**Zawiadomienie o naruszeniu bezpieczeństwa danych osobowych**

Prezydent Wrocławia, działając jako administrator danych osobowych, zawiadamia, że w związku z nieprawidłowym działaniem mechanizmu pamięci podręcznej systemu Nasz Wrocław (cache serwera) zachodzi ryzyko, że z danymi zapisanymi w profilu użytkownika 7 (siedmiu) nieidentyfikowalnych użytkowników systemu Nasz Wrocław, którzy logowali się do niego pomiędzy piątkiem 17 listopada godz. 22:48 a sobotą 18 listopada 2023 r. godz. 11:27 mogli zapoznać się inni użytkownicy systemu, którzy logowali się do niego w tym samym czasie.

Po wykonaniu analizy ryzyka dotyczącej praw i wolności osób potencjalnie dotkniętych naruszeniem, w związku w wynikiem tej analizy, administrator danych osobowych podjął decyzję o zgłoszeniu naruszenia Prezesowi Urzędu Ochrony Danych Osobowych. Zgłoszenie zostało dokonane w dniu 22 listopada 2023 r.

W związku z zakresem potencjalnie ujawnionych danych (imię, nazwisko, numer PESEL, adres, adres poczty elektronicznej, opcjonalnie numer telefonu) administrator danych ocenił ryzyko jako wysokie wobec czego niniejszym komunikatem realizuje swoje obowiązki wynikające z art. 34 RODO.

W Urzędzie Miejskim Wrocławia do ochrony danych osobowych przykładamy szczególną wagę dlatego też administrator danych osobowych uznał za konieczne wskazać Państwu potencjalne ryzyka związane z niniejszym incydentem, których nie można całkowicie wykluczyć w związku z możliwością zapoznanie się przez osoby postronne (innych użytkowników systemu Nasz Wrocław) z danymi zgromadzonymi w Państwa profilu.

Potencjalne możliwe konsekwencje oraz informacje, jak się przed nimi ustrzec:

1. wykorzystanie danych osobowych pozyskanych z centralnej bazy danych ksiąg wieczystych, w celu podszycia się pod osobę fizyczną (tzw. „kradzież tożsamości”), a w konsekwencji tego:
2. uzyskanie przez osoby trzecie kredytów na szkodę osoby, której dane pozyskano w instytucjach pozabankowych, które umożliwiają realizację procedury uzyskania kredytu przez Internet lub telefonicznie i wymagają jedynie podania podstawowych danych identyfikacyjnych bez okazywania innych dokumentów potwierdzających tożsamość.

**Środek zaradczy:** weryfikacja danych w systemie BIK (Biurze Informacji Kredytowej);

1. wygenerowanie innego niż kredyt zadłużenia w przypadku nieopłacania przez nieuczciwe osoby nabytych przez nie usług lub towarów, np. tytułem zakupu usług telewizji kablowej, telefonicznych, Internetu, wynajęcia samochodu, wynajęcia pokoju hotelowego lub mieszkania.

**Środek zaradczy:**obserwacja korespondencji, która może wzbudzić wątpliwości (np. korespondencja z przygotowanymi do podpisu umowami, informacjami marketingowymi, powiadomieniami o braku terminowego uiszczenia należności) od firm telekomunikacyjnych, telewizji kablowych lub innych podmiotów, z którymi nie zawierano umów;

1. przypisanie oszustwa w postaci wyłudzenia odszkodowania od ubezpieczyciela. Istnieją firmy ubezpieczeniowe, które wydają polisy ubezpieczeniowe, a także wypłacają odszkodowania z ubezpieczenia bez weryfikacji dokumentów tożsamości ubezpieczonego.

**Środek zaradczy:** obserwacja przychodzącej korespondencji od firm ubezpieczeniowych, a w razie wątpliwości kontakt z firmą w celu wyjaśnienia niezgodności;

1. ograniczenie możliwości korzystania z praw obywatelskich i usług kierowanych do ogółu obywateli (np. głosowanie w ramach budżetu obywatelskiego, internetowa rejestracja wizyt w urzędach) lub ujawnienie danych z centralnych rejestrów publicznych w związku z wykorzystaniem numeru PESEL, w tym celu.

**Środek zaradczy:** uważność na wszelkie ograniczenia podczas elektronicznych rejestracji (np. komunikat o tym, że nie można założyć konta, bo już istnieje) lub prób korzystania z usług. Ograniczenia lub nieprawidłowości te mogą być sygnałem, że osoba niepowołana korzystała z możliwości elektronicznej obsługi w kontaktach z urzędami lub używając danych skorzystała z oferowanych usług. W przypadku stwierdzenia anomalii wskazany jest kontakt z właściwym urzędem;

1. uzyskanie dostępu do świadczeń z opieki zdrowotnej oraz do danych o stanie zdrowia w oparciu o numer PESEL. Potwierdzonym niebezpieczeństwem, które może dotyczyć tej sytuacji jest zmiana przypisania pacjenta do innej przychodni NFZ oraz innego lekarza pierwszego kontaktu.

**Środek zaradczy:** śledzenie historii medycznej np. na rządowym portalu [https://pacjent.gov.pl](https://pacjent.gov.pl/). Przy najbliższym kontakcie z pracownikiem przychodni, wskazane jest zwrócenie uwagi na wszelkie informacje w zakresie zmian
w przypisaniu do lekarza pierwszego kontaktu.

1. dyskomfort z powodu tego, że potencjalnie z informacjami o osobie mogła zapoznać się osoba postronna.

**Środki zaradcze,** które można zastosować to:

* zachowanie ostrożności przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem Internetu czy telefonu;
* zgłoszenie możliwości „kradzieży tożsamości” właściwym organom w celu zapobieżenia wszelkim negatywnym skutkom zdarzenia;
* w przypadku stwierdzenia próby dyskryminacji, szantażu, zgłoszenie tego faktu właściwym organom;
* skorzystanie ze środków ochrony dóbr osobistych wskazanych w przepisach ustawy Kodeks cywilny;
* zwracanie uwagi na wszelkie nieprawidłowości lub nietypowe reakcje systemów informatycznych ponieważ kradzież tożsamości może dotyczyć również sfery funkcjonowania osoby w Internecie (media społecznościowe, fora dyskusyjne, blogi, sklepy, platformy aukcyjne, usługi podmiotów publicznych).

Źródłem dodatkowych informacji w zakresie przeciwdziałania oraz reakcji na niepożądane zdarzenia – naruszenia ochrony danych osobowych – są również informacje publikowane przez Urząd Ochrony Danych Osobowych.

<https://uodo.gov.pl/pl/138/1222> (Co zrobić w przypadku kradzieży tożsamości?)

<https://www.uodo.gov.pl/pl/138/1267> (Warto wiedzieć, jak minimalizować ryzyko kradzieży tożsamości)

<https://uodo.gov.pl/pl/138/1221> (Jak chronić swoje dane osobowe?)

<https://www.uodo.gov.pl/pl/file/2463> (Chroń swoje dane)

W przypadku jakichkolwiek pytań, wątpliwości w związku zaistniałym zdarzeniem,
w szczególności o sposobach zapobiegania jego negatywnym skutkom, prosimy o kontakt z inspektorem ochrony danych Urzędu Miejskiego Wrocławia na dane jak poniżej:

Sebastian Sobecki, Biuro ds. Bezpieczeństwa Informacji, ul. Gabrieli Zapolskiej 4,
pok. 512, 50-032 Wrocław, e-mail: iod@um.wroc.pl, tel.: +48 71 777 77 24.

Prawdopodobieństwo wystąpienia poniżej wskazanych konsekwencji dla ochrony danych osobowych w związku z wystąpieniem niniejszego incydentu jest ograniczone ze względu na poniższe okoliczności:

* jest mało prawdopodobne, by osoba, która zupełnie przypadkowo zapoznała się nie ze swoimi danymi zgromadzonymi w profilu użytkownika Nasz Wrocław, skoro motywem jej działania nie było przestępcze zamierzenie, a chęć zalogowania się na własne konto, wykorzystała te dane w celach niezgodnych z prawem,
* osoby, które zgłosiły do administratora danych wystąpienie zdarzenia przedstawiały jego przebieg „po swojej stronie” w taki sposób, że prawdopodobieństwo trwałego zachowania nieprawidłowo udostępnionych danych jest nikłe,
* nieprawidłowe działanie systemu trwało przez 12 godzin i miało miejsce wyłącznie w godzinach nocnych i porannych weekendu,

Administrator danych osobowych zapewnia, że dokłada wszelkich starań, aby Państwa dane były przetwarzane w sposób gwarantujący ich bezpieczeństwo. Informujemy, że w wyniku analizy zaistniałego zdarzenia zostały zrealizowane środki korekcyjne i zostaną wdrożone dalsze działania zapobiegawcze i korygujące.

Ponadto w ramach działań mających na celu zapobieganie ewentualnym negatywnym konsekwencjom tego (i tego typu zdarzeń w których dochodzi do ujawnienia numeru PESEL) administrator danych przekazuje Państwu poniższą informację.

Od dnia 17 listopada 2023 r. została uruchomiona usługa "Zastrzeż PESEL".

Usługa ta umożliwi obywatelom:

* zastrzec swój numer PESEL,
* cofnąć zastrzeganie numeru PESEL,
* ustawić automatyczne zastrzeganie numeru PESEL,
* sprawdzić historię weryfikacji numeru PESEL przez instytucje, firmy i osoby prywatne,
* przeglądać historię zmian statusu numeru PESEL.

Działania te zostaną odnotowane w Rejestrze Zastrzeżonych Numerów PESEL.

Celem usługi jest ograniczenie wyłudzania pieniędzy poprzez zaciąganie zobowiązań finansowych na inną osobę, m.in. umów kredytów i pożyczek, czy sprzedaży nieruchomości bez wiedzy i zgody właściciela i zjawiska tzw. SIM swappingu, czyli wyrobienia duplikatu karty SIM, która może być potem użyta do autoryzowania transakcji wykonanych przez złodzieja w instytucji finansowej.

Reasumując „Zastrzeż PESEL” to usługa, po skorzystaniu z której nikt np. nie weźmie kredytu, ani nie kupi sprzętów na raty wykorzystując zastrzeżony numer.

Jak zastrzec swój PESEL?

Swój numer PESEL będzie można zastrzec na kilka sposobów:

* przez stronę <https://www.mobywatel.gov.pl/twoje-dane/rzp-pesel> *(już działa)*,
* w dowolnym urzędzie gminy (również poprzez pełnomocników, opiekunów prawnych, kuratorów) *(już działa)*,
* w aplikacji mobilnej mObywatel *(od 18 grudnia 2023 r.)*,
* w placówce bankowej lub na poczcie *(od czerwca 2024 r.)*,

Usługa będzie w pełni funkcjonalna (w odniesieniu do banków i telekomów) od czerwca 2024 r., choć niektóre instytucje planują wdrożenie jej już od początku 2024 r.