Zawiadomienie o naruszeniu bezpieczeństwa danych osobowych

Prezydent Wrocławia, w imieniu którego działa Geodeta Miejski - w zakresie realizacji zadań wynikających z prawa geodezyjnego i kartograficznego, zastrzeżonych dla starosty zgodnie z art. 7d ustawy prawo geodezyjne i kartograficzne, działając jako Administrator Danych Osobowych, zawiadamia, że dane osobowe osób fizycznych znajdujących się na dokumentach stanowiących dowody zmian w operacie ewidencyjnym w latach 2013-2015 są przetwarzane przez Podmiot nieuprawniony. Podmiot, który realizował zamówienie publiczne polegające na skanowaniu dokumentacji ze wskazanego okresu, mimo iż stracił uprawnienia do przetwarzania danych osobowych, z wiedzy Administratora jest dalej w ich posiadaniu oraz przetwarza je bezpodstawnie.

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 11 grudnia 2023 r.

W związku z zakresem powierzonych w ramach umowy danych, to jest dane podmiotów zawarte w dokumentach stanowiących podstawię zmian w operacie ewidencyjnym:

1. imię i Nazwisko Osoby Fizycznej (imiona);
2. numer PESEL Osoby Fizycznej;
3. adres Osoby Fizycznej;
4. adres do korespondencji Osoby Fizycznej;
5. imiona rodziców Osoby Fizycznej;
6. oznaczenie dokumentu stwierdzającego tożsamość Osoby Fizycznej;
7. płeć Osoby Fizycznej;
8. obywatelstwo Osoby Fizycznej;
9. informacja czy dana Osoba Fizyczna jest cudzoziemcem;
10. nazwa Instytucji;
11. adres do korespondencji Instytucji;
12. adres Instytucji;
13. numer REGON;
14. numer NIP;
15. informacja o posiadanych nieruchomościach na terenie miasta Wrocławia wraz z numerem Księgi Wieczystej prowadzonej dla nieruchomości;
16. wszelkie inne informacje, zawarte w dokumentach stanowiących dowody zmian w operacie ewidencyjnym, w szczególności w aktach notarialnych, orzeczeniach

sądowych, złożonych wnioskach na które Zamawiający nie ma wpływu,

Administrator Danych ocenił ryzyko jako wysokie wobec czego niniejszym komunikatem realizuje swoje obowiązki wynikające z art. 34 RODO.

Administrator Danych Osobowych do ochrony danych osobowych przykłada szczególną wagę dlatego też uznał za konieczne wskazać Państwu potencjalne ryzyka związane z niniejszym incydentem.

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

1. wykorzystanie danych osobowych pozyskanych z dokumentów stanowiących dowody zmian w operacie ewidencyjnym oraz centralnej bazy danych ksiąg wieczystych, w celu podszycia się pod osobę fizyczną (tzw. "kradzież tożsamości"), a w konsekwencji tego:
   1) 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);
   2) 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;
   3) 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;
   4) 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;

5) 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 pacjent.gov. Przy najbliższym kontakcie z pracownikiem przychodni, wskazane jest zwrócenie uwagi na wszelkie informacje w zakresie zmian w przypisaniu do lekarza pierwszego kontaktu.

2. dyskomfort z powodu tego, że potencjalnie z informacjami o osobie mogła zapoznać się osoba postronna.
   1) **Środki zaradcze**, które można zastosować to:
      a) zachowanie ostrożności przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem Internetu czy telefonu;
      b) zgłoszenie możliwości "kradzieży tożsamości" właściwym organom w celu zapobieżenia wszelkim negatywnym skutkom zdarzenia;
      c) w przypadku stwierdzenia próby dyskryminacji, szantażu, zgłoszenie tego faktu właściwym organom;
      d) skorzystanie ze środków ochrony dóbr osobistych wskazanych w przepisach ustawy Kodeks cywilny;
      e) 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.

W przypadku jakichkolwiek pytań, wątpliwości w związku zaistniałym zdarzeniem, w szczególności o sposobach zapobiegania jego negatywnym skutkom, prosimy o kontakt z Inspektorem Ochrony Danych na dane jak poniżej:

Grzegorz Stopka, Inspektor Ochrony Danych Osobowych, al. Marcina Kromera 44, 51-163 Wrocław, e-mail: iodo@zgkikm.wroc.pl , tel.: +48 71 327 21 00.

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 mObywatel (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.