**Komunikat: incydent naruszenia bezpieczeństwa danych osobowych**

Ogólnopolskie Stowarzyszenie ,,Kominki i Piece” (dalej: stowarzyszenie) 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 (uzyskanie dostępu do serwera, panelu administracyjnego oraz skrzynki mailowej przez osobę trzecią). Incydent ten jest wynikiem działalności przestępczej – zostały wysłane do różnych adresatów wiadomości mailowe zawierające fałszywe proformy do opłacenia. Ze względu na fakt, iż osobie trzeciej udało się przełamać zabezpieczenia i zalogować do skrzynki mailowej istnieje ryzyko, że uzyskała dostęp do danych osobowych zawartych w wiadomościach mailowych.

W dniu 30 kwietnia 2025 roku ujawniono przełamanie zabezpieczeń oraz masową wysyłkę fałszywych proform do opłacenia. Po dokonaniu analizy zdarzenia ustalono, że dostęp do skrzynki mailowej i znajdujących się tam danych mogły w sposób bezprawny uzyskać osoby nieuprawnione. Dokonano natychmiast analizy ryzyka incydentu i wstępnie oszacowano wartość ryzyka jako wysoką.

Wstępna analiza incydentu wykazała, że osoby trzecie w sposób bezprawny mogły uzyskać dostęp do następujących danych osobowych: imię i nazwisko, miejsce zamieszkania, numer PESEL oraz seria i numer dowodu osobistego, data urodzenia, miejsce urodzenia, numer rachunku bankowego, adres mailowy, numer telefonu oraz staż pracy w branży kominkowej. W związku z powyższym wdrożono awaryjne procedury bezpieczeństwa i komunikacji zmierzające do likwidacji skutków ataku oraz ustalenia zakresu szkód. Jednocześnie stowarzyszenie zgłosiło naruszenie do Prezesa Urzędu Ochrony Danych Osobowych.

Równolegle wdrożono procedury wewnętrzne dotyczące naruszeń ochrony danych osobowych..

Szczegółowa analiza możliwych negatywnych konsekwencji incydentu dla klientów (obecnych i przyszłych) oraz pracowników stowarzyszenia wraz z rekomendowanymi działaniami znajduje się poniżej.

Wszelkie informacje oraz pytania dotyczące incydentu należy zgłaszać pod adresem mailowym: stowarzyszenie@kominkipolskie.com.pl

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

\*\*\*

Możliwe negatywne z punktu widzenia klientów/pracowników i 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: 06.05.2025