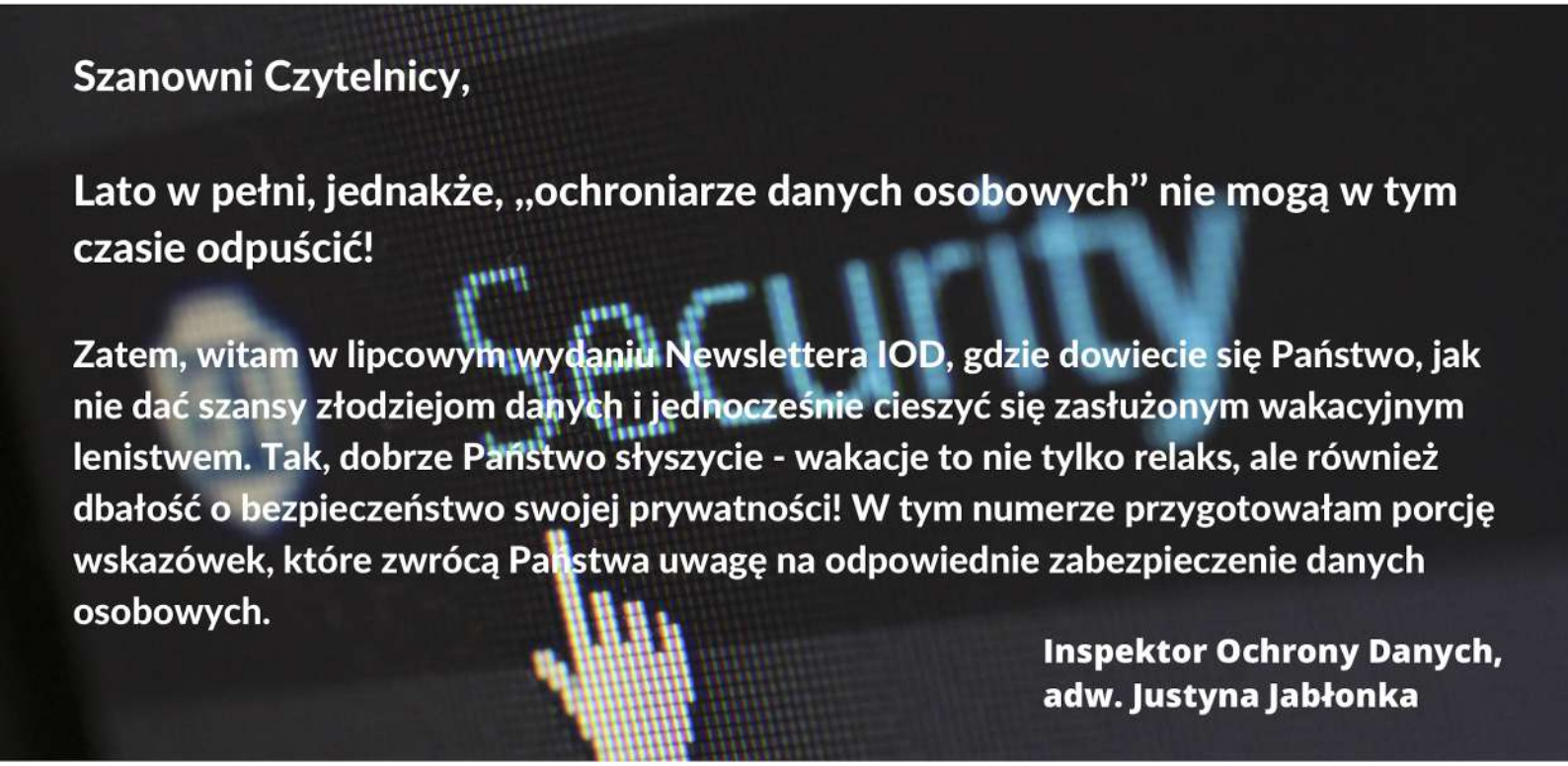
JUSTYNA JABŁONKA

Lipiec 2023
Nr 5/2023

KANCELARIA WYRZYKOWSCY

Newsletter
INSPEKTORA OCHRONY DANYCH
ADW. JUSTYNY JABŁONKI



Szanowni Czytelnicy,

Lato w pełni, jednakże, „ochroniarze danych osobowych" nie mogą w tym czasie odpuścić!

Zatem, witam w lipcowym wydaniu Newslettera IOD, gdzie dowiecie się Państwo, jak nie dać szansy złodziejom danych i jednocześnie cieszyć się zasłużonym wakacyjnym lenistwem. Tak, dobrze Państwo słyszycie - wakacje to nie tylko relaks, ale również dbałość o bezpieczeństwo swojej prywatności! W tym numerze przygotowałam porcję wskazówek, które zwrócą Państwa uwagę na odpowiednie zabezpieczenie danych osobowych.

Inspektor Ochrony Danych,
adw. Justyna Jabłonka

Wakacyjno-lipcowe tematy to:

I. Dane osobowe na wakacjach.

Wakacje powinny być czasem odpoczynku a nie zmartwieniem dotyczącym skutków kradzieży tożsamości. W tym artykule przedstawię kilka istotnych wskazówek, które pomogą chronić dane osobowe podczas wakacji.

Ogranicz udostępnianie kopii dokumentów.

Unikaj oddawania przypadkowym instytucjom kopii swoich dokumentów tożsamości. Wiele wypożyczalni sprzętu czy hoteli może prosić o wykonanie kserokopii lub zdjęcia dokumentu. Jednak taka praktyka jest niezgodna z prawem i stanowi ryzyko dla naszych danych osobowych. Wystarczy, że pracownik zanotuje nasze dane, które są niezbędne do dochodzenia roszczeń. Poproś o usunięcie swoich danych z baz i zniszczenie kartki z danymi po zwróceniu sprzętu.

Dane osobowe przekazywane do biura podróży.

Biuro podróży może gromadzić tylko te dane osobowe, które są niezbędne do zawarcia umowy i świadczenia usług, takich jak rezerwacja biletów czy kontakt z klientem.

Jeśli masz wątpliwości co do zakresu danych, które są od ciebie wymagane, masz prawo żądać informacji o podstawie prawnej takiego działania.
Pamiętaj, że biuro podróży powinno zrealizować wobec Ciebie obowiązek informacyjny, tj. poinformować m.in. o celu i zakresie przetwarzania, jak również wskazać komu będą przekazywane dane.

Dane osobowe w hotelu.

Hotel może żądać tylko tych danych osobowych, które są niezbędne do świadczenia usługi i rozliczenia, a także w celu dochodzenia ewentualnych roszczeń. Hotel nie ma prawa pytać o cel i czas trwania twojego pobytu w danym miejscu.
Nie zostawiaj w pokoju hotelowym przedmiotów zawierających prywatne informacje. Korzystaj z hotelowego sejfu.
Dane osobowe w wypożyczalni sprzętu sportowego.
Nie zgadzaj się na żądanie pozostawienia swojego dowodu osobistego w zastaw za wypożyczany sprzęt. Przechowywanie cudzego dowodu osobistego jest niezgodne z prawem. Wypożyczalnia może spisać niezbędne dane identyfikacyjne, a także poprosić o inne formy zabezpieczenia, takie jak kaucja.

Opublikuj zdjęcia z wakacji po powrocie. Unikaj publikowania na bieżąco zdjęć z wakacyjnych podróży, szczególnie gdy nikogo nie ma w domu. Opóźnij udostępnianie swoich przygód dopiero po powrocie z urlopu. W ten sposób nie informujesz potencjalnych złodziei, że twój dom jest pusty. Unikaj również ujawniania swojej lokalizacji w mediach społecznościowych.

Na stronie Urzędu Ochrony Danych Osobowych znajdziemy również wskazówki odnośnie **publikacji zdjęć dzieci w Internecie**: Trzeba pamiętać, że treści, które udostępniamy w Internecie, pozostają w nim na zawsze. Dlatego przed zamieszczeniem zdjęcia dzieci, zawsze warto pomyśleć o konsekwencjach takiego działania, zarówno teraz, jak i w przyszłości. Kradzież, powielenie fotografii i wykorzystanie wizerunku dziecka w negatywnym kontekście, modyfikacja zdjęcia i udostępnienie go w postaci mema, a w skrajnych przypadkach kradzież tożsamości lub pożywka dla osób o pedofilskich skłonnościach – to tylko przykładowe zagrożenia, na jakie rodzice bez namysłu publikujący zdjęcia w Internecie, narażają swoje dzieci. Dziecko, tak jak dorosły, ma prawo do prywatności i prawo ochrony dóbr osobistych.

Co więcej, fakt, że samo nie umie jeszcze nimi zarządzać, tym bardziej powinien skłaniać rodziców do tego, by robili to w jego imieniu rozważnie (https://uodo.gov.pl/pl/71/119).

Zabezpiecz swój smartfon na wypadek utraty lub kradzieży.

Zagubienie smartfona to nie tylko utrata finansowa, ale również ryzyko utraty ważnych danych, takich jak zdjęcia czy dokumenty. Ustaw blokadę ekranu, włącz usługę lokalizacji i zdalnego blokowania zawartości telefonu. Wykonuj regularne kopie zapasowe danych i przechowuj je w bezpiecznej chmurze.

Bądź ostrożny, udostępniając swój telefon.

Nie udostępniaj swojego telefonu nieznajomym osobom.

Ostrożnie korzystaj z publicznych sieci Wi-Fi.

Wyłącz automatyczne łączenie z publicznymi sieciami Wi-Fi. Zwróć uwagę, z jaką siecią się łączysz i upewnij się, że jest to bezpieczna sieć. Oszuści mogą podszywać się pod autentyczne sieci Wi-Fi i przechwytywać twoje dane. W razie potrzeby korzystaj z własnego połączenia internetowego lub zabezpiecz swoje połączenie za pomocą wirtualnej sieci prywatnej (VPN).

Zainstaluj oprogramowanie antywirusowe na swoim urządzeniu.

Odpowiednie oprogramowanie antywirusowe to podstawa w dzisiejszych czasach. Zainstaluj program antywirusowy, który chroni przed cyberatakami i złośliwym oprogramowaniem. Wybierz bezpieczne, sprawdzone rozwiązania, zarówno darmowe, jak i płatne.

Utrata dokumentu z danymi osobowymi.

Zgłoś utratę dokumentu na Policji i w odpowiednich urzędach. Zastrzeż dokument w ogólnopolskiej bazie Dokumenty Zastrzeżone (https://dokumentyzastrzezone.pl/). Utrata dokumentów tożsamości może prowadzić do nadużyć, dlatego należy działać szybko i podjąć odpowiednie kroki.

Warto zajrzeć:
https://uodo.gov.pl/pl/71/119 -> projekt UOKiK, w którym uczestniczy 40 instytucji, zawiera cenne porady i informacje dotyczące planowania urlopu.

Autor:
Justyna Jabłonka
Inspektor Ochrony Danych
adwokat

II. Obowiązki administratora w przypadku naruszenia w zakresie przetwarzania danych osobowych

W ostatnim czasie Prezesa UODO wydał szereg decyzji, w których nałożył na administratorów kary z tytułu niedopełnienia, wynikających z przepisów RODO, obowiązków związanych z wystąpieniem naruszenia przy przetwarzaniu danych osobowych. Kary nałożone w decyzjach z dnia 07 lutego 2023 r. (DKN.5131.31.2021), z dnia 01 marca 2023 r. (DKN.5131.49.2021) i z dnia 14 marca 2023 r. (DKN.5131.45.2022) wynosiły od ok. 1,5 tys. zł do blisko 52 tys. zł. Uchybienia stwierdzone przez PUODO polegały na niezgłoszeniu naruszenia organowi nadzoru i na niezawiadomieniu o naruszeniu osoby, której dane dotyczą. Warto zatem przypomnieć co powinno być traktowane jako naruszenie w zakresie ochrony danych i jakie obowiązki spoczywają na administratorze w sytuacji, gdy do takiego naruszenia dojdzie.

Pojęcie i kategorie naruszeń w zakresie przetwarzania danych osobowych

W świetle art. 4 pkt 12 RODO przez naruszenie ochrony danych osobowych należy rozumieć naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Podkreślenia wymaga przy tym, że nieprawidłowości przy przetwarzaniu danych osobowych, mogą przybierać postać nie tylko naruszenia poufności, które polega na ujawnieniu danych osobowych nieuprawnionej osobie, ale także naruszenia dostępności rozumianej jako czasowa, bądź trwała utrata danych (np. zniszczenie dokumentu, przypadkowe usunięcie danych) lub naruszenia integralności, które polega na nieautoryzowanej zmianie treści danych osobowych (por. Grupa Robocza Art. 29 Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679, WP 250 rev. 01). Naruszeniem w zakresie przetwarzania danych osobowych jest więc nie tylko bezprawne ujawnienie danych osobie nieupoważnionej, ale także np. przypadkowe zniszczenie dokumentu, zagubienie kluczy do pomieszczeń, w których przechowywane są dane osobowe, uszkodzenie nośnika, na którym są przechowywane czy czasowy brak dostępu do danych, np. z powodu braku prądu.

Zakres obowiązków spoczywających na administratorze w przypadku naruszenia przy przetwarzaniu danych osobowych zależy od stopnia naruszenia. Przepisy RODO pozwalają na wyodrębnienie trzech poziomów naruszeń, różniących się rzeczywistym i potencjalnym wpływem danego zdarzenia na prawa i wolności osób fizycznych, w tym w szczególności osoby, której dane dotyczą. Pierwszą grupę stanowią zdarzenia, w przypadku których prawdopodobieństwo zaistnienia ryzyka naruszenia praw i wolności osób fizycznych nie występuje albo jest małe. Druga grupa obejmuje zdarzenia, w przypadku których prawdopodobieństwo to jest większe niż małe, ale nie jest wysokie. Trzecią grupę stanowią zdarzenia, w przypadku których prawdopodobieństwo zaistnienia ryzyka naruszenia praw i wolności osób fizycznych jest wysokie. Ocena poziomu ryzyka związanego z wystąpieniem określonego zdarzenia musi być dokonywana osobno w odniesieniu do każdej sytuacji i powinna brać pod uwagę wszelkie zagrożenia dla podmiotu danych, a nie interesy administratora (por. decyzja PUODO z dnia 1 marca 2023 r., DKN.5131.49.2021).

Zgodnie ze stanowiskiem prezentowanym przez Prezesa UODO, ryzyko naruszenia praw lub wolności osób fizycznych powstaje, kiedy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych, których dane naruszono. Szkodami takimi mogą być w szczególności dyskryminacja, kradzież tożsamości lub oszustwo dotyczące tożsamości, nadużycia finansowe, straty finansowe, nieuprawnione cofnięcie pseudonimizacji, utrata poufności danych osobowych chronionych tajemnicą zawodową; naruszenie dobrego imienia oraz inne znaczące skutki gospodarcze lub społeczne dla danej osoby fizycznej. Ocena poziomu ryzyka związanego z wystąpieniem określonego zdarzenia może być trudna. Warto jednak pamiętać, że zgodnie z wytycznymi Prezesa UODO, w każdym przypadku, gdy naruszenie dotyczy danych osobowych wrażliwych albo dojdzie do ujawnienia danych osobowych obejmujących łącznie: imię, nazwisko i numer PESEL, należy uznać, że występuje duże prawdopodobieństwo takiej szkody (Prezes UODO, Obowiązki administratorów związane z naruszeniami ochrony danych osobowych, wersja 1.0 , 2019).

Prezes UODO wskazuje, że administrator powinien udokumentować, że przeprowadził analizę ryzyka naruszenia praw lub wolności osób fizycznych objętych przedmiotowym naruszeniem ochrony danych osobowych (por. uzasadnienie decyzji Prezesa UODO z dnia 14 marca 2023 r., DKN.5131.45.2022).

Warto zatem, aby miała ona postać sformalizowaną, a jej kolejne etapy były odpowiednio dokumentowane, np. w postaci protokołów. W tym zakresie niewystarczające może być przedstawienie organowi nadzorczemu jedynie ogólnych dokumentów nie odnoszących się do tego konkretnego przypadku (por. uzasadnienie decyzji Prezesa UODO z dnia 1 marca 2023 r., DKN.5131.49.2021). Zgodnie ze stanowiskiem prezentowanym przez Prezesa UODO, ważne jest, aby zgodnie z zasadą rozliczalności, administrator wykazał dokonanie bilansu możliwych szkód materialnych i niematerialnych, jakie mogą wiązać się z powstaniem naruszenia dla osób, których dane dotyczą (por. uzasadnienie decyzji PUODO z dnia 7 lutego 2023 r., DKN.5131.31.2021).

Ewidencja naruszeń

Niezależnie od poziomu ryzyka związanego z wystąpieniem naruszenia, obowiązkiem administratora jest odnotowanie naruszenia w wewnętrznej ewidencji naruszeń. Ewidencję taką zobowiązany jest prowadzić każdy administrator. Art. 33 ust. 5 RODO nakłada na administratorów obowiązek dokumentowania w ewidencji wszelkich naruszeń ochrony danych osobowych, które spełniają kryteria określone w definicji zawartej w art. 4 pkt 12 RODO. Ewidencja powinna obejmować: przyczyny naruszenia, przebieg wydarzeń, zakres danych osobowych, których dotyczyło naruszenie, skutki i konsekwencje naruszenia, działania zaradcze podjęte przez administratora, uzasadnienie decyzji podjętych w odpowiedzi na naruszenie w przypadku niezgłoszenia naruszenia (Grupa Robocza Art. 29, Wytyczne dotyczące zgłaszania...).

Obowiązek zgłoszenia naruszenia organowi nadzoru

W przypadku, gdy prawdopodobieństwo zaistnienia ryzyka naruszenia praw i wolności osób fizycznych jest wyższe niż małe, pojawia się obowiązek zgłoszenia naruszenia Prezesowi UODO. Zgłoszenia takiego można dokonać za pomocą formularza dostępnego na stronie uodo.gov.pl; elektronicznie poprzez wypełnienie dedykowanego formularza dostępnego bezpośrednio na platformie biznes.gov.pl; poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP: UODO/SkrytkaESP, za pomocą pisma ogólnego dostępnego na platformie biznes.gov.pl lub tradycyjną pocztą na adres UODO. Administrator jest zobowiązany dokonać zgłoszenia bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. „Stwierdzenie" naruszenia, od którego należy liczyć wskazany termin ma miejsce, kiedy administrator ma wystarczający stopień pewności co do tego, że miało miejsce zdarzenie, które doprowadziło do naruszenia ochrony danych. Z kolei to czy zawiadomienia dokonano bez zbędnej zwłoki, należy ustalić z uwzględnieniem w szczególności charakteru i wagi naruszenia, jego konsekwencji oraz niekorzystnych skutków dla osoby, której dane dotyczą (UODO, Obowiązki administratorów związane z naruszeniami...). Zasadniczo każde pojedyncze naruszenie należy zgłosić osobno, jednak jeśli naruszenia dotyczą tego samego rodzaju danych osobowych, których ochrona została naruszona w taki sam sposób i doszło do nich w stosunkowo krótkim odstępie czasu możliwe jest dokonanie zgłoszenia zbiorczego (Grupa Robocza Art. 29, Wytyczne dotyczące zgłaszania...).

Obowiązek zawiadomienia osoby, której dane dotyczą

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Im poważniejsze jest ryzyko naruszenia praw lub wolności podmiotu danych, tym szybciej powinno nastąpić zawiadomienie. Administrator nie ma konieczności zawiadomienia osoby, której dane dotyczą jeżeli: przed wystąpieniem naruszenia zastosował odpowiednie techniczne i organizacyjne środki w celu ochrony danych osobowych, w szczególności środki uniemożliwiające odczyt danych osobom, które nie są uprawnione do dostępu do tych danych; natychmiast po wystąpieniu naruszenia podjął działania w celu wyeliminowania prawdopodobieństwa powstania wysokiego ryzyka naruszenia

praw lub wolności osoby fizycznej lub skontaktowanie się z danymi osobami fizycznymi wymagałoby niewspółmiernie dużego wysiłku. W tym ostatnim przypadku administrator powinien jednak wydać publiczny komunikat lub zastosować inny podobny środek, aby skutecznie poinformować osoby, których dane dotyczą. Należy też pamiętać, że bez względu na wskazane wyłączenia, obowiązek zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych może zostać nałożony na administratora przez Prezesa UODO na podstawie art. 58 ust. 2 lit. e RODO.

Forma, w jakiej należy dokonać zawiadomienia osoby, której dane dotyczą nie została wprost wskazana w RODO. Wskazuje się jednak, że zawiadomienie musi zostać dostarczone adresatowi w możliwie najkrótszym czasie i powinno być sporządzone w formie, która umożliwi podmiotowi danych na wielokrotne zapoznanie się z jego treścią. (UODO, Obowiązki administratorów związane z naruszeniami...). Co za tym idzie należy wskazać, że o ile jest to możliwe, najlepszą formą dokonania zawiadomienia jest poczta elektroniczna. Zawiadomienie osoby, której dane dotyczą powinno zawierać: charakter naruszenia ochrony danych osobowych, 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 - w tym w stosownych przypadkach - środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

Wdrożenie środków zaradczych

Niezależnie od poziomu prawdopodobieństwa zaistnienia ryzyka naruszenia praw i wolności osób fizycznych administrator ma obowiązek wprowadzić środki zaradcze mające na celu zminimalizowanie ryzyka i zabezpieczenie danych osobowych. Środki te muszą odpowiadać charakterowi naruszenia i pozwalać na skuteczne wyeliminowanie podobnych zdarzeń w przyszłości. Praktyka pokazuje, że jednym z najważniejszych środków zaradczych mogą być szkolenia personelu ukierunkowane na eliminowanie zagrożeń określonego rodzaju.

W przypadku wszczęcia przez Prezesa UODO postępowania w przedmiocie stwierdzonego naruszenia ważna jest dobra współpraca z organem nadzoru, w tym w szczególności możliwie szybkie udzielanie wyczerpujących odpowiedzi na kierowane przez ten organ pytania i stosowanie się do jego zaleceń. Jak pokazuje praktyka, jest to jeden z istotnych element branych przez PUODO przy podejmowaniu o nałożeniu na administratora ewentualnej kary i ustalaniu jej wysokości.

Procedura postępowania na wypadek wystąpienia naruszenia ochrony danych

W powiązaniu ze wskazanymi obowiązkami, zaleca się aby administrator opracował i wdrożył procedurę postępowania na wypadek wystąpienia naruszenia ochrony danych. W założeniu taka procedura ma pomóc ujednolicić, usprawnić i przyśpieszyć działania w przypadku wykrycia naruszenia ochrony danych. Procedura taka powinna zawierać w szczególności: katalog zagrożeń i naruszeń, jakie mogą wystąpić w związku z przetwarzaniem danych u konkretnego administratora; opis etapów zarządzania naruszeniem, od jego wykrycia do usunięcia oraz opis postępowania personelu administratora w przypadku wystąpienia naruszenia ochrony danych. Procedura taka może stanowić element polityki ochrony danych u administratora. Należy przy tym zapewnić, by zawarte w procedurze zasady postępowania były znane pracownikom administratora, czemu mogą służyć odpowiednie szkolenia.

Autor:
Grzegorz Lubeńczuk
zespół Inspektora Ochrony Danych
doktor, radca prawny

III. Dostęp do informacji publicznej a RODO, czyli o tym, czy można powołać się na RODO odmawiając udostępnienia informacji publicznej. Analiza ogólna.

Przepisy, które regulują udostępnianie informacji publicznej to przede wszystkim ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej. Ustawa ta odnosi się przede wszystkim do art. 61 ust. 1 Konstytucji Rzeczypospolitej Polskiej, który stanowi, że: *„Obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Prawo to obejmuje również uzyskiwanie informacji o działalności organów samorządu gospodarczego i zawodowego, a także innych osób oraz jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa”*.

Pojawienie się RODO spowodowało, że często nie wiemy, czy informację możemy udostępnić, czy też nie. **Często też odmawiamy jej udostępnienia, powołując się na RODO. Ale czy słusznie?**

Jaki jest cel informacji publicznej?

Celem dostępu do informacji publicznej jest przede wszystkim realizacja prawa każdego z nas, do uzyskiwania informacji o działalności organów władzy publicznej oraz działalności osób pełniących funkcje publiczne. Dostęp do takich informacji gwarantuje nam również możliwość społecznej kontroli tego, w jaki sposób organy władzy publicznej rozporządzają środkami publicznymi.

Czym jest informacja publiczna?

Przez informację publiczną można rozumieć każdą informację dotyczącą spraw publicznych. Sprawy publiczne z kolei, to działalność organów, które realizując zadania publiczne, wykorzystują środki (mienie) publiczne. Przyjmuje się, że jeśli podmiot, nie będące organem władzy publicznej wykonuje zadania publiczne, to wystarcza, aby uznać, że jest on zobowiązany do udostepnienia informacji publicznej.

Komu przysługuje prawo dostępu do informacji publicznej?

Art. 2 powołanej powyżej ustawy o dostępie do informacji publicznej stanowi, że prawo dostępu do informacji publicznej przysługuje „każdemu". Zawarte z kolei w art. 61 naszej Konstytucji sformułowanie „Obywatel ma prawo (...)" wskazuje przede wszystkim na osobę fizyczną, a ponadto mogłoby sugerować, że dotyczy tylko obywateli państwa polskiego. Jednak międzynarodowe standardy praw człowieka, na które wielokrotnie zwracał uwagę Trybunał Konstytucyjny nakładają na państwo obowiązek gwarantowania praw i osobistych wolności wszystkim, nie tylko swoim obywatelom. Dlatego uznaje się, że dostęp do informacji publicznej ma każda osoba fizyczna, posiadająca pełną zdolność do czynności prawnych (czyli nie została ubezwłasnowolniona i jest osoba pełnoletnią), bez względu na pochodzenie (obywatelstwo). Ponadto, w orzecznictwie sądów przyjęto, że pojęcie „każdy" dotyczy także osób prawnych jak i jednostek organizacyjnych niemających osobowości prawnej, np. organizacji społecznych, a w postępowaniu o udostępnienie informacji publicznej, konieczne jest ustalenie, czy osoby działające w imieniu osoby prawnej lub innego podmiotu niebędącego osobą fizyczną są umocowane do ich reprezentowania.

Przechodząc do meritum. Czy RODO dopuszcza możliwość udostepnienia informacji publicznej, jeśli zawierają one dane osobowe?

Realizacja prawa dostępu do informacji publicznej wiąże się niejednokrotnie z ujawnieniem danych osobowych. W swojej pracy często spotkałam się z zarzutem, że RODO i ustawa o dostępie do informacji publicznej są skonfliktowane. Ale czy na pewno?

Spójrzmy na art. 1 ust. 2 ustawy o dostępie do informacji publicznej. Mówi on, że „Przepisy ustawy nie naruszają przepisów innych ustaw określających odmienne zasady i tryb dostępu do informacji będących informacjami publicznymi". Co to oznacza? **Że ustawa ta, w swym zamiarze, nie ma naruszenia przepisów o ochronie danych osobowych, a wręcz daje im pierwszeństwo stosowania.**

Samo RODO również mówi o dostępie do informacji publicznej. Wystarczy sięgnąć do art. 86, który wprost dopuszcza możliwość udostępniania danych osobowych w sprawach związanych z dostępem do informacji publicznej. Dane osobowe zawarte w dokumentach urzędowych mogą zostać ujawnione zgodnie z prawem państwa członkowskiego do informacji publicznej.

Należy zatem uznać, że RODO również nie ogranicza stosowania ustawy o dostępie do informacji publicznej, a skoro tak, nie może stanowić podstawy do odmowy udostępnienia takiej informacji.

A może ochrona prywatności?

Pochylając się jeszcze nad art. 6 ustawy o dostępie do informacji publicznej zauważymy, że użyto tam wyrażenia „w szczególności", co wskazuje na otwarty katalog informacji, które podlegają udostępnieniu. Spośród obszernej wyliczanki, to, czego najczęściej w mojej pracy dotyczą wnioski o dostęp do informacji publicznej to informacje o organach i osobach sprawujących w nich funkcje, o zawartych umowach, o zajmowanych stanowiskach czy też postępowań w związku z konkursami, zamówieniami publicznymi itp. Przy udostępnieniu informacji dotyczących powyższego, niejednokrotnie możemy znaleźć dane osobowe - również takie, które wkraczają w sferę prywatności osoby, której wnioski dotyczą. Bardzo trudne jest niekiedy wyważenie tego, kiedy ochrona prywatności powinna stać się już przesłanką do odmowy udostępnienia informacji publicznej. Uznaje się, że jeżeli informacja dotycząca danej osoby, której dotyczy wniosek, nie pozostaje w bezpośrednim związku z wykonywaną przez tę osobę funkcją, to nie jest to informacja publiczna (np. miejsce zamieszkania) i korzysta z ochrony prywatności, w tym z ochrony zagwarantowanej przepisami RODO. Warto przywołać w tym miejscu Wyrok Wojewódzkiego Sądu Administracyjnego w Krakowie z dnia 9 kwietnia 2019, sygn. akt: II SA/Kr 133/19, w którym stwierdzono, że „w razie kolizji między zasadą jawności informacji publicznych a ochroną prywatności i danych osobowych osób fizycznych, dopuszczalny będzie jedynie taki sposób udostępniania informacji publicznej, który nie naruszy dóbr chronionych (np. anonimizacja danych wrażliwych). W przypadku, gdy pomimo dokonania takiego zabiegu, możliwa będzie identyfikacja osoby, której dane dotyczą, należy odmówić udostępnienia informacji publicznej".

Podsumowanie.

Motyw 4 preambuły do RODO stanowi, że prawo do ochrony danych osobowych nie jest prawem bezwzględnym. Należy je wyważyć względem innych praw podstawowych w myśl zasady proporcjonalności. Prawo do informacji publicznej jest jednym z praw podstawowych, bowiem zostało zagwarantowane w Konstytucji. Ograniczeniami i ochroną objęte będą przede wszystkim dane osób fizycznych, które nie pełnią funkcji publicznych, lub takie dane, które wkraczają już w sferę prywatności. W ich przypadkach (gdy np. gdy ww. dane figurują na dokumentach udostępnianych w ramach dostępu do informacji publicznej) powinniśmy ograniczyć dostęp do informacji umożliwiających ich identyfikację, co w praktyce oznacza udostępnienie dokumentów odpowiednio zanonimizowanych ze względu na prywatność osób fizycznych.

Każdy przypadek jednak, czyli każdy złożony wniosek o udostepnienie informacji publicznej, należy traktować indywidualnie, mając na względzie na jednej szali prawo każdego z nas do dostępu do informacji, a na drugiej prawo do tego, by nasze dane osobowe były chronione.
A jak to z RODO bywa, to niestety nie zawsze jest łatwe.

Autor:
Justyna Cybulska
zespół Inspektora Ochrony Danych
adwokat

IV. Czy Twój telefon może stanowić zagrożenie dla twojej prywatności? Czym jest SIM swap?

Na telefonach komórkowych przechowujemy coraz więcej naszych cennych danych, tj. zdjęcia, wiadomości, kontakty, dane bankowe. Wszystko to znajduje się w naszych urządzeniach mobilnych, które niejednokrotnie, jak widzę, pozostają niezabezpieczone. Niezwykle istotne jest zrozumienie i przestrzeganie zasad bezpieczeństwa, a jednym z kluczowych aspektów jest posiadanie silnego hasła do telefonu.
Hasło do telefonu to pierwsza linia obrony przed nieuprawnionym dostępem do naszych danych, to tytułem wstępu i jednocześnie wskazaniem na potrzebę jego posiadania, dalej wpis ten zostanie poświęcony metodzie SIM swap.

Czym jest SIM swap?

SIM swap to technika, w której przestępcy przejmują kontrolę nad twoim numerem telefonu, przekierowując go na inny telefon. Aby dokonać SIM swap, atakujący muszą zdobyć pewne informacje, takie jak numer telefonu, dane osobowe i szczegóły konta ofiary. Gdy przestępcy uzyskają te informacje, mogą skontaktować się z dostawcą usług telekomunikacyjnych podając się za właściciela numeru i poprosić o przekierowanie numeru na inny telefon.

Metody wykorzystywane do dokonania SIM swap.

Istnieje kilka metod, które przestępcy mogą wykorzystać do przeprowadzenia ataku SIM swap.

Jednym z najczęstszych jest wykorzystanie socjotechniki, czyli manipulowania ofiarą w celu zdobycia jej danych. Przestępcy mogą kontaktować się z ofiarą pod różnymi pretekstami, takimi jak oszustwa podatkowe, nagrody loteryjne lub inne atrakcyjne oferty, aby uzyskać potrzebne informacje.

Inną metodą jest phishing, czyli wysyłanie fałszywych wiadomości lub e-maili, które wyglądają jak oficjalne wiadomości od dostawcy usług telekomunikacyjnych. W takich wiadomościach przestępcy proszą o potwierdzenie danych lub kliknięcie w podejrzane linki, które kierują do stron, na których ofiara ma podać swoje dane osobowe.

Jak się obronić przed SIM swap?

Obrona przed atakami SIM swap wymaga podjęcia kilku środków ostrożności. Poniżej wskazuję na kilka zaleceń, które mogą pomóc zabezpieczyć nasze dane osobowe:

1. Zachowaj ostrożność podczas udostępniania danych osobowych. Dbaj o swoją prywatność i staraj się ograniczać udostępnianie danych na niezbędne minimum.
2. Bądź czujny wobec podejrzanych wiadomości e-mail i SMS. Nie klikaj w podejrzane linki ani nie podawaj swoich danych na podejrzanych stronach internetowych. Jeśli otrzymasz dziwną dla Ciebie wiadomość, skontaktuj się bezpośrednio z dostawcą usług telekomunikacyjnych, aby zweryfikować jej autentyczność.
3. Wzmocnij zabezpieczenia swojego konta. Skorzystaj z funkcji dwuskładnikowego uwierzytelniania (2FA) oferowanej przez dostawców usług telekomunikacyjnych. Dzięki temu dodatkowemu zabezpieczeniu konieczne będzie podanie dodatkowego kodu autoryzacyjnego przy próbie zmiany numeru telefonu.
4. Regularnie sprawdzaj swoje konto telekomunikacyjne. Monitoruj swoje konto, aby zauważyć ewentualne nieprawidłowości, takie jak niespodziewane zmiany w numerze telefonu czy nieautoryzowane operacje. Jeśli zauważysz coś podejrzanego, natychmiast skontaktuj się z dostawcą usług telekomunikacyjnych.

Co robić w przypadku wycieku danych?

Jeśli podejrzewasz, że padłeś ofiarą SIM swap i doszło do wycieku Twoich danych osobowych, natychmiast podejmij następujące kroki:

1. Skontaktuj się z dostawcą usług telekomunikacyjnych. Powiadom dostawcę o sytuacji, zabezpiecz swoje konto oraz przywróć oryginalny numer telefonu.
2. Zmień swoje hasła. Zmiana haseł do wszystkich swoich kont online (np. poczty elektronicznej, mediów społecznościowych, bankowości internetowej) może pomóc w ochronie przed dalszymi naruszeniami prywatności.
3. Monitoruj swoje konta. Regularnie sprawdzaj swoje konta bankowe, karty kredytowe i inne konta finansowe, aby wykryć nieautoryzowane transakcje. Powiadom odpowiednie instytucje finansowe o potencjalnym wycieku danych.

Pamiętaj!

Bezpieczeństwo twoich danych zaczyna się od Ciebie samego!

Autor:
Justyna Cybulska
zespół Inspektora Ochrony Danych
adwokat

JUSTYNA JABŁONKA

KANCELARIA WYRZYKOWSCY

Inspektor Ochrony Danych,
adw. Justyna Jabłonka

www.justynajablonka.pl
www. kancelariawyrzykowscy.pl

BLOG dla JST:
https://kancelariawyrzykowscy.pl/pl/blog-jst/
FB:
https://www.facebook.com/kancelariawyrzykowscy