



NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

str. 2 **WYSTĄPIENIE PREZESA UODO**

str. 3 **POWIAT NIE POWINIEN ZAWIERAĆ UMOWY POWIERZENIA PRZETWARZANIA
DANYCH OSOBOWYCH Z PUP ANI PCPR**

str. 4 **KONTROLA WYKORZYSTANIA DOTACJI NA REALIZACJĘ ZADANIA PUBLICZNEGO**

str. 5 **KTO JEST ADMINISTRATOREM DANYCH PRZETWARZANYCH W ZWIĄZKU
Z MEDIACJĄ W POSTĘPOWANIU ADMINISTRACYJNYM**

str. 8 **MIĘDZYNARODOWE**

- Oświadczenie w sprawie cyfrowego śledzenia kontaktów
- Belgia: Ochrona danych osobowych nie przeszkadza w użyciu technologii przeciw COVID-19, o ile jest to zgodne z zasadami
- Norwegia: analiza dotycząca zamówienia aplikacji śledzącej infekcje Infect Stop

str. 10 **KARY**

- Szwecja: ukarano Krajowe Rządowe Centrum Usług
- Niewłaściwe publikowanie wrażliwych danych osobowych na stronie internetowej regionu Örebro

str. 11 **NOWE ODPOWIEDZI NA PYTANIA INSPEKTORÓW**



Szanowni Państwo!

Za nami 2 lata stosowania ogólnego rozporządzenia o ochronie danych osobowych (RODO), a za mną rok pełnienia zaszczytnej funkcji Prezesa Urzędu Ochrony Danych Osobowych.

Jak Państwo doskonale wiecie, RODO to akt, który bezpośrednio obowiązuje we wszystkich państwach członkowskich Unii Europejskiej, w sposób jednolity regulując prawa obywateli i obowiązki administratorów danych. Ale prawna regulacja ochrony danych osobowych to nie tylko RODO. System ochrony danych w Polsce ma już ponad 20-letnią tradycję. A w naszym kraju mamy do czynienia z kilkuset aktami prawnymi na poziomie ustaw i rozporządzeń do nich, które regulują kwestie przetwarzania i ochrony danych osobowych.

Minione lata stosowania RODO, ale i okres przygotowawczy do wprowadzenia rozporządzenia, to czas podnoszenia świadomości społeczeństwa i edukacji na temat ochrony danych osobowych.

Obecnie edukacja, którą prowadzimy, w nieco większym stopniu ukierunkowana jest do osób fizycznych. Natomiast zawsze jednym z najważniejszych zadań regulatora była i jest współpraca z inspektorami ochrony danych. Jesteście Państwo ekspertami, którzy pełnią ogromną rolę w systemie ochrony danych w naszym kraju. Funkcja inspektora ochrony danych, która tworzyła się na naszych oczach, jest fundamentalna dla budowy systemu skutecznej ochrony danych osobowych. Chciałem to stanowczo podkreślić i podziękować za to.

Jako Urząd staramy się Państwa wspierać w podnoszeniu fachowości oraz zachować jednolitość stosowania ogólnego rozporządzenia, dostarczając Państwu na bieżąco merytorycznych treści, zarówno poprzez nasze kanały informacyjne, w tym infolinię, jak i media. Niebawem uruchamiamy także cykl szkoleń online, tak aby jak najwięcej osób mogło z nich skorzystać, będąc jednocześnie bezpiecznym w kontekście zagrożeń związanych z koronawirusem.

Zgodnie z raportem Komisji Europejskiej, na tle Europejczyków Polacy mają dużą świadomość funkcjonowania RODO (56 proc). Te dane potwierdza liczba skarg i naruszeń, która z roku na rok szybko wzrasta. W 2019 r. do UODO wpłynęło ponad 9 tys. skarg, a administratorzy zgłosili w tym czasie ponad 6 tys. naruszeń ochrony danych osobowych. Tylko w pierwszym kwartale tego roku mamy prawie 2 tys. naruszeń i niewiele mniej skarg. Przed nami coraz więcej pracy, ale wiem, że także z Państwa wsparciem sprostamy tym zadaniom.

Przed nami kolejne wyzwania. Należy do nich m.in. ciągle budowanie świadomości wśród administratorów jak ważna jest ochrona danych osobowych oraz dalsze umacnianie pozycji inspektora ochrony danych w organizacjach. Jestem przekonany, że wspólnymi siłami uda nam się temu sprostać.

Jan Nowak
Prezes UODO



POWIAT NIE POWINIEN ZAWIERAĆ UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH Z PUP ANI PCPR

Choć to powiaty mają realizować zadania określone w ustawie o promocji zatrudnienia i instytucjach rynku pracy oraz w ustawie o rehabilitacji zawodowej i społecznej oraz o zatrudnianiu osób niepełnosprawnych, to jednak robią to za pośrednictwem swoich jednostek organizacyjnych mających status administratora. Niezasadne byłoby zatem zawieranie z nimi umów powierzenia przetwarzania danych osobowych.

Do takiego wniosku prowadzi analiza przepisów ustawy z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy oraz ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz o zatrudnianiu osób niepełnosprawnych. Stanowią one, że w zakresie polityki rynku pracy właściwe są powiatowe urzędy pracy (art. 9 ust. 1 i 2), natomiast w zakresie rehabilitacji zawodowej i zatrudniania osób niepełnosprawnych – powiatowe centra pomocy rodzinie albo powiatowe urzędy pracy (art. 35a ust. 1 i ust. 2).

Z ustawy o promocji zatrudnienia i instytucjach rynku pracy wynika, że powiatowym urządowi pracy należy przyznać status administratora danych, gdyż same wykonują nałożone na nich zadania ustawowe i decydują tym samym o celach przetwarzania danych osobowych, np. rejestrują bezrobotnych i poszukujących pracy oraz prowadzą rejestr tych osób, prowadzą pośrednictwo pracy dla zarejestrowanych osób, a w razie braku możliwości zapewnienia odpowiedniej pracy, świadczą usługę poradnictwa zawodowego czy przyznają i wypłacają zasiłki oraz inne świad-

czenia z tytułu bezrobocia (m.in. art. 4 ust. 5h, art. 4a, art. 33 ust. 1, art. 9a, art. 34).

Również przepisy ustawy o rehabilitacji zawodowej i społecznej oraz o zatrudnianiu osób niepełnosprawnych wskazują, że wymienione w tej ustawie zadania wykonują albo powiatowe centra pomocy rodzinie (art. 35a ust. 2 pkt 1), albo powiatowe urzędy pracy (art. 35a ust. 2 pkt 2). Oznacza to, że w ramach tych zadań przyznaje się im status administratora.

Zatem skoro powiatowy urząd pracy i powiatowe centrum pomocy rodzinie pełnią rolę administratora danych przetwarzanych w celu realizacji zadań określonych w ustawie o promocji zatrudnienia i instytucjach rynku pracy oraz w ustawie o rehabilitacji zawodowej i społecznej oraz o zatrudnianiu osób niepełnosprawnych, to zawieranie z nimi przez powiat umowy powierzenia przetwarzania danych na potrzeby wykonania tych zadań byłoby niezasadne i niezgodne z prawem.



KONTROLA WYKORZYSTANIA DOTACJI NA REALIZACJĘ ZADANIA PUBLICZNEGO

Prawa i obowiązki stron, w tym sposób rozliczania dotacji na realizację zadania publicznego przyznanej podmiotowi prowadzącemu działalność pożytku publicznego przez organ administracji publicznej, powinny być określone w umowie. Jeśli do kontroli wydatkowania środków publicznych niezbędne byłyby wyciągi bankowe dotyczące wynagrodzenia poszczególnych pracowników podmiotu realizującego dotowane zadania, to ich udostępnienie podmiotowi, który przyznał dotację, znajduje podstawę prawną w szczególnych przepisach prawa.

Zasady realizacji zadań publicznych przez podmioty prowadzące działalność pożytku publicznego regulują przepisy ustawy z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie. Przesądżają one, że organizacje pozarządowe oraz podmioty wymienione w art. 3 ust. 3, takie jak stowarzyszenia jednostek samorządu terytorialnego czy spółdzielnie socjalne, prowadzące działalność statutową w danej dziedzinie, mogą realizować zadania publiczne po uzyskaniu wsparcia ze strony organu administracji publicznej albo po jego powierzeniu przez taki organ (art. 11 ust. 1).

Podstawą do realizacji takiego zadania publicznego jest pisemna umowa zawarta między tymi podmiotami (art. 16), która powinna zostać sporządzona z uwzględnieniem art. 151 ust. 2 i art. 221 ust. 3 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych. Wynika z nich, że umowa dotacyjna między dysponentem części budżetowej a organizacją pozarządową oraz umowa o dotacje celowe na cele publiczne dla podmiotów niezaliczanych do sektora finansów publicznych powinny określać m.in. termin i sposób rozliczenia udzielonej dotacji. Ponadto, podmiot, któremu organ publiczny zleca wykonywanie zadania publicznego, ma obowiązek wyodrębnienia w ewidencji księgowej środków otrzymanych na realizację tej umowy (art. 16 ust. 5).

Przepisy ustawy o działalności pożytku publicznego i o wolontariacie wprost określają (art. 17), że organ administracji publicznej zlecający realizację zadania publicznego może dokonywać kontroli i oceny realizacji zadania, w szczególności:

- stopnia realizacji zadania;
- efektywności, rzetelności i jakości realizacji zadania;
- prawidłowości wykorzystania środków publicznych otrzymanych na realizację zadania;
- prowadzenia dokumentacji związanej z realizowanym zadaniem.

Prawa i obowiązki stron, w tym także kwestie związane z terminem i sposobem rozliczenia udzielonej dotacji, powinna określać umowa zawarta między podmiotem, który otrzymał dotację na realizację zadania publicznego, a organem administracji, który ją przyznał.

Niemniej, ponieważ art. 17 ustawy o działalności pożytku publicznego i o wolontariacie przyznaje organowi zlecającemu realizację zadania publicznego uprawnienie do dokonywania kontroli zadania przez podmiot przyjmujący zlecenie, w tym prawidłowości wykorzystania środków publicznych i prowadzenia dokumentacji związanej z realizowanym zadaniem, to jeśli do takiej kontroli byłyby niezbędne wyciągi bankowe dotyczące pożytkowania środków publicznych na wynagrodzenia poszczególnych pracowników podmiotu realizującego zadanie publiczne, to ich udostępnienie podmiotowi, który przyznał dotację, znajduje podstawę prawną w tych szczególnych przepisach prawa. Tym samym spełniona jest legalizująca takie działanie przesłanka z art. 6 ust. 1 lit. e RODO.



KTO JEST ADMINISTRATOREM DANYCH PRZETWARZANYCH W ZWIĄZKU Z MEDIACJĄ W POSTĘPOWANIU ADMINISTRACYJNYM

W przypadku podmiotów realizujących zadania określone przepisami prawa, rozstrzygając, który z nich w danej sytuacji jest administratorem w odniesieniu do konkretnych danych osobowych, zazwyczaj należy dokonać analizy przepisów prawa określających te zadania. Tak jest również w przypadku mediacji w postępowaniu administracyjnym.

Kwestie związane z przeprowadzaniem mediacji w postępowaniu administracyjnym uregulowano w art. 96a-96n ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (k.p.a.). Stanowią one, że mediacja może być przeprowadzona w toku postępowania administracyjnego, jeżeli pozwala na to charakter sprawy (art. 96a § 1 k.p.a.). Określają też zakres zadań (kompetencji) zarówno organu administracji publicznej, jak i mediatora.

Kiedy mediator staje się administratorem?

Z art. 96h k.p.a. wynika, że organ administracji publicznej przekazuje niezwłocznie mediatorowi dane kontaktowe uczestników mediacji, po uzyskaniu zgody uczestników mediacji na jej przeprowadzenie. W przepisie zabrakło wskazania, że wraz z danymi kontaktowymi organ przekazuje mediatorowi odpis postanowienia o skierowaniu sprawy do mediacji. Taka praktyka – jak wskazuje się w literaturze przedmiotu – jest jednak zasadna. Nie ulega zatem wątpliwości, że mediator staje się administratorem danych osobowych udostępnionych wraz z postanowieniem o skierowaniu sprawy do mediacji, w związku z przypisanym mu w ustawie zadaniem polegającym na przeprowadzeniu mediacji mającej na celu wyjaśnienie i rozważenie okoliczności faktycznych i prawnych sprawy oraz dokonanie ustaleń dotyczących jej załatwienia w granicach obowiązującego prawa.

Pozyskiwanie przez mediatora danych osobowych może następować także w toku przeprowadzanego przez niego „spotkania” mediacyjnego (art. 96n § 2 k.p.a.) i innych czynności związanych z mediacją (np. zgodnie z art. 96i k.p.a., mediator zapoznaje się z aktami sprawy wraz ze sporządzeniem z nich notatek, kopii lub odpisów, chyba że uczestnik mediacji nie wyraził zgody na zapoznanie się z aktami).

Jego zadaniem jest również wspieranie uczestników mediacji w formułowaniu przez nich propozycji ugodowych (art. 96k k.p.a.).

Mediator jest nie tylko osobą, której działanie ma doprowadzić do merytorycznego zakończenia sporu, ale także wykonuje związane z mediacją obowiązki o charakterze administracyjnym lub technicznym. Między innymi mediator przeprowadza mediację w ustalonym przez niego terminie i miejscu (art. 96k k.p.a.). W przepisach Kodeksu postępowania administracyjnego dotyczących mediacji pozostawiono mediatorom swobodę co do sposobu organizacji przebiegu mediacji. Nie przesądza się bowiem ani o formie mediacji (czy ma ona przyjmować formę spotkania lub spotkań mediatora z uczestnikami mediacji albo innych sposobów dokonywania ustaleń, np. w drodze komunikacji elektronicznej, wideokonferencji itp.), ani o jej technikach. Wskazanie czasu i miejsca mediacji powinno jednak znaleźć się w protokole z przebiegu mediacji, o którym mowa w art. 96m k.p.a. Na tym tle dopuszczalne jest prowadzenie mediacji zarówno w trybie gabinetowym, w drodze indywidualnych negocjacji ze stroną i przedstawicielem organu lub z tymi podmiotami łącznie, jak i zorganizowanie posiedzenia w sposób zbliżony do rozprawy administracyjnej. Mediator sporządza także protokół z przebiegu mediacji o treści określonej w art. 96m § 2 k.p.a. i niezwłocznie przedkłada go organowi administracji publicznej w celu włączenia go do akt sprawy, a odpisy doręcza uczestnikom mediacji.

Mediator jako administrator zobowiązany jest również do spełnienia w stosunku do stron postępowania obowiązku informacyjnego, o którym mowa w art. 13–15 RODO. Przetwarzanie danych osobowych w toku postępowania mediacyjnego zobowiązuje również mediatora

do przestrzegania zasad przetwarzania danych osobowych wskazanych w art. 5 RODO, takich jak: zgodność z prawem, rzetelność i przejrzystość, ograniczenie celu przetwarzania, minimalizacja danych, prawidłowość, ograniczenie przechowywania oraz integralność i poufność.

Organ administracji publicznej jako odrębny administrator

Administratorem danych osobowych stron postępowania mediacyjnego jest również organ administracji publicznej.

Należy podkreślić, że zgodnie z zasadą wyrażoną w art. 13 kpa § 2 k.p.a., organ administracji publicznej podejmuje wszystkie uzasadnione na danym etapie postępowania czynności umożliwiające przeprowadzenie mediacji lub zawarcie ugody, a zwłaszcza udziela wyjaśnień o możliwościach i korzyściach polubownego załatwienia sprawy. Mediacja może być podjęta zarówno z urzędu przez organ administracji publicznej, jak i na wniosek strony postępowania. W pierwszym przypadku będzie wyrazem pozytywnej oceny przez organ przesłanki materialnej (charakter sprawy pozwala na przeprowadzenie mediacji) i formalnej (sprawa w toku) mediacji. Ponadto powinna ona być następstwem oszacowania przez organ, że mediacja ma szanse zakończenia się akceptowanymi przez jej uczestników ustaleniami, a w wyniku mediacji możliwe jest realizowanie w szerszym zakresie standardów postępowania wynikających z zasad ogólnych (m.in. zasady prawdy obiektywnej, zasady przekonywania, zasady czynnego udziału w postępowaniu) niż w tradycyjnym modelu postępowania[5]. A zatem w przypadku wydania postanowienia o skierowaniu sprawy do mediacji organ administracji będzie administratorem danych osobowych stron postępowania mediacyjnego. Jemu również przekazywany jest protokół z przebiegu mediacji sporządzony przez mediatora, wraz z ustaleniami mediacyjnymi, celem załączenia go do akt postępowania administracyjnego (art. 96m k.p.a.). Załatwienie sprawy przez organ administracji polega przede wszystkim na wydaniu decyzji administracyjnej, która powinna uwzględniać w swym rozstrzygnięciu w całości ustalenia mediacyjne. Jeżeli jednak część z ustaleń mediacyjnych nie mieści się w granicach obowiązującego prawa, organ powinien rozstrzygnąć sprawę z uwzględnieniem jedynie tych ustaleń, które nie naruszają prawa. Zobowiązany jest on bowiem w każdym przypadku respektować zasadę legalności. W sytuacji gdy ustalenia mediacyjne odpowiadają prawu,

organ zobligowany jest do rozstrzygnięcia sprawy w sposób zgodny w całości z tymi ustaleniami.[6] Organ administracji jako odrębny administrator zatwierdza też ugody zawartą przed mediatorem (o ile oczywiście zakres sprawy objętej danym postępowaniem dopuszcza taki sposób załatwienia sprawy).

A zatem odrębni administratorzy?

W postępowaniu mediacyjnym zarówno organ administracji publicznej, jak i mediator to odrębni administratorzy przetwarzanych przez siebie danych. Każdy we własnym zakresie realizuje konkretne zadania wynikające z powołanych wyżej przepisów prawa. Żeby możliwe było przeprowadzenie mediacji, której celem jest wyjaśnienie i rozważenie okoliczności faktycznych i prawnych sprawy oraz dokonanie ustaleń dotyczących jej załatwienia w granicach obowiązującego prawa, niezbędne jest przetwarzanie określonych danych osobowych przez mediatora. W tym przypadku mamy jednak do czynienia z udostępnieniem danych osobowych niebędącym powierzeniem – podmiot, który otrzymuje dane osobowe, przetwarza je w celach, które samodzielnie kształtuje – nie w celach własnych udostępniającego, gdyż jak wynika to z art. 96k k.p.a., mediator – prowadząc mediację – dąży do polubownego rozwiązania sporu, a także wspiera uczestników mediacji w formułowaniu propozycji ugodowych. To do niego właśnie należy przyjęcie rozwiązania zmierzającego do porozumienia między stronami (uczestnikami mediacji).

Wobec powyższego w tej sytuacji nie zachodzi konieczność zawarcia między tymi podmiotami umowy powierzenia przetwarzania danych. Mamy tu bowiem do czynienia z udostępnieniem danych na podstawie przepisów prawa.

Przypadek współadministrowania

Inaczej przedstawia się relacja pomiędzy mediatorem a organem administracji prowadzącym postępowanie w sytuacji, gdy jest on uczestnikiem mediacji, a uzgodnienia mediacyjne przyjmą formę posiedzenia mediacyjnego w siedzibie tego organu administracji. Zapewnienie obsługi technicznej posiedzenia mediacyjnego należeć będzie do organu administracji prowadzącego postępowanie. W takich uwarunkowaniach dochodzi do sytuacji, kiedy organ administracji oraz mediator wspólnie będą ustalać cele i sposoby przetwarzania danych osobowych, w ramach ustawowo przypisanych

im zadań. Pomiedzy tymi administratorami będzie zachodziła relacja współadministracji uregulowana w art. 26 RODO.

Zatem mediator oraz organ administracji prowadzący postępowanie jako współadministratorzy powinni w drodze wspólnych uzgodnień w przejrzysty sposób określić odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków odnoszących się do podawania informacji, o których mowa w art. 13 i 14, chyba że przypadające im obowiązki i ich zakres określa prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą. W myśl natomiast art. 26 ust. 2 RODO, uzgodnienia, o których mowa w ust. 1, muszą należycie odzwierciedlać odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą.

Takie wspólne uzgodnienia muszą uwzględniać faktyczne obowiązki mediatora i organu administracji prowadzącego postępowanie, związane z przetwarzaniem danych osobowych uczestników mediacji. Zarówno mediator, jak i organ administracji prowadzący postępowanie mają swoje autonomiczne uprawnienia, z którymi związane jest przetwarzanie danych osobowych uczestników mediacji w innych celach.

Przykładowo, jedynie do mediatora jako podmiotu aktywnego w procesie mediacji należy podejmowanie

czynności polegających na wspieraniu uczestników mediacji w formułowaniu przez nich propozycji ugodowych. Organ administracji prowadzący postępowanie, w ramach współadministrowania, może być uprawniony np. do zapewnienia ochrony pomieszczeń. Należy wskazać, że odpowiedzialność za przestrzeganie przepisów o ochronie danych osobowych w zakresie realizacji takich autonomicznych uprawnień kształtują przepisy prawa. Mediator i organ administracji prowadzący postępowanie, w ramach wspólnych uzgodnień, powinni więc określić inne zagadnienia, nieuregulowane wprost w przepisach prawa, w tym m.in. kwestię odpowiedzialnego zabezpieczenia danych osobowych czy też realizacji określonych obowiązków informacyjnych.

Dokonanie wspólnych ustaleń pomiędzy współadministratorami, o których mowa w art. 26 RODO, umożliwia doprecyzowanie sposobu obsługi technicznej mediatorów przez organ administracji prowadzący postępowanie przy zachowaniu autonomicznych kompetencji mediatora w zakresie jego odrębnych zadań jako administratora.

Przypisy:

- [1] Wilbrandt-Gotowicz Martyna. Art. 96(h). W: Komentarz aktualizowany do Kodeksu postępowania administracyjnego. System Informacji Prawnej LEX, 2019.)
- [2] Ziemiannin Karolina. RODO W POSTĘPOWANIU MEDIACYJNYM. W: Ochrona danych osobowych w postępowaniach sądowych i przed organami administracji publicznej. Wolters Kluwer Polska, 2019
- [3] Wilbrandt-Gotowicz Martyna. Art. 96(k). W: Komentarz aktualizowany do Kodeksu postępowania administracyjnego. System Informacji Prawnej LEX, 2019.
- [4] J. Wegner-Kowalska, Mediacja (art. 13, art. 96a–96g [w:] Reforma prawa o postępowaniu administracyjnym. Raport zespołu eksperckiego z prac w latach 2012–2016, red. Z. Kmiecik, Warszawa 2017, s. 81).
- [5] Wilbrandt-Gotowicz Martyna. Art. 96(b). W: Komentarz aktualizowany do Kodeksu postępowania administracyjnego. System Informacji Prawnej LEX, 2019
- [6] Wilbrandt-Gotowicz Martyna. Art. 96(n). W: Komentarz aktualizowany do Kodeksu postępowania administracyjnego. System Informacji Prawnej LEX, 2019



MIĘDZYNARODOWE

Zarówno organy unijne, jak i organy nadzorcze państw członkowskich podjęły działania, także o charakterze informacyjno-edukacyjnym, w walce z koronawirusem. Zapraszamy do zapoznania się z kilkoma przykładami, które dotyczą m.in. działań służących ochronie danych osobowych i prywatności w kontekście wdrażania aplikacji służących śledzeniu kontaktów osób zakażonych.

Oświadczenie w sprawie cyfrowego śledzenia kontaktów

Wspólne oświadczenie Alessandry Pierucci, przewodniczącej Komitetu Konsultacyjnego Konwencji 108 oraz Jean-Philippe'a Waltera, komisarza ds. ochrony danych Rady Europy w sprawie cyfrowego śledzenia kontaktów.

Od początku pandemii, rządy i strony zaangażowane w zwalczanie wirusa (m.in. środowisko naukowe), aby zaradzić nowemu zagrożeniu, polegają na analizie wielu danych i technologii cyfrowej.

W walce z COVID-19 wykorzystuje się dane i technologie mobilne, które obejmują: wykorzystanie danych o lokalizacji mobilnej do oceny przemieszczania się ludności lub egzekwowania środków ograniczających, wykorzystanie urządzeń jako cyfrowego dowodu odporności, wykrywanie objawów, samokontrola lub wreszcie cyfrowe śledzenie kontaktów osoby zarażonej.

Dlatego, jeżeli stosowanie tych środków i przetwarzanie danych jest konieczne do walki z koronawirusem, powinno być proporcjonalne w stosunku do realizowanego celu, oraz odzwierciedlać właściwą równowagę między wszystkimi zainteresowanymi stronami oraz właściwymi prawami i swobodami, jak nakazują Europejska Konwencja Praw Człowieka (art. 8) i Konwencja 108+ (art. 5 i 11).

Zanim państwa przystąpią do systemowego wdrażania technologii, powinny zastanowić się, czy są one jedynym możliwym rozwiązaniem. Warto odpowiedzieć na pytania:

- Czy przewidywany efekt jest wart ryzyka społecznego i prawnego, biorąc pod uwagę brak dowodów na skuteczność zastosowanych rozwiązań?
- Jakie prawne i techniczne zabezpieczenia należy wprowadzić, aby zmniejszyć ryzyko w przypadku, gdy rządy decydują się na cyfrowe śledzenie kontaktów w zarządzaniu pandemią COVID-19?

Pandemia koronawirusa stworzyła bezprecedensowe wyzwanie, które wymaga największego zaangażowania i zachowania ostrożności, nie tylko w stosunku do podejmowanych wyborów politycznych, ale i wsparcia społecznego oraz indywidualnego zaangażowania. Oprócz kwestii związanych z prywatnością i ochroną danych, cyfrowe śledzenie kontaktów rodzi pytania o nierówności i dyskryminację, które również należy wziąć pod uwagę.

Więcej informacji odnośnie do ochrony danych osobowych i prywatności w kontekście wdrażania aplikacji służących cyfrowemu śledzeniu kontaktów znajduje się pod adresem: <https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7>

Belgia: Ochrona danych osobowych nie przeszkadza w użyciu technologii przeciw COVID-19, o ile jest to zgodne z zasadami

W celu wydania opinii w sprawie dwóch wstępnych projektów dekretów królewskich dotyczących odpowiednio stosowania aplikacji śledzącej oraz utworzenia bazy danych „w celu zapobiegania rozprzestrzenianiu się koronawirusa”, skonsultowano się z organem ochrony danych.

Ten stwierdził, że ochrona danych osobowych nie stanowi przeszkody we wdrażaniu narzędzi technologicznych w walce z epidemią COVID-19, o ile są one zgodne z pewnymi podstawowymi zasadami. Dekrety, które przewidują i regulują korzystanie z tych narzędzi, muszą być precyzyjne i kompletne, aby zapewnić optymalną przejrzystość w stosunku do obywateli, a także należy wykazać potrzebę korzystania z aplikacji śledzących, jak uważa belgijski organ nadzorczy. W ramach walki z rozprzestrzenianiem się koronawirusa przewiduje się śledzenie osób, które mogły zostać zarażone przez osobę, która uzyskała wynik pozytywny. Śledzenie to można by przeprowadzić, próbując zapamiętać osoby, z którymi się spotkał, a dodatkowo za pomocą aplikacji (działałaby w oparciu o klucze cyfrowe, które nie identyfikują bezpośrednio zainteresowanych osób). Projekty normatywne

stanowią ramy dla stosowania aplikacji cyfrowego śledzenia kontaktów oraz dla stworzenia bazy danych.

Opinie organu ds. ochrony danych osobowych na temat tych projektów można streścić w dwóch głównych punktach:

1. Należy wykazać konieczność i proporcjonalność aplikacji śledzących i utworzenia bazy danych przez Sciensano (krajowy instytut zdrowia publicznego w Belgii – red.): – Ingerencja w życie prywatne obywateli dopuszczalna na mocy niniejszych dekrétów królewskich jest dozwolona tylko wtedy, gdy jest konieczna i proporcjonalna do osiągnięcia celu interesu publicznego, jakim jest zwalczanie rozprzestrzeniania się wirusa. Wdrożenie systemu śledzenia za pomocą aplikacji jest dopuszczalne tylko wtedy, gdy jest to najmniej inwazyjny środek do osiągnięcia zamierzonego celu i gdy istnieje właściwa równowaga między interesami, o których mowa (proporcjonalność).

2. Projekty muszą zapewniać dodatkowe gwarancje dla obywateli:

- Teksty wymagają dalszego doprecyzowania. Dekret dotyczący utworzenia bazy danych musi być bardziej przejrzysty, jeśli chodzi o pochodzenie gromadzonych danych, osoby trzecie, którym te dane medyczne mogą być przekazywane i sposoby ich wykorzystania.

- Teksty muszą również stanowić, że nie powinno być możliwe tworzenie odniesień między różnymi bazami danych utworzonymi w kontekście walki z epidemią (lub z jakąkolwiek inną bazą danych) lub, że zebrane dane nie powinny być ponownie wykorzystywane do innych celów.

Poza uwagami, które przedstawił w odniesieniu do wstępnych projektów, APD przypomina, że każda aplikacja śledząca musi być zgodna z zasadami i specyfikacjami określonymi przez Europejską Radę Ochrony Danych (EROD), która niedawno opublikowała wytyczne i „zestaw narzędzi” na ten temat. Konieczne jest np. zapewnienie, aby pobieranie i korzystanie z aplikacji umożliwiającej śledzenie było rzeczywiście dobrowolne i, aby żaden obywatel odmawiający korzystania z niej nie ponosił żadnych negatywnych skutków (takich jak odmowa dostępu do towaru lub usługi). Kod źródłowy każdej aplikacji będzie również musiał zostać opublikowany z wyprzedzeniem, aby zapewnić ekspertom odpowiednią ilość czasu na sprawdzenie jego działania.

Norwegia: analiza dotycząca zamówienia aplikacji śledzącej infekcje Infect Stop

Norweski organ nadzorczy powiadomił Norweski Instytut Zdrowia Publicznego (FHI) o decyzjach związanych z zamówieniem aplikacji Infect Stop.

Norweski odpowiednik UODO uważa, że istnieją niedociągnięcia w protokole leczenia pacjenta FHI oraz analizie ryzyka, które zostały wykonane w związku z wdrażaniem aplikacji. W protokole leczenia cel aplikacji określono jako „cyfrowe śledzenie infekcji”. W ocenie Inspektoratu nie jest to wystarczająco dokładne. Zdaniem organu nadzorczego, aplikacja ta ma kilka celów, takich jak śledzenie i powiadamianie o zakażeniu COVID-19, monitorowanie ruchów populacji, prace analityczne i badania. Cele te powinny zostać określone w protokole leczenia. Natomiast, jeśli chodzi o analizę ryzyka i podatności na zagrożenia (analiza ROS), brakuje w niej oceny kluczowych elementów rozwiązania: ostrzegania populacji przed infekcją COVID-19, anonimizacji danych osobowych i prac analitycznych. Celem takiej analizy jest przedstawienie ryzyka rozwiązania technicznego, aby umożliwić wdrożenie środków jego ograniczających. Tylko wtedy gdy znane jest ryzyko, można zdecydować, czy dane rozwiązanie jest dopuszczalne.

Ponadto zdaniem norweskiego organu nadzorczego Norweski Instytut Zdrowia Publicznego nie udokumentował, że te niezbędne oceny kluczowych części rozwiązania zostały przeprowadzone przed nabyciem aplikacji i udostępnieniem jej społeczeństwu. Norweski organ nadzorczy kontynuuje prace nad kontrolą FHI i aplikacji. Zajmie się m.in. kwestiami związanymi z celem, użytecznością, gromadzeniem i przechowywaniem danych osobowych, a także bezpieczeństwem aplikacji.



Szwecja: ukarano Krajowe Rządowe Centrum Usług

Szwedzki urząd ochrony danych nałożył karę administracyjną w wysokości 200 tys. koron szwedzkich (około 18,7 tys. euro) na Krajowe Rządowe Centrum Usług (dalej: KRCU) za brak zawiadomienia osób, których dane dotyczą oraz brak zgłoszenia naruszenia ochrony danych organowi nadzorczemu w odpowiednim terminie.

Szwedzki organ nadzorczy zainicjował postępowanie po otrzymaniu zgłoszeń dotyczących naruszenia ochrony danych dotyczących błędu w systemie informatycznym odpowiedzialnym za zarządzanie płacami. Błąd ten dopuszczał możliwość nieuprawnionego dostępu do danych osobowych zarówno personelu organów korzystających z systemu, jak i kadr KRCU.

Organ ochrony danych odnotował, że KRCU potrzebowało prawie pięciu miesięcy by zawiadomić strony, których sprawa dotyczy, a niespełna trzy miesiące upłynęły zanim organ nadzorczy otrzymał zgłoszenie naruszenia ochrony danych.

W swojej decyzji organ ochrony danych nakazał KRCU wprowadzenie wewnętrznych procedur dokumentacji naruszeń ochrony danych osobowych oraz weryfikacji ich przestrzegania. Wraz z tym nakazem organ ochrony danych nakłada na KRCU karę administracyjną w wysokości 200 tys. koron szwedzkich.

Pełna decyzja w języku szwedzkim dostępna jest pod adresem: <https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-tillsyn-ssc-20200428.pdf>

Źródło: https://edpb.europa.eu/news/national-news/2020/swedish-data-protection-authority-issues-fine-against-national-government_pl

Niewłaściwe publikowanie wrażliwych danych osobowych na stronie internetowej regionu Örebro

Szwedzki organ nadzorczy nałożył karę administracyjną w wysokości 120 tys. koron szwedzkich (ok. 11 tys. euro) na Komisję ds. Ochrony Zdrowia regionu Örebro.

Postępowanie przeprowadzone na skutek skargi wykazało, że Komisja ds. Ochrony Zdrowia w regionie Örebro popełniła błąd, publikując na stronie internetowej regionu wrażliwe dane osobowe, dotyczące pacjenta przyjętego do kliniki psychiatrii sądowej.

Szwedzki organ udowodnił, że nie istnieją żadne pisemne instrukcje w zakresie publikacji dokumentów i danych osobowych na przedmiotowej stronie internetowej. Polecenia w sprawie publikacji informacji były komunikowane ustnie, co doprowadziło do przypadkowej publikacji dokumentu. Na podstawie tego przypadku należy przypuszczać, że Komisja ds. Ochrony Zdrowia regionu Örebro nie powzięła wystarczających środków organizacyjnych w celu zapewnienia, że dane osobowe są zabezpieczone przed błędną publikacją na stronie internetowej regionu.

Z tego powodu organ szwedzki nakazał Komisji stworzenie pisemnych instrukcji i wprowadzenie środków, które zapewnią, by osoby publikujące dane osobowe na stronie internetowej regionu robiły to zgodnie z ustalonymi zasadami.

Dokument, którego dotyczyło postępowanie, został usunięty ze strony internetowej regionu.

Pełna treść decyzji dostępna jest w języku szwedzkim pod adresem: <https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-tillsyn-region-orebro-2020-05-11.pdf>

Źródło: https://edpb.europa.eu/news/national-news/2020/wrongful-publish-sensitive-personal-data-region-orebro-countys-website_pl

NOWE ODPOWIEDZI NA PYTANIA INSPEKTORÓW

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



Wyjaśnienia dotyczą takich kwestii, jak:

Czy szczególny obowiązek upubliczniania decyzji administracyjnej zwalnia z anonimizacji danych?
W jaki sposób identyfikować osoby, które zwracają się do IOD jako punktu kontaktowego?
Na jakiej podstawie gmina może udostępniać obraz z kamer policji?
Który podmiot należy uznać za administratora danych przetwarzanych poza systemem EKSMON?
Czy dopuszczalne jest rejestrowanie egzaminów przeprowadzanych zdalnie przez uczelnie wyższe?

