KOMUNIKAT:

INCYDENT NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Samodzielny Publiczny Zakład Opieki Zdrowotnej Gminny Ośrodek Zdrowia w Imielnie, jako administrator danych osobowych, działając w trybie art. 34 pkt 1 i 2 RODO, informuje naszych pacjentów o możliwym naruszeniu ochrony Państwa danych osobowych, w wyniku ataku hakerskiego na bazy danych pacjentów firmy ALAB laboratoria sp. z o.o., ul. Stępińska 22/30, 00-739 Warszawa, która w imieniu naszej Przychodni wykonywała badania laboratoryjne, jako Podmiot przetwarzający.

W wyniku przedmiotowego incydentu mogło dojść do naruszenia Państwa danych osobowych w postaci: imienia, nazwiska, numeru PESEL, daty urodzenia, miejsca zamieszkania oraz wyniku badania laboratoryjnego (zakres możliwych do naruszenia danych został przyjęty, na podstawie komunikatu firmy ALAB laboratoria).

Jednocześnie, pragniemy poinformować, iż wskazany incydent został zgłoszony Prezesowi Urzędu Ochrony Danych Osobowych jako naruszenie ochrony danych osobowych.

Poniżej przedstawiamy treść komunikatu wydanego przez firmę ALAB laboratoria, jednocześnie zachęcając Państwa do wdrożenia czynności zmierzających do zminimalizowania konsekwencji przedmiotowego incydentu, na które wskazuje firma ALAB w treści swojego komunikatu.

Ministerstwo Cyfryzacji udostępniło specjalne narzędzie, dzięki któremu można sprawdzić, czy nasze dane zostały naruszone. Można to zrobić wchodząc na stronę https://bezpiecznedane.gov.pl.

Treść komunikatu firmy ALAB laboratoria:

„ALAB laboratoria sp. z o.o. (dalej: spółka) jako administrator danych osobowych w trybie art. 34 pkt 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO) informuje o możliwości naruszenia ochrony danych osobowych w związku z incydentem bezpieczeństwa w postaci ataku hakerskiego. Incydent ten jest wynikiem działalności przestępczej mającej na celu wymuszenie na spółce okupu.

W dniu 19 listopada 2023 roku zaobserwowano próbę zmasowanego ataku na serwery spółki. Po dokonaniu analizy zdarzenia ustalono, że dostęp do znajdujących się tam danych mogły w sposób bezprawny uzyskać osoby nieuprawnione. Zespół ekspercki dokonał natychmiast analizy ryzyka incydentu zgodnie z rekomendacjami ENISA (Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji) i wstępnie oszacował wartość ryzyka jako wysoką.

Wstępna analiza incydentu wykazała, że osoby trzecie w sposób bezprawny mogły uzyskać dostęp do następujących danych osobowych: imię i nazwisko, numer PESEL, data urodzenia, miejsce zamieszkania oraz wynik badania laboratoryjnego. W związku z powyższym wdrożono awaryjne procedury bezpieczeństwa i komunikacji zmierzające do likwidacji skutków ataku oraz ustalenia zakresu szkód, jednocześnie informując administratorów, których dane zostały powierzone spółce do przetwarzania. Jednocześnie spółka zgłosiła naruszenie do Prezesa Urzędu Ochrony Danych Osobowych oraz poinformowała uprawnione instytucje (CERT Polska, Ministerstwo Zdrowia, Centrum E-Zdrowia), a także złożyła zawiadomienie o podejrzeniu popełnienia przestępstwa do policyjnego Centralnego Biura Zwalczania Cyberprzestępczości.

Równolegle wdrożono procedury wewnętrznego i zewnętrznego audytu bezpieczeństwa danych osobowych oraz uruchomiono monitoring sieci Internet pod kątem możliwego upublicznienia nielegalnie pozyskanych danych.

Szczegółowa analiza możliwych negatywnych konsekwencji incydentu dla klientów i partnerów spółki wraz z rekomendowanymi działaniami znajduje się poniżej.

Wszelkie informacje oraz pytania dotyczące incydentu można należy zgłaszać pod adresem mailowym: iod@alab.com.pl lub na poniższe dane kontaktowe:

Marta Jędrzejczak (Inspektor ochrony danych spółki), ul. Stępińska 22/30, 00-739 Warszawa.

Spółka pragnie zapewnić, że sprawa jest traktowana priorytetowo i z najwyższą powagą. Głównym celem Spółki jest wyjaśnienie incydentu we współpracy z uprawnionymi instytucjami publicznymi.

Bezpieczeństwo Państwa danych można sprawdzić na stronie: https://bezpiecznedane.gov.pl/

***

Możliwe negatywne z punktu widzenia klientów konsekwencje incydentu:

- *uzyskanie przez osoby trzecie, na szkodę osób, których dane naruszono, kredytów w instytucjach poza bankowych, ponieważ wiele takich instytucji umożliwia uzyskanie pożyczki lub kredytu w łatwy i szybki sposób np. przez Internet lub telefonicznie bez konieczności okazywania dokumentu tożsamości,*
- *uzyskanie dostępu do korzystania ze świadczeń opieki zdrowotnej przysługujących osobom, których dane naruszono oraz ich danych o stanie zdrowia, ponieważ często dostęp do systemów rejestracji pacjenta można uzyskać telefonicznie potwierdzając swoją tożsamość za pomocą numeru PESEL,*
- *korzystanie z praw obywatelskich osób, których dane naruszono, np.: do głosowania nad środkami budżetu obywatelskiego co z kolei uniemożliwiałoby to osobom których dane w sposób nieuprawniony użyto skorzystanie z przysługującego im prawa,*
- *wyłudzenie ubezpieczenia lub środków z ubezpieczenia, co może spowodować dla osób, których dane dotyczą, negatywne konsekwencje w postaci problemów związanych z próbą przypisania im odpowiedzialności za dokonanie takiego oszustwa,*
- *zarejestrowanie przedpłaconej karty telefonicznej (pre-paid), która może posłużyć do celów przestępczych.*

Rekomendowane działania mogące zminimalizować szkodliwość takich konsekwencji:

- *założenie konta w systemie informacji kredytowej i gospodarczej w celu monitorowania swojej aktywności kredytowej, rozporządzenie RODO daje możliwość, uzyskania darmowego dostępu do zebranych na swój temat danych w formie „kopii danych", którą mamy prawo uzyskać od BIK,*
- *zachowanie szczególnej ostrożności przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem Internetu czy telefonu,*
- *zgłoszenia faktu naruszenia danych właściwym organom w celu zapobieżenia tzw. „kradzieży tożsamości"*
- *Zastrzeżenie numeru PESEL w serwisie mobywatel.gov.pl Poprzez zalogowanie się do systemu, wejście do sekcji „Twoje dane", potem Rejestr Zastrzeżeń PESEL i wybrać „Zastrzeż PESEL" lub „Cofnij zastrzeżenie".*

Data publikacji: 27.11.2023 r."