Image not found or type unknown

Wyciek danych osobowych z MyDr: obowiązki lekarza - administratora danych pacjentów

Administrator musi zgłosić wyciek, do którego doszło w podmiocie przetwarzającym.

W związku z doniesieniami medialnymi dotyczącymi wycieku danych osobowych niemal 19 mln Polaków u dostawcy **systemu Elektronicznej Dokumentacji Medycznej MyDr** Prezes Urzędu Ochrony Danych Osobowych przypomina administratorom danych osobowych, którzy powierzyli przetwarzanie danych osobowych firmie MyDr o obowiązku dokonania analizy pod kątem ryzyka naruszenia praw lub wolności osób fizycznych niezbędnej do oceny, czy doszło do naruszenia ochrony danych osobowych skutkującego koniecznością zawiadomienia Prezesa UODO oraz osób, których dotyczy naruszenie.

Zgodnie z art. 33 ust. 1 RODO, w przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

Przypominamy, że w sytuacji gdy naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, zgodnie z art. 34 ust. 1 i 2 w zw. z art. 33 ust. 3 rozporządzenia 2016/679, czyli RODO administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie takie co najmniej powinno:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych (przykładowo w przypadku naruszenia poufności danych w zakresie imienia i nazwiska wraz z nr PESEL, administrator może wskazać na ryzyko wyłudzenia przez osoby trzecie pożyczek na dane osób fizycznych, natomiast w przypadku naruszenia poufności danych dotyczących zdrowia może wskazać na ryzyko dyskryminacji, ostracyzmu społecznego czy też naruszenia dóbr osobistych osób, których incydent dotyczy);

d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków (przykładowo: w przypadku naruszenia poufności danych w zakresie imienia i nazwiska wraz z nr PESEL administrator może zarekomendować osobom fizycznym zastrzeżenie nr PESEL, z kolei w przypadku naruszenia poufności danych dotyczących zdrowia administrator może zarekomendować użycie środków ochrony dóbr osobistych wskazanych w kodeksie cywilnym oraz kodeksie postępowania cywilnego, czy też może zaproponować skorzystanie ze wsparcia psychologicznego w sytuacjach silnego stresu lub niepokoju).

Informacje, o których mowa powyżej, można przekazać do tut. Urzędu przy pomocy dedykowanego formularza zgłaszania naruszeń ochrony danych osobowych, który dostępny jest pod adresem https://uodo.gov.pl/pl/501/2278.

Więcej informacji na temat zgłaszania naruszeń ochrony danych osobowych organowi

nadzorczemu oraz zawiadamiania osób, których dane dotyczą, o naruszeniu ochrony danych osobowych, dostępnych jest w Poradniku UODO dotyczącym naruszeń ochrony danych osobowych, który znajdą Państwo pod adresem https://uodo.gov.pl/pl/138/3561.

Wyciek danych – co dalej?

W związku z licznymi doniesieniami medialnymi dotyczącymi incydentu cyberbezpieczeństwa i możliwego wycieku danych w systemach **firmy MyDr** pragniemy poinformować, za Ministerstwem Cyfryzacji, że o zdarzeniu zostały poinformowane odpowiednie służby, które obecnie prowadzą działania mające na celu ustalenie jego okoliczności.
Jednocześnie informujemy, że obowiązek powiadomienia osób, dotkniętych wyciekiem danych, spoczywa na administratorach, którzy korzystali z usług spółki MyDr.
Przypominamy jednak zasady, jakich należy przestrzegać, gdy doszło do naruszenia naszych danych oraz podstawowe zasady związane z ochroną danych osobowych, których warto przestrzegać na co dzień.

Jak się zabezpieczyć, gdy wiesz, że Twoje dane wyciekły?

Atak hakera, zgubiona korespondencja, niezabezpieczone dane na serwerze - to sytuacje, w przypadku których osoby do tego nieuprawnione wchodzą (albo potencjalnie jest to możliwe) w posiadanie Twoich danych osobowych. Niestety, nie masz na to wpływu. W sytuacji, gdy administrator uzna, że istnieje ryzyko wykorzystania Twoich danych i powiadomi Cię o zaistniałym incydencie, podejmij działania, by zminimalizować ewentualne negatywne konsekwencje wykorzystania danych.
Takimi działaniami może być np. zastrzeżenie nr PESEL oraz zachowanie jeszcze większej ostrożności podczas podawania danych przez internet lub telefon, by np. osoby o nieuczciwych zamiarach nie uzyskały np. dodatkowych danych, które ułatwią im np. tzw. kradzież tożsamości.
Dokładnie analizuj więc kierowane do Ciebie komunikaty, zawarte np. w wiadomościach SMS, e-mail, by uniknąć np. ataku phishingowego, którego celem może być wyłudzenie właśnie dodatkowych danych czy uzyskanie dostępu do internetowych systemów bankowych bądź innych usług, z których korzystasz.

W jakich sytuacjach możesz zwrócić się do Prezesa Urzędu Ochrony Danych Osobowych?

Jeżeli przypuszczasz, że firma czy instytucja przetwarza Twoje dane bez podstawy prawnej, nie informuje skąd ma dane osobowe i w jakim celu je przetwarza, to w pierwszej kolejności zwróć się do niej, z żądaniem realizacji swoich praw, np. wyjaśnienia zasad na jakich Twoje dane są przetwarzane. Gdy nie otrzymasz odpowiedzi, pozyskane informacje są niewystarczające lub niepełne albo gdy administrator nie respektuje Twojego żądania dotyczącego np. wycofania zgody na przetwarzanie danych (jeżeli to zgoda była podstawą przetwarzania), czy sprzeciwu wobec przetwarzania Twoich danych, to możesz złożyć skargę do Prezesa UODO. W pierwszej kolejności zwracaj się zatem o realizację Twoich praw do administratora - podmiotu przetwarzającego Twoje dane. O ile Twoje żądania nie będą respektowane, zignorowane czy po części jedynie wypełnione możesz zwrócić się następnie do Prezesa UODO o ich wyegzekwowanie.
Składając skargę indywidualną, podaj swoje dane, opisz sprawę i określ jakich działań oczekujesz od Prezesa UODO, czyli np. wskaż, by organ nakazał wykonanie Twoich praw, poprzez usunięcie danych czy spełnienie obowiązku informacyjnego. Konieczne jest także wskazanie administratora, który dopuścił się naruszenia Twoich praw. Trzeba więc podać np. nazwę firmy, czy instytucji lub imię i nazwisko osoby oraz adres siedziby przetwarzających Twoje dane osobowe.
Jeżeli działanie administratora nie dotyczy Twoich danych, ale masz podejrzenie, że narusza ono ogólne zasady przetwarzania danych, możesz o tym zawiadomić UODO. Organ nadzorczy może wówczas przeprowadzić postępowanie z urzędu w celu wyjaśnienia, czy faktycznie zaszły nieprawidłowości. W takiej sytuacji nie występujesz w charakterze strony, jak to ma miejsce w przypadku skargi indywidualnej, która związana jest z praktyką naruszającą Twoje prawa. Dlatego w przypadku, gdy Prezes UODO podejmie działania z urzędu, nie będziesz informowany o etapach takiego postępowania.

Czy Prezes UODO może ustalić sprawcę naruszenia, gdy masz np. tylko jego numer telefonu?

Organ nadzoru nie zawsze ma możliwości prawne czy techniczne by ustalić tożsamość niedookreślonego administratora. Samo wskazanie np. numeru telefonu, z którego wykonywane jest połączenie, niezidentyfikowanego serwera, gdzie są np. ujawnione Twoje dane czy przedstawienie dokumentów zawierających dane bez wskazania źródła ich pochodzenia to za mało.

Pamiętaj, że Prezes UODO nie jest organem ścigania i nie ma w związku z tym takich kompetencji jak Policja, czy Prokuratura. Działalność Prezesa UODO ma na celu zapewnienie, by wskazany administrator przetwarzał dane zgodnie z prawem. Dlatego, gdy składasz skargę indywidualną konieczne jest precyzyjne wskazanie jakiego podmiotu ona dotyczy, by było możliwe wszczęcie postępowania administracyjnego i merytoryczne rozstrzygniecie sprawy poprzez wydanie decyzji administracyjne.

Wyciekły moje dane. Czy Prezes UODO może ukarać administratora?

Decyzję o nałożeniu kary finansowej na podmiot podejmuje Prezes UODO, analizując indywidualnie każdy przypadek. Nałożenie kary nie następuje na wniosek.

Kary finansowe to tylko jeden z instrumentów oddziaływania, jakimi dysponuje Prezes UODO, by zapewnić przestrzeganie ogólnego rozporządzenia o ochronie danych osobowych. RODO zawiera bowiem całą gamę różnych rozwiązań, które służą wzmocnieniu ochrony danych osobowych, osób, których dane są przetwarzane. W przypadku stwierdzenia naruszenia przepisów może to być m.in.: wydane ostrzeżenie odnoszące się do planowanych procesów przetwarzania, udzielone upomnienie w związku z uchybieniem o niewielkim charakterze, wydany nakaz dostosowania określonych działań do obowiązujących przepisów. Prezes UODO korzysta w pierwszej kolejności m.in. z tych rozwiązań. Kary są ostatecznością i są nakładane o ile wymagają tego okoliczności indywidulanego przypadku. Decyzje, mocą których kary takie są nakładane są poprzedzone bardzo dokładną i wnikliwą analizą zaistniałych okoliczności i wynikającą z nich konieczność nałożenia kary oraz na jej wysokość.

Przy wymierzaniu kary finansowej, Prezes UODO musi brać pod uwagę co najmniej 11 różnych czynników. Są to m.in.: charakter, waga i czas trwania naruszenia, to czy miało ono charakter umyślny, czy nieumyślny, warunki, w jakich do niego doszło, liczba poszkodowanych osób, kategorie przetwarzanych danych, rozmiar poniesionej przez nie szkody. A także czy jest to pierwsze czy kolejne naruszenie , jak zachował się administrator (np. czy sam zgłosił wyciek danych oraz – o ile to konieczne – poinformował o tym osoby poszkodowane), wszelkie inne czynniki obciążające lub łagodzące zaistniałe w indywidulanym przypadku.

Finansową karę administracyjną z tytułu naruszenia przepisów o ochronie danych osobowych Prezes UODO nakłada w drodze decyzji administracyjnej po przeprowadzeniu postępowania administracyjnego w sprawie, analizując każdy przypadek indywidualnie.

Jak chronić swoje dane osobowe?

- Uważaj na to co i komu udostępnisz o sobie w Internecie.

W XXI w., w szczególności media społecznościowe mogą być kopalnią wiedzy o Tobie, o Twoim stanie majątkowym, miejscu pracy, wydarzeniach z Twojego codziennego życia. Zdarza się, że nadmiernie dzielisz się informacjami na swój temat. Przez to Internet jest źródłem wiedzy także o Twoich poglądach, zachowaniach konsumenckich, zainteresowaniach. Dane te są cenne nie tylko dla działów marketingu różnych firm, po to by na Twoich zachowaniach w sieci oprzeć kierowaną ofertę, ale niekiedy i dla przestępców. Szczególnie gdy profil, który Ciebie dotyczy jest w pełni publiczny, możesz być narażony na użycie Twoich danych bez Twojej wiedzy i przyzwolenia niezgodnie z celami, dla których dane udostępniłeś.

- Nie zostawiaj dokumentów w zastaw

Podczas urlopu, wykonując różnego rodzaju aktywności, wypożyczając sprzęt, np. kajaki, łódki, czy narty albo łyżwy, nie oddawaj w zastaw dowodu osobistego, paszportu, prawa jazdy, legitymacji

szkolnej lub studenckiej. Warto pamiętać, że zgodnie z prawem zatrzymywanie dowodu osobistego bez podstawy prawnej jest karane, natomiast nie wszystkie dane osobowe zawarte we wskazanych dokumentach są niezbędne dla realizacji celu wypożyczenia sprzętu. Utrata kontroli nad dowodem osobistym naraża Cię na posłużenie się tym dokumentem bez Twojej wiedzy i woli, co z kolei stwarza niebezpieczeństwo kradzieży tożsamości. Osoby dysponujące kompletem informacji o Tobie, czy kopią Twojego dokumentu tożsamości, mogą podszyć się pod Ciebie i np. dokonywać na Twoją szkodę różnych transakcji, takich jak chociażby zaciągnięcie kredytu w banku czy wypożyczenie drogiego sprzętu i niezwrócenie go (np. samochodu). Nieodpowiedzialne zachowanie, o którym mowa – utrata kontroli nad identyfikującym Cię dokumentem, zwłaszcza potwierdzającym Twoją tożsamość – naraża Cię na wykorzystanie Twojego wizerunku oraz innych danych osobowych w celu wyrządzenia Ci szkody majątkowej lub osobistej. Osoby, które przejmą taki dokument mogą, korzystając z Twojej tożsamości, zawrzeć w Twoim imieniu różnego rodzaju umowy, np. z zakresu usług telekomunikacyjnych, z dalszymi tego faktu obciążającymi Ciebie konsekwencjami.
Co do zasady nie powinieneś się godzić na kopiowanie Twojego dokumentu tożsamości. Tylko w niektórych sytuacjach jest to wyjątkowo dopuszczalne, gdy pozwalają na to przepisy. Gdy administrator domaga się kopii np. Twojego dowodu osobistego, poproś, aby wskazał Ci podstawę prawną, która nakłada na niego obowiązek takiego działania.

- Nie podawaj danych przez telefon

Unikaj przekazywania danych telefonicznie – szczególnie, gdy to nie Ty inicjujesz rozmowę, ale ktoś dzwoni do Ciebie. Udostępnianie danych na odległość obarczone jest ryzykiem, brakiem pewności co do tego komu faktycznie dane są przekazane. Nie daj się zaskoczyć, sprowokować do udostępniania danych wbrew Twojej woli, dla nieznanych, niewyjaśnionych przez rozmówcę celów. Upewnij się, komu faktycznie udostępniasz dane w trakcie rozmowy telefonicznej, a jeżeli trzeba zweryfikuj kontakt, np. oddzwaniając i sprawdzając, czy dany numer i osoba faktycznie reprezentuje podmiot, na który się powołała.

- Uważaj na różne formularze, poprzez które udostępniasz dane

Zachowaj rozwagę przy wypełnianiu i podpisywaniu różnego rodzaju ankiet, formularzy czy umów. Zastanów się czy faktycznie chcesz założyć kartę lojalnościową w sklepie, by mieć rabaty lub dodatkowe promocje. W takich sytuacjach podajesz sklepom imię, nazwisko, adres zamieszkania, datę urodzenia, adres e-mail, numer telefonu, a w zamian otrzymujesz promocje, bony rabatowe, dodatkowe upominki przy zakupach. Ale czy rzeczywiście warto?
Należy pamiętać, że administrator musi spełnić wobec Ciebie obowiązek informacyjny, czyli przekazać Ci niezbędne informacje na swój temat, podając m.in. swoją tożsamość, dane kontaktowe oraz dane kontaktowe swojego inspektora danych osobowych (o ile go wyznaczył), a także cel i podstawę prawną przetwarzania danych.
Nie podawaj wszelkich danych, które pozwalają na pełną identyfikację, jeżeli w danej sytuacji nie jest to konieczne, danych nadmiarowych. Jeśli musisz skorzystać z danej usługi, to podaj tylko dane niezbędne do jej wykonania – dobrze przemyśl przekazanie tych, których przekazanie oznaczone jest jako opcjonalne.
Zanim zaznaczysz wszystkie zgody, upewnij się czego dotyczą. Zwróć uwagę czy w formularzu zgody nie są zaznaczone domyślnie. Zgodnie z prawem nie powinno tak być. Dokładnie też czytaj, czego dotyczą klauzule zgód. W przypadku wątpliwości, zadawaj pytania administratorom. Powinni Cię poinformować o okresie przez jaki dane będą przetwarzane oraz o przysługujących Ci prawach, w tym dostępu do danych, ich sprostowania, usunięcia czy wniesienia sprzeciwu wobec przetwarzania, a także, czy Twoje dane będą komuś innemu (innym odbiorcom) przekazywane.
Pamiętaj, że wyrabiając kartę lojalnościową często udzielasz zgód na wykorzystywanie danych w celach marketingowych nie tylko administratora, ale i jego partnerów biznesowych. O ile możesz, zweryfikuj, kim oni są, jakie to są firmy. Zgody na marketing „cudzy” powinny być

nieobowiązkowe, powinna być Ci pozostawiona możliwość wyboru co do tego, czy taką zgodę wyrazisz.
Administrator powinien Ci zapewnić, by możliwość wycofania zgody była równie łatwa, jak jej udzielenie oraz powinieneś być poinformowany o prawie do cofnięcia zgody nim ją wyrazisz.

- Nie wyrzucaj danych na śmietnik, dopóki ich nie zniszczysz

Wszelkie dokumenty z Twoimi danymi, to kolejne źródło wiedzy o Tobie, zwłaszcza gdy zawierają one wiele różnych informacji umożliwiających wyciągania wniosków na Twój temat, np. ustalenie tego, gdzie pracujesz, ile zarabiasz, kiedy nie ma Ciebie w domu, ile masz dzieci, jak drogie robisz zakupy. Dlatego też - zanim wyrzucisz dokumenty do kosza – należy je zniszczyć (np. faktury, rachunki), zapiski, naklejki na opakowaniach od korespondencji czy po dostarczonych towarach, w sposób uniemożliwiający odtworzenie zawartych w nich danych osobowych.

- Usuwaj trwale dane z nośników

Ogrom danych o Tobie może znajdować się na Twoich starych dyskach twardych, kartach pamięci, pendrive’ach czy innych nośnikach. Zwróć uwagę, że coraz więcej informacji na Twój temat jest zapisanych w komputerach, smartfonach, aparatach fotograficznych czy tabletach. Zanim się pozbędziesz takich urządzeń lub nośników, trwale usuń z nich dane. Jednak zwykłe ich skasowanie nie będzie wystarczające, gdyż wiele danych da się odzyskać. Dlatego zanim wyrzucisz nośnik albo go sprzedasz, usuń z niego dane, korzystając przy tym z odpowiedniego do tego oprogramowania. Warto też przywrócić ustawienia fabryczne urządzenia, aby nie było w nim zapamiętanych loginów i haseł do różnych usług i aplikacji, z jakich korzystałeś, a zwłaszcza z takich, z których nadal korzystasz.

- Używaj programów chroniących komputer

Używaj oprogramowania chroniącego komputer i urządzenia mobilne przed niepożądanymi działaniami z zewnątrz, np. złośliwego oprogramowania. Oprócz popularnych programów antywirusowych przydatne mogą być również te, które zabezpieczą przed ingerencją z zewnątrz tzw. firewall.

- Bądź czujny w sieci

Nie odpowiadaj na maile od osób, których nie znasz np. tzw. spamerów, zwłaszcza gdy domagają się podania jakichś informacji o tobie czy namawiają do kliknięcia w przesłany link lub otwarcia przesłanego załącznika, sugerują zmianę identyfikatora i hasła. Zachowaj ostrożność także przy korzystaniu z usług bankowości elektronicznej i dokonywaniu zakupów przez Internet. Zwracaj uwagę czy aby na pewno logujesz się do serwisu bankowości internetowej ze strony banku, która ma certyfikat SSL (widoczny w pasku adresu przeglądarki). Weryfikuj sklepy, w których chcesz coś kupić: czy w ogóle istnieją, czy i jakie mają opinie, czy są to podmioty zidentyfikowane, gdzie mają siedzibę, czy podany jest kontakt z ich właścicielem i czy kontakt ten nie jest ograniczony tylko do elektronicznego. Jeśli masz wątpliwości co do bezpieczeństwa Twoich danych zastanów się czy koniecznie musisz dokonać zakupów u tego sprzedawcy. Weryfikuj regulaminy i polityki prywatności – unikaj sprzedawców nieprzedstawiających takich dokumentów czy też prezentujących w nich postanowienia zbyt ogólne, niejasno czy nieprecyzyjnie brzmiące, sformułowane niepoprawnie gramatycznie czy językowo, może to bowiem oznaczać, że są to podmioty niepodlegające polskiemu czy europejskiemu prawu.

- Zmieniaj hasła

Zazwyczaj to głównie pracodawcy wymagają od pracowników zmiany haseł co pewien czas, by chronić nie tylko dane osobowe, ale i tajemnice firm. Taką zasadę warto też wdrożyć w życiu prywatnym i okresowo zmieniać hasła dostępu do swojego komputera, do poczty elektronicznej, systemów bankowości elektronicznej, ale nawet sklepów internetowych, w których -masz konto użytkownika. Staraj się przy tym korzystać z różnych haseł. Dobrze jest, aby nie miały one nic wspólnego z Twoimi życiem osobistym, miejscem zamieszkania, Twoim imieniem i nazwiskiem, datą urodzin, imionami Twoich bliskich czy Twoich zwierząt itp., tj. informacjami, które łatwo można skojarzyć z Tobą obserwując Twoje zachowania w sieci, czy połączyć z innymi informacjami o Tobie.

Zapraszamy też do zapoznania się z materiałem dotyczącym praw osób, których dane dotyczą: Materiały edukacyjne - UODO.

Zachęcamy też do zapoznania się z zasadami bezpieczeństwa i higieny cyfrowej dostępnymi na stronie Ministerstwa Cyfryzajj w poradniku Higiena cyfrowa i cyberbezpieczeństwo.

Źródło: UODO