświecać jakiekolwiek złe intencje związane z ich wykorzystaniem. Administrator przyjął również wysoką możliwość identyfikacji osoby, której dane dotyczą.
Podsumowując powyższe ustalenia i sumując wartości uzyskane z analizy wskazanych aspektów, administrator wprowadził wyniki do kalkulatora i uzyskał kwalifikację naruszenia jako związanego z niskim ryzykiem naruszenia praw lub wolności osoby fizycznej. Uzupełniając tak uzyskany wynik stwierdzeniem m.in., że nieprawidłowo wysłane dane nie zawierały numeru PESEL ani informacji o zadłużeniu, spółka poprzestała na odnotowaniu zdarzenia w wewnętrznym rejestrze incydentów.

Istnieją „przypadki pośrednie", a metod analizy ryzyka jest wiele

Badając prawidłowość przeprowadzonej analizy organ nadzorczy w pierwszej kolejności zauważył, że pomiędzy sytuacjami, w których istnieje małe prawdopodobieństwo by naruszenie ochrony danych osobowych skutkowało ryzykiem naruszeniem praw lub wolności osób fizycznych (co zwykle uzasadnia brak obowiązku informacyjnego z art. 33 ust. 1 RODO), a sytuacjami gdy ryzyko naruszenia praw lub wolności osób fizycznych jest wysokie pozostają przypadki „pośrednie", których nie można pominąć i przy których samo odnotowanie incydentu w ewidencji naruszeń jest zwykle niewystarczające.
Organ przypomniał również, że art. 33 ust. 1 nie zawiera zamkniętego katalogu przypadków, dla których konieczne jest zgłoszenie naruszenia. Takie podejście pozwala na zachowanie niezbędnej elastyczności przy rozbudowanym wachlarzu zdarzeń, w których okoliczności naruszenia i powiązane z nim ryzyka mogą być bardzo różne i o bardzo różnym poziomie „dotkliwości". Tego rodzaju elastyczność pozostawia również administratorom na swobodę w doborze odpowiednich metod analizy ryzyka, wśród których, jak podkreślił organ, metodologia ENISA jest jedną z wielu, a Prezes UODO nie narzuca stosowania żadnej z nich. Organ zwrócił również uwagę, że „szacowanie" przyjmowanych wartości przed ujęciem ich we wzorze, w ramach tej i podobnych praktyk, często bywa zbyt „optymistyczne".

Szczególne obowiązki ustawowe

Organ zwrócił również uwagę, że spółka jest podmiotem, na którym ciążą szczególne obowiązki nałożone na mocy art. 35 ust. 1 ustawy z 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej, zgodnie z którym zakład ubezpieczeń i osoby w nim zatrudnione, a także osoby i podmioty, za pomocą których zakład ubezpieczeń wykonuje czynności ubezpieczeniowe, są obowiązane do zachowania tajemnicy dotyczącej poszczególnych umów ubezpieczenia. Zdaniem organu, ujawnienie danych osoby fizycznej nieuprawnionemu odbiorcy wiąże się w przypadku spółki z niedopełnieniem tych dodatkowych obowiązków.

5 KARY

Naruszenie praw lub wolności osób fizycznych nie jest warunkiem koniecznym nałożenia kary
Organ przechodząc do meritum swych rozważań przypomniał, że zgodnie z ustalonym orzecznictwem sądów administracyjnych, zgłoszenie przez administratora naruszenia ochrony danych osobowych, nie może być uzależnione od zaistnienia naruszenia praw lub wolności osób fizycznych. Samo bowiem ryzyko zmaterializowania się takiego naruszenia uzasadnia zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu.

Ocena wagi i prawdopodobieństwa potencjalnych skutków naruszenia
Wyraźnego podkreślenia wymaga również, że przy dokonywaniu oceny pod kątem ryzyka naruszenia praw lub wolności osób fizycznych, od której uzależnione jest zgłoszenie naruszenia, należy łącznie uwzględnić czynnik prawdopodobieństwa i wagę potencjalnych negatywnych skutków. Wysoki poziom któregokolwiek z tych czynników ma wpływ na wysokość ogólnej oceny, od której uzależnione jest wypełnienie obowiązku określonego w art. 33 ust. 1 RODO. Przyjmując zatem, iż w badanej sprawie wystąpiła możliwość zmaterializowania się negatywnych konsekwencji dla osoby, której dane dotyczą, to wagę potencjalnego wpływu na prawa lub wolności osoby fizycznej należy uznać za większą niż niska.
Organ powołując się na Wytyczne EROD 9/2022 (zwłaszcza na Dział II dotyczący art. 33 RODO) wskazał również, że przypadek, gdy nie powstaje obowiązek zgłoszenia naruszenia ochrony danych organowi nadzorczemu ze względu na małe prawdopodobieństwo wystąpienia naruszenia praw lub wolności osób fizycznych należy rozumieć wąsko t.j. jako wyjątek, który znajdzie zastosowanie w sytuacjach, gdy to prawdopodobieństwo jest w sposób oczywisty małe.

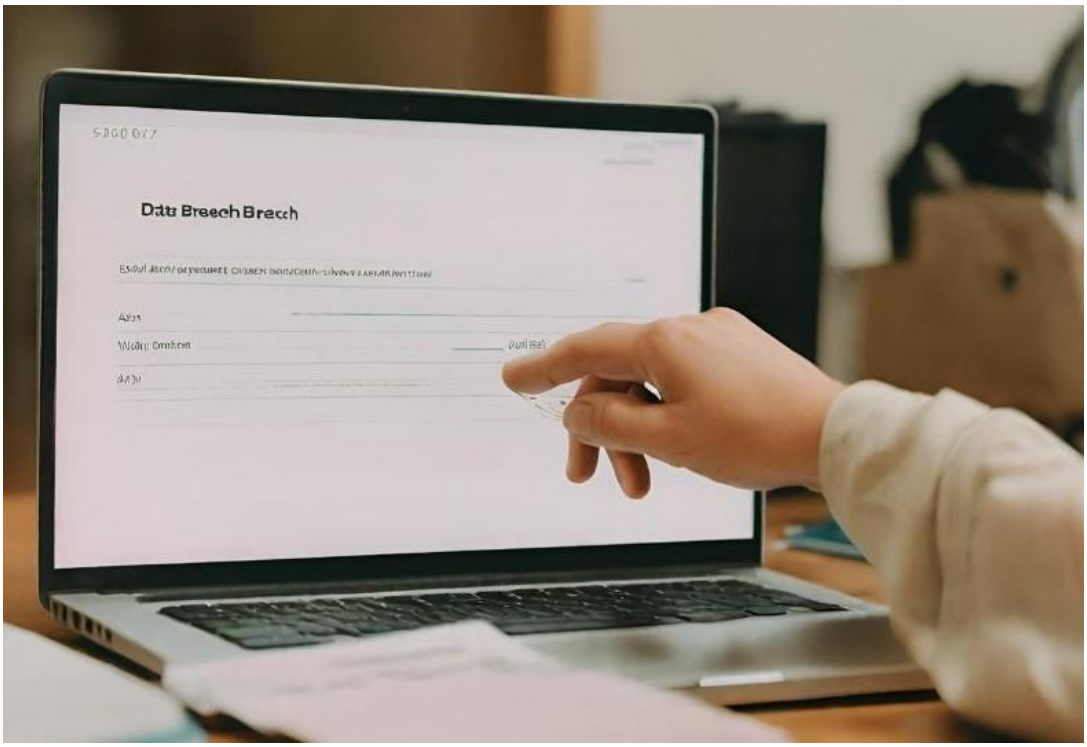
W sprawie wystąpiło ryzyko naruszenia praw lub wolności
Konkludując organ uznał, że w analizowanym przypadku wystąpiło ryzyko naruszenia praw lub wolności osoby, dotkniętej naruszeniem. Okoliczności sprawy nie pozwalają bowiem przyjąć, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osoby fizycznej. Tym samym po stronie spółki zaktualizował się obowiązek zgłoszenia naruszenia do Prezesa UODO, którego to obowiązku ostatecznie nie dopełniła.
Decydując się na zastosowanie środka w postaci administracyjnej kary pieniężnej, organ nadzorczy zwrócił uwagę na m. in. następujące okoliczności obciążające:

- długi czas trwania naruszenia, który wedle ustaleń organu trwał od ponad 17 miesięcy,
- niezgłoszenie naruszenia pomimo przekazania spółce informacji o „omyłkowej" wysyłce korespondencji, a potem również o wszczęciu postępowania administracyjnego,
- stwierdzenie naruszenia przepisów o ochronie danych osobowych w innym postępowaniu toczącym się wobec spółki,
- niezadowalający poziom współpracy z organem nadzorczym – ocena ta dotyczy reakcji spółki na pisma Prezesa UODO o obowiązkach ciążących na administratorze w związku z naruszeniem ochrony danych, a następnie wszczęcia postępowania administracyjnego w przedmiocie obowiązku zgłoszenia naruszenia ochrony danych.

5 KARY

Ocena pod kątem ochrony praw osoby fizycznej

Badając sprawę, organ kilkukrotnie podkreślał, że ocena ryzyka naruszenia praw lub wolności osoby fizycznej powinna być dokonywana przez pryzmat osoby, której dane dotyczą, a nie interesów administratora. Gruntownie przeprowadzona analiza zdarzenia, w tym uwzględnienie prawdopodobieństwa wystąpienia negatywnych skutków oraz ich doniosłości ma służyć przede wszystkim ochronie praw osób fizycznych, których dotknęło naruszenie i które ostatecznie będą zmuszone ponieść jego, niekiedy bardzo poważne, konsekwencje. Zgłoszenie naruszenia to również bardzo ważne narzędzie weryfikacji, pozwalające ustalić organowi nadzorczemu czy administrator zastosował właściwe środki w celu zaradzenia naruszeniu i zminimalizowania jego negatywnych skutków oraz czy zastosował odpowiednie środki w celu zminimalizowania ryzyka jego ponownego wystąpienia.



6 NOWE TECHNOLOGIE

AR – JAK BEZPIECZNIE KORZYSTAĆ Z ROZSZERZONEJ RZECZYWISTOŚCI?

W dzisiejszym świecie nowe technologie rozwijają się w zawrotnym tempie, zmieniając nasze życie i otaczającą nas rzeczywistość w sposób, który jeszcze kilka lat temu wydawał się możliwy tylko w filmach science fiction. Narzędzia nowych technologii pozwalają nam rozszerzyć zakres zdolności rozumienia świata zmysłami i doświadczyć go zupełnie na nowo, całkowicie odmieniając nasze interakcje z otoczeniem.

Jednym z najbardziej fascynujących aspektów tych przemian jest rozszerzona rzeczywistość (ang. Augmented Reality), która stanowi pomost między światem wirtualnym a rzeczywistością. Technologia otwiera przed nami nowe możliwości, ale również stwarza wyzwania w kontekście ochrony danych i prywatności.

Co to jest rozszerzona rzeczywistość (AR)?
Rozszerzona rzeczywistość (AR) to technologia, która umożliwia projektowanie wirtualnych obiektów i informacji na tle świata rzeczywistego. Za pomocą specjalnych urządzeń, takich jak okulary AR lub aplikacje na smartfony, użytkownicy mogą oglądać obiekty wirtualne, które nie istnieją w ich realnym otoczeniu.

Przykłady zastosowań AR są liczne. Gry wideo wykorzystują AR, aby przenieść graczy do wirtualnych światów w ich własnych pokojach, a także wnieść wrażenia jakich doświadczają na wyższy poziom. Technologia AR jest też wykorzystywana w marketingu rewolucjonizując sposób prezentacji produktów. Może też wspierać edukację umożliwiając tworzenie interaktywnych lekcji i prezentacji.

Zagrożenia AR dla ochrony danych osobowych
AR może gromadzić różnego rodzaju informacje o użytkowniku, takie jak lokalizacja, ruchy, gesty, a nawet jego wizerunek. To z kolei rodzi obawy dotyczące zachowania prywatności, zwłaszcza w przypadku nadużyć ze strony dostawców usług AR. Jednym z największych wyzwań jest realizacja całego szeregu obowiązków wynikających z rozporządzenia RODO, w tym między innymi wykazanie podstawy dla przetwarzania danych, o której mowa w art. 6 RODO, realizacja obowiązków informacyjnych zgodnie z art. 13 i 14 RODO, a także prowadzenie rejestru czynności przetwarzania (art. 30 RODO) czy zapewnienie odpowiednich środków technicznych i organizacyjnych, o których mowa w art. 24 RODO.
Należy mieć na uwadze, że jednym z kluczowych elementów, który umożliwia urządzeniom AR dostarczenie użytkownikom wzbogacanych doświadczeń w oparciu o ich aktualną lokalizację jest tzw. geolokalizacja, która odnosi się do zdolności urządzeń AR do określania i monitorowania fizycznego położenia użytkownika w rzeczywistości. Dzięki informacjom o lokalizacji, urządzenia te mogą umieszczać wirtualne obiekty, takie jak znaczniki, modele 3D lub informacje, tak aby były widoczne, za pośrednictwem urządzenia AR, w konkretnych miejscach w rzeczywistym środowisku użytkownika

6 NOWE TECHNOLOGIE

Na przykład, użytkownik wskazując smartfonem na budynki w okolicy może zobaczyć informacje o nich na ekranie. W związku z coraz większą popularnością aplikacji mobilnych wykorzystujących technologię geolokalizacji Urząd Ochrony Danych Osobowych wielokrotnie zachęcał do ostrożnego i bezpiecznego korzystania z urządzeń mobilnych.

Jak bezpiecznie korzystać z rozszerzonej rzeczywistości (AR)?

Aby bezpiecznie korzystać z technologii AR i chronić swoje dane osobowe, warto przestrzegać kilku zasad:

1. **Wybór urządzenia AR**. Przed zakupem urządzenia AR zorientuj się, kim jest producent i dostawca. Wybieraj renomowane firmy, które stosują środki bezpieczeństwa i posiadają dobre opinie.
2. **Regulamin i polityka prywatności**. Przede wszystkim zapoznaj się z polityką prywatności aplikacji oraz udostępnionymi przez nią regulaminami, z których dowiesz się, do jakich danych będzie miała dostęp konkretna aplikacja i w jakim celu będzie je wykorzystywać. W tym zakresie szczególną uwagę zwróć na postanowienia dotyczące przekazywania za pośrednictwem aplikacji danych osobowych do państw trzecich. Dlatego zanim udzielisz dostępu do swoich danych osobowych, zastanów się, czy jest to absolutnie konieczne. Zauważ, że w przypadku danych dotyczących dzieci przetwarzanie danych powinno być ograniczone do tego, co jest absolutnie niezbędne.
3. **Zgoda i Transparentność**. Upewnij się, że masz pełną świadomość, do czego służą twoje dane i na co wyraziłeś zgodę. Firmy stosujące AR powinny dostarczać jasnych i zrozumiałych informacji.
4. **Aktualizuj Oprogramowanie**. Regularnie aktualizuj oprogramowanie swojego urządzenia AR lub urządzenia za pomocą którego korzystasz z oprogramowania AR. Umożliwi to stosowanie wszystkich najnowszych funkcji i poprawek.
5. **Szyfrowanie i Bezpieczne Hasła**. Używaj silnych i unikalnych haseł do zabezpieczenia swojego urządzenia AR. Włącz także funkcje szyfrowania danych, jeśli to możliwe.
6. **Ochrona Lokalizacji**. Jeśli urządzenie AR korzysta z informacji o twojej lokalizacji, kontroluj, które aplikacje mają do niej dostęp i używaj trybu „tylko w trakcie działania aplikacji" lub wyłączaj lokalizację, gdy nie jest potrzebna.
7. **Edukacja i Świadomość**. Pogłębiaj swoją wiedzę na temat technologii AR, aby zrozumieć jej potencjalne zagrożenia.
8. **Zgłaszanie Incydentów Bezpieczeństwa**. Jeśli podejrzewasz naruszenie bezpieczeństwa swoich danych w związku z urządzeniem AR, natychmiast zgłoś ten incydent dostawcy usługi oraz odpowiednim organom.

6 NOWE TECHNOLOGIE

Rozszerzona rzeczywistość to niezwykle interesująca technologia z ogromnym potencjałem, której tempo rozwoju jest bardzo duże. Zachowanie prywatności i ochrona danych osobowych pozostają priorytetami, które należy uwzględnić w dynamicznie rozwijającym się świecie technologii również w odniesieniu do AR. Tylko świadomi i odpowiedzialni użytkownicy tej technologii mogą cieszyć się jej możliwościami, zachowując pełną kontrolę nad swoimi danymi osobowymi.

7 SPRAWY MIĘDZYNARODOWE

REKRUTACJA UCZESTNIKÓW DO SZÓSTEJ EDYCJI KONKURSU IM. STEFANO RODOTY

Komitet Konsultacyjny ds. Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych (Komitet T-PD) zaprasza do składania wniosków o przyznanie Nagrody im. Stefano Rodoty w 2024 r. w ramach szóstej edycji konkursu.

Nagroda przyznawana jest na cześć i ku pamięci czołowego włoskiego profesora prawa i polityka, Stefano Rodoty, który przez całe życie pracował na rzecz promowania praw podstawowych, w szczególności na rzecz rozwoju i wdrażania prawa do ochrony danych w Europie. Tym samym pozostawił niezatarty ślad w kształtowaniu polityki europejskiej w tej dziedzinie. Nagroda honoruje innowacyjne i oryginalne akademickie projekty badawcze w dziedzinie ochrony danych.

Konkurs jest otwarty dla studentów i naukowców z krajów będących członkami lub obserwatorami Komitetu T-PD. Jury nagrody Stefano Rodoty składa się z członków Biura Komitetu.

Każdego roku wyróżnione projekty są ogłaszane 28 stycznia w Dniu Ochrony Danych Osobowych. Zwycięzca dostaje możliwość zaprezentowania swojej pracy na kolejnej sesji plenarnej Komitetu T-PD – na globalnym forum renomowanych międzynarodowych ekspertów w dziedzinie ochrony danych osobowych i decydentów z około 90 krajów. Jest to wyjątkowa okazja, by mieć swój wkład w kształtowanie polityki ochrony danych.

UODO jako członek Komitetu T-PD, z ramienia Rzeczypospolitej Polskiej, zachęca do wysłania formularza zgłoszeniowego **do 30 listopada 2023 r.**
Wszystkie niezbędne informacje oraz formularz zgłoszeniowy dostępne są na stronie:
2024 Rodotà Award.

7 SPRAWY MIĘDZYNARODOWE

FRANCJA: KARA ZA NADMIERNE GROMADZENIE DANYCH I BRAK WSPÓŁPRACY

Francuski organ ochrony danych CNIL (Commission Nationale de l'Informatique et des Libertés) 18 września 2023 r. nałożył na SAF LOGISTICS administracyjną karę pieniężną w wysokości 200 000 euro za gromadzenie zbyt dużej ilości danych swoich pracowników, naruszanie ich prywatności i brak wystarczającej współpracy z organem.

SAF LOGISTICS to spółka zajmująca się transportem lotniczym, której jednostka macierzysta ma siedzibę w Chinach. Pracownik firmy zgłosił do CNIL, że w ramach wewnętrznego procesu rekrutacji na stanowisko w spółce macierzystej, zbierała ona dane dotyczące życia prywatnego zatrudnionych w organizacji osób.

Podczas postępowania kontrolnego CNIL stwierdził kilka naruszeń, w szczególności nadmierne gromadzenie danych, nieprzestrzeganie zakazu przetwarzania danych szczególnie chronionych i danych dotyczących przestępstw, jak również brak współpracy z organem. W rezultacie CNIL nałożył na spółkę karę w wysokości 200 000 euro.

Główne naruszenia objęte sankcjami

Określając wysokość kary, CNIL wziął pod uwagę fakt, że kilka ze stwierdzonych naruszeń dotyczyło kluczowych zasad RODO:

- naruszenie zasady minimalizacji danych (art. 5 ust.1 lit. c RODO) – bowiem za pomocą formularza wysłanego do swoich pracowników spółka zbierała informacje o członkach ich rodzin, takich jak ich tożsamość, dane kontaktowe, stan cywilny, informacje o pracodawcach i zajmowanych stanowiskach;

- naruszenie zakazu przetwarzania danych szczególnie chronionych (art. 9 RODO – część informacji, które należało wprowadzić do formularza, stanowiło dane wrażliwe, takie jak grupa krwi, pochodzenie etniczne i przynależność polityczna. CNIL stwierdził, że spółka nie spełniła żadnego z warunków określonych w RODO (art. 9 ust. 2) dotyczących zbierania tego typu danych;

- naruszenie zakazu przetwarzania danych dotyczących przestępstw, wyroków skazujących i środków bezpieczeństwa (art. 10 RODO) – spółka przechowywała wyciągi m.in. z rejestrów karnych pracowników zatrudnionych w transporcie lotniczym, mimo że zostali oni już oczyszczeni z zarzutów przez właściwe organy;

- niedopełnienie obowiązku współpracy z organem nadzorczym (art. 31 RODO) – po tym jak CNIL zwrócił się do spółki o przetłumaczenie formularza, który był napisany w języku chińskim, przedstawiła ona niekompletne tłumaczenie, w którym brakowało pól dotyczących pochodzenia etnicznego lub przynależności politycznej. Organ nadzorczy musiał zatem sam przetłumaczyć formularz, aby uzyskać dostęp do wszystkich pól formularza. Tym samym uznał, że SAF LOGISTICS celowo dążył do uniemożliwienia mu wykonywania jego uprawnień nadzorczych.

Źródło: komunikat organu nadzorczego

7 SPRAWY MIĘDZYNARODOWE

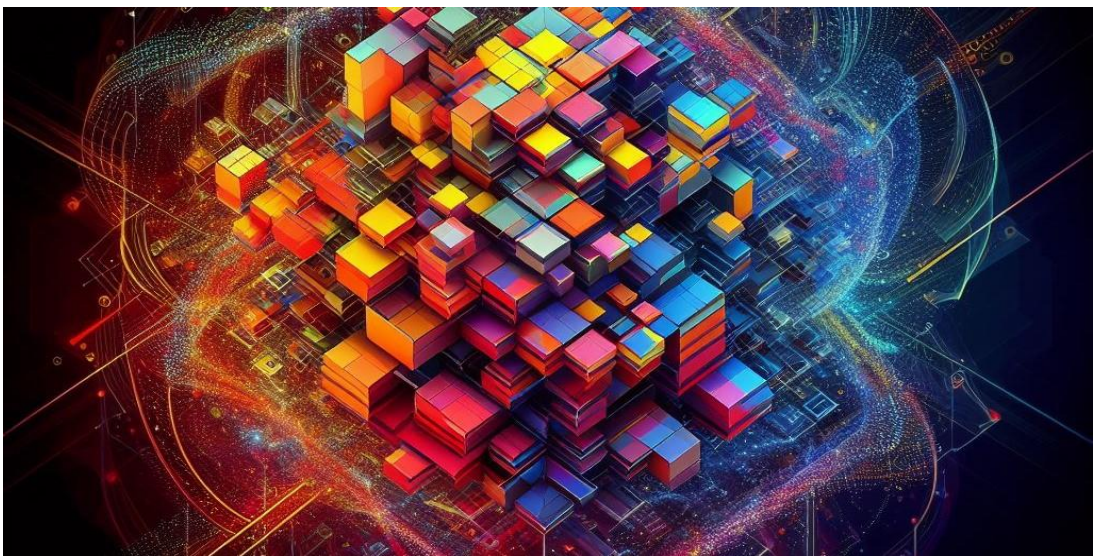
NIDERLANDY: ALGORYTMY MUSZĄ BYĆ POD KONTROLĄ

Raport „Algoritmic Risks Report Netherlands", wydany przez organ nadzorczy ds. ochrony danych Królestwa Niderlandów Autoriteit Persoonsgegevens (AP), wzywa do podjęcia dodatkowych działań w celu kontrolowania ryzyka algorytmicznego i sztucznej inteligencji. Podkreśla, że innowacje takie jak inteligentne chatboty oraz problem niewystarczającego zrozumienia przez organizacje istniejących algorytmów, stanowią obecnie najbardziej znaczące zagrożenia algorytmiczne w Królestwie Niderlandów.

Niderlandzki organ nadzorczy utworzył rejestr algorytmów dla organizacji rządowych, by móc lepiej kontrolować algorytmy i sztuczną inteligencję oraz kompleksowo nadzorować sposób, w jaki są one wykorzystywane przez podmioty publiczne i organizacje prywatne. Zdaniem AP wymóg rejestracji powinien być ustanowiony w sposób proporcjonalny, tak aby skupić się na skutecznej identyfikacji algorytmów wysokiego ryzyka i zarządzaniu nimi. Ponadto niderlandzki regulator, świadomy potencjalnych korzyści z eksperymentowania i odkrywania możliwych innowacji i wzrostu wydajności, przestrzegł przed wdrażaniem najnowszych innowacji sztucznej inteligencji w niekontrolowany sposób. Możliwe przypadki użycia algorytmów objęły oceny pracowników, wykrywanie oszustw, oceny klientów pod kątem zakupów lub pożyczek oraz oceny pacjentów.

Bezpieczne wdrożenie algorytmów bez ryzyka naruszenia podstawowych praw i wartości jest możliwe tylko wtedy, gdy to ryzyko jest odpowiednio zarządzane, a więc organizacje przed zastosowaniem algorytmów, muszą je ocenić na równi z korzyściami.

Raport opublikowany przez niderlandzki organ nadzorczy to pierwszy kompleksowy i okresowy przegląd rozwoju, zagrożeń i wyzwań związanych z wykorzystaniem algorytmów i sztucznej inteligencji. Jego celem jest stworzenie nadrzędnej perspektywy ryzyka, która może zostać uwzględniona w inicjatywach politycznych, wymogach dotyczących danych i sprawozdawczości, strategiach i ocenach ryzyka poszczególnych (sektorowych) organów nadzorczych i ich agendzie pracy oraz funkcji zarządzania ryzykiem w poszczególnych organizacjach.



Źródło: komunikat organu nadzorczego

7 SPRAWY MIĘDZYNARODOWE

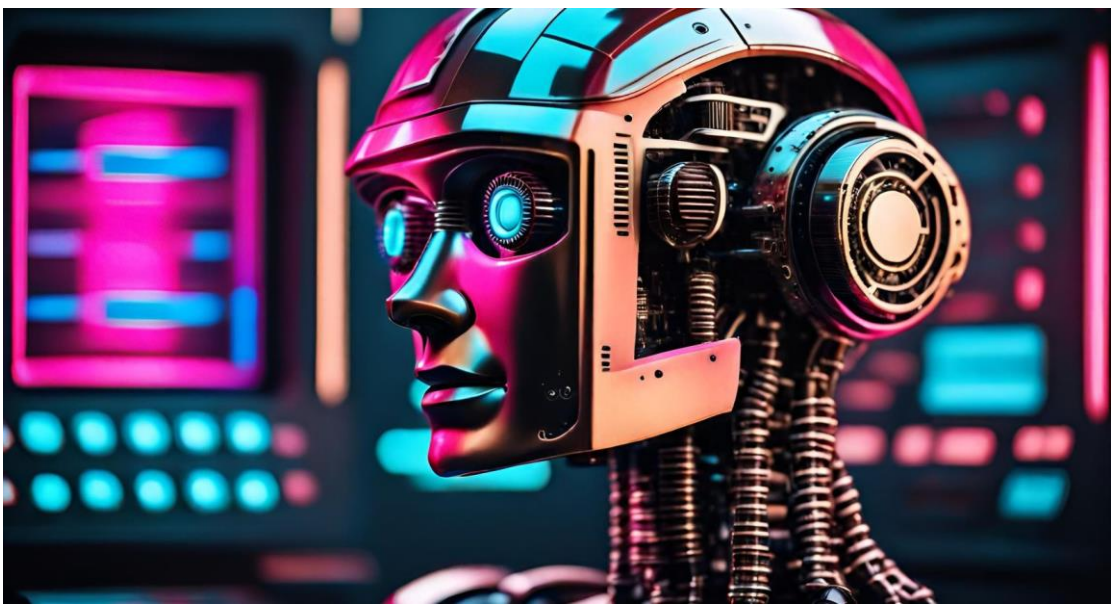
HISZPAŃSKI ORGAN NADZORCZY WYDAŁ WYTYCZNE ODNOŚNIE DO PRZEJRZYSTOŚCI W ŚWIETLE PROJEKTU AKTU WS. SZTUCZNEJ INTELIGENCJI I RODO

Hiszpański organ nadzorczy Agencia Española de Protección de Datos (AEPD) w swojej publikacji zaakcentował różnice ujęcia transparentności w projekcie rozporządzenia o AI i w RODO.

Koncepcja przejrzystości w projekcie aktu ws. sztucznej inteligencji różni się od tego samego terminu określonego w RODO, którego zakres przedmiotowy nie dotyczy systemów, ale przetwarzania danych osobowych. Oba pojęcia przejrzystości dotyczą różnych podmiotów i informacji przeznaczonych dla odrębnych odbiorców. Wytyczne AEPD wskazują, że transparentność w rozumieniu projektu aktu ws. sztucznej inteligencji to informacje, które trafiają głównie od dostawców systemów sztucznej inteligencji do użytkowników/podmiotów wdrażających system sztucznej inteligencji. Administratorzy powinni uzyskać wystarczającą ilość informacji na temat systemów sztucznej inteligencji, aby wypełnić swoje obowiązki na gruncie RODO.

Kluczowe wytyczne dla organizacji z UE i USA tłumaczą, że systemy sztucznej inteligencji muszą być zaprojektowane w sposób umożliwiający przejrzystość i audyt w celu ułatwienia przestrzegania zobowiązań prawnych wynikających zarówno z przepisów o ochronie danych, jak i innych przepisów (dotyczących zakazu dyskryminacji). Ponadto, co podkreśla AEPD, twórcy systemów sztucznej inteligencji muszą dostarczyć klientom, wdrażającym te systemy, wystarczających informacji na ich temat, aby spełnić obowiązki w zakresie zgodności z RODO. Co ważne, na twórców systemów sztucznej inteligencji mogą być nałożone obowiązki wynikające zarówno z aktu ws. sztucznej inteligencji, jak i z RODO, jeśli:

1. wykorzystują dane osobowe przy projektowaniu lub opracowywaniu systemu sztucznej inteligencji lub
2. przechowują czy przetwarzają dane zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych.



Źródło: komunikat organu nadzorczego

ZAKAZ MONITOROWANIA LOKALIZACJI PRACOWNIKÓW W AUSTRII

Austriacki organ nadzorczy Österreichische Datenschutzbehörde (DSB) dokonał kontroli w przedsiębiorstwie, które korzystało z urządzeń śledzących GPS w pojazdach służbowych używanych przez pracowników. Kontrolę zainicjowały anonimowe doniesienia dotyczące stosowania przez pracodawcę monitoringu nie tylko w zakresie podróży służbowych, ale także prywatnych wyjazdów swoich pracowników, do których również byli upoważnieni przez firmę.

Po przeprowadzeniu postepowania austriacki organ nadzorczy ustalił, że przedsiębiorstwo posiadało 15 pojazdów w leasingu. W 2020 r. w samochodach tych zainstalowano urządzenia GPS. Początkowo urządzenia te używane były tylko – gdy wystąpiła taka potrzeba – do znajdowania lokalizacji samochodu. Jednak od lipca 2021 r. system rejestrował również godziny pracy pracowników podczas podróży służbowych i pomagał w obliczaniu kosztów z nią związanych. System aktywował się po uruchomieniu silnika i dezaktywował po jego wyłączeniu, kierowcy mogli go również wyłączyć ręcznie. Zebrane dane pokazywały szczegóły, takie jak: przebyta odległość, data, godzina, punkt początkowy i końcowy oraz rzeczywista trasa pojazdu. Dostęp do tych danych miała tylko wybrana grupa pracowników i spółka instalująca urządzenia. Śledzenie to było, zgodnie z informacjami przekazanymi organowi nadzorczemu, wykorzystywane do tworzenia profili pracowników.

Przedsiębiorstwo powoływało się na dwie podstawy prawne monitoringu zgodnie z RODO – na obowiązek prawny i prawnie uzasadniony interes. Jednak organ nadzorczy nie podzielił argumentów administratora. Uznał, że przedsiębiorstwo może uzyskać informacje nt. lokalizacji pracowników za pomocą innych metod i nie potrzebuje stosować urządzeń GPS do monitorowania ich podróży. DSB zauważył, że brakuje podstaw do używania GPS do rejestrowania godzin pracy lub kosztów podróży. Spółka nie była w stanie udowodnić, że GPS był niezbędny do zapobiegania kradzieżom lub uszkodzeniom wynajmowanych samochodów.

Jeśli chodzi o obowiązek prawny, przedsiębiorstwo stwierdziło, że prawo austriackie wymaga dokładnej ewidencji godzin pracy i uważa, że GPS może w tym pomóc. Jednak organ nadzorczy zauważył, że spółka ręcznie rejestrowała godziny pracy przed lipcem 2021 r. bez żadnych problemów. Podsumowując, austriacki organ nadzorczy orzekł, że spółka naruszyła przepisy RODO, stosując śledzenie GPS bez podstawy prawnej i nakazał natychmiastowe zaprzestanie korzystania z niego.

Źródło: komunikat organu nadzorczego

7 SPRAWY MIĘDZYNARODOWE

45. MIĘDZYNARODOWA KONFERENCJA GLOBAL PRIVACY ASSEMBLY 2023

Global Privacy Assembly (GPA) to forum zrzeszające ponad 130 organów regulacyjnych ds. ochrony danych i prywatności na całym świecie. W dniach 15-20 października odbyła się 45. Konferencja GPA, której gospodarzem był komisarz ds. prywatności na Bermudach (PrivCom).

Konferencja poświęcona kwestiom dotyczącym sztucznej inteligencji składała się z sesji zamkniętej i otwartej. Podczas gdy w sesji zamkniętej wzięli udział tylko akredytowani członkowie GPA i obserwatorzy, w sesji otwartej uczestniczyła szersza publiczność, w tym eksperci zajmujący się ochroną danych i prywatnością, przedsiębiorstwa, przedstawiciele społeczeństwa obywatelskiego, środowiska akademickie i reprezentanci rządu.

Oprócz przekrojowego motywu proaktywnej, interdyscyplinarnej i wielosektorowej współpracy, omówiono szeroki zakres tematów związanych z ochroną danych i prywatnością, w tym najnowsze osiągnięcia technologiczne i przyspieszone wykorzystanie szerokiej gamy narzędzi technologicznych. Dyskusje dotyczyły też sztucznej inteligencji (AI), programowania algorytmicznego, zautomatyzowanego podejmowania decyzji. Poruszono także tematy związane z blockchain, metaverse, analizą dużych zbiorów danych i transgranicznymi transferami danych.

Dyskusja nt. powyższych zagadnień unaoczniła pilną potrzebę stworzenia solidnych, dynamicznych ram regulacyjnych zgodnych z międzynarodowymi standardami najlepszych praktyk. Rozmowy te miały kluczowe znaczenie dla zrozumienia etycznego zarządzania danymi oraz ochrony i gwarancji praw człowieka.

Jak co roku, także podczas tegorocznej konferencji, przyznano nagrodę im. Giovanniego Buttarellego, która upamiętnia byłego Europejskiego Inspektora Ochrony Danych, gospodarza konferencji GPA 2018 i byłego członka Komitetu Wykonawczego GPA. Nagroda ta jest silnie powiązana z wizją GPA, polegającą na zapewnieniu wiodącej pozycji na szczeblu międzynarodowym i zachęcaniu do współpracy ponad granicami. Tegoroczną laureatką została Andrea Jellinek, która otrzymała nagrodę za swoją pracę jako przewodnicząca Europejskiej Rady Ochrony Danych i prezes austriackiego organu nadzorczego.

Źródło: komunikat organu nadzorczego

8 EDUKACJA

SZKOLENIA DLA UCZESTNIKÓW PROGRAMU „TWOJE DANE – TWOJA SPRAWA”

Urząd Ochrony Danych Osobowych zorganizował dwudniowe szkolenie dla nauczycieli i dyrektorów szkół w ramach programu „Twoje dane – Twoja sprawa”. Wydarzenie odbyło się w dniach 25-26 października 2023 r. i miało na celu dostarczenie wiedzy i narzędzi do skutecznego zarządzania cyberbezpieczeństwem w szkołach oraz wzmocnienie świadomości nauczycieli w zakresie ochrony danych osobowych i przygotowanie ich do wyzwań cyfrowej rzeczywistości.

Podczas szkolenia omówiono kwestie dotyczące ochrony danych osobowych w edukacji dzieci i młodzieży, zwracając uwagę na kluczowe aspekty współpracy dyrektorów szkół z Inspektorem Ochrony Danych Osobowych. Poza przekazaniem uczestnikom solidnej porcji wiedzy, przedstawiono również praktyczne aspekty szeroko pojętego cyberbezpieczeństwa. Dyskutowano między innymi na temat bezpieczeństwa uczniów w świecie cyfrowym, w tym zagrożeń związanych z uzależnieniem od nowych technologii czy korzystaniem z mediów społecznościowych, a także cyberprzemocą, hejtem, sextingiem, dezinformacją czy deepfake’ami. Poruszono temat ochrony prywatności w kontekście rozwoju nowych technologii, włącznie z wirtualną rzeczywistością i sztuczną inteligencją. Prelegenci podkreślali nie tylko zagrożenia związane z wykorzystywaniem przez dzieci nowych technologii, ale także korzyści oraz potrzeby jakie mogą one zaspokoić. Dopiero zestawienie tych argumentów daje pełny pogląd na skomplikowane zagadnienie rozwoju technologii cyfrowych.

Nauczyciele podzielili się swoimi pomysłami na to jak ująć tematykę ochrony danych osobowych w codziennych lekcjach. Wśród propozycji nie zabrakło ciekawych przykładów takich jak szkolne konkursy na komiks poświęcony tematyce bezpieczeństwa danych czy wizyt w domach pomocy społecznej. Pojawił się nawet kreatywny sposób na połączenie tego niełatwego tematu z elementami mitologii greckiej czy przypowieściami biblijnymi. Zaprezentowano też, stworzoną przez uczniów w ramach szkolnych obchodów Dnia Ochrony Danych Osobowych, grę podłogową sprawdzającą wiedzę z zakresu ochrony danych osobowych.

Szczególnie wartościowa była prezentacja Romana Sobotki z Departamentu Orzecznictwa i Legalizacji UODO, który omówił zasadę legalności przetwarzania danych, kładąc nacisk na współpracę z Inspektorem Ochrony Danych Osobowych i wagę niezależności tego stanowiska.
„W trosce o prywatność uczniów i pracowników szkół, kluczowe jest przestrzeganie zasady minimalizacji danych – przetwarzamy tylko te informacje, które są niezbędne do osiągnięcia określonego celu”. – podkreślał Roman Sobotka.

W szkoleniu wzięło udział 132 uczestników tegorocznej edycji programu „Twoje dane – Twoja sprawa”, spotkanie zakończyło się sesją pytań, na które odpowiedzi udzielali pracownicy infolinii UODO.
Działania w ramach programu realizowane są dwuetapowo. Najpierw szkoleni są dyrektorzy szkół i nauczyciele, następnie uczniowie. Każda edycja kończy się w czerwcu wręczeniem nagrody „Złotego Pióra” przez Prezesa Urzędu Ochrony Danych Osobowych.

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl