

ZAWIADOMIENIE O NARUSZENIU OCHRONY DANYCH OSOBOWYCH CZŁONKÓW RODZIN BYŁYCH PRACOWNIKÓW

Działając w imieniu administratora danych ePWN sp. z o.o. („**Spółka**” lub „**Administrator**”), wypełniając obowiązek wskazany w art. 34 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych; „**RODO**”), informujemy że w dniu 21 lipca 2025 r. w Spółce doszło do incydentu z zakresu cyberbezpieczeństwa, który skutkował naruszeniem ochrony danych osobowych.

Co się stało?

W dniu 21 lipca 2025 r. Zespół IT Spółki wykrył incydent z zakresu cyberbezpieczeństwa, w wyniku, którego doszło do nieautoryzowanego dostępu do infrastruktury informatycznej Spółki. Zdarzenie to miało miejsce pomimo uprzedniego wdrożenia przez Spółkę odpowiednich środków technicznych i organizacyjnych, mających na celu zapewnienie wysokiego poziomu ochrony danych osobowych.

W wyniku incydentu Spółka utraciła dostęp do danych w niektórych systemach informatycznych, w tym również do danych osobowych dotyczących członków rodzin byłych pracowników. Dane te zostały udostępnione Spółce przez byłych pracowników w okresie ich zatrudnienia w Spółce, w związku ze zgłoszeniem członków rodzin do ubezpieczenia zdrowotnego i/lub realizacją uprawnień pracowniczych. Incydent mógł skutkować naruszeniem poufności danych osobowych.

Co zrobiliśmy?

Niezwłocznie po zidentyfikowaniu naruszenia podjęliśmy następujące działania w celu usunięcia lub minimalizacji możliwych skutków, w tym:

- **Zabezpieczenia:** Zabezpieczyliśmy nasze systemy informatyczne,
- **Zablokowanie dostępu:** Wdrożyliśmy środki mające na celu zablokowanie dalszego dostępu do zaatakowanych zasobów,
- **Procedury awaryjne:** Uruchomiliśmy procedury awaryjne oraz dodatkowe środki ochrony.
- **Zgłoszenie incydentu do odpowiednich organów:** w terminie przewidzianym w RODO zgłosiliśmy naruszenie ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych.

Jakie dane członków rodzin byłych pracowników zostały naruszone?

Naruszenie objęło dane, które otrzymaliśmy od naszych byłych pracowników w celu zgłoszenia ich członków rodzin do ubezpieczenia zdrowotnego i/lub realizacją uprawnień pracowniczych. Dane te mogły zawierać:

- imiona i nazwiska,
- numery PESEL,
- daty urodzenia,
- adresy zamieszkania,
- w przypadku dzieci: numery dowodów osobistych (Administrator nie zbiera tych numerów od pracowników, w niektórych przypadkach system ZUS automatycznie udostępnia nam numer dowodu osobistego dziecka, np. przy wyrejestrowaniu ubezpieczonego).

Jakie są możliwe konsekwencje naruszenia?

W związku z naruszeniem ochrony danych mogą wystąpić następujące negatywne konsekwencje:

1. Utrata kontroli nad danymi osobowymi
 - a. Nieuprawnione wykorzystanie danych przez osoby trzecie.
 - b. Podszywanie się pod osobę, której dane dotyczą, w kontaktach z instytucjami publicznymi, pracodawcą lub innymi podmiotami.
 - c. Rejestracja usług bez wiedzy i zgody osoby, której dane dotyczą.

2. Kradzież lub sfalszowanie tożsamości
 - a. Zaciąganie zobowiązań finansowych na cudze dane.
 - b. Zawieranie niekorzystnych umów cywilnoprawnych.
 - c. Wykorzystanie danych do ukrycia tożsamości.
3. Szkody finansowe
 - a. Uzyskanie dostępu do rachunku bankowego lub dokonanie nieautoryzowanych transakcji.
 - b. Wyludzenie świadczeń ubezpieczeniowych.
 - c. Wykorzystanie danych do manipulacji lub wyludzenia dodatkowych informacji finansowych.
4. Naruszenie prywatności i poufności danych
 - a. Uzyskanie dostępu do danych medycznych lub innych informacji objętych tajemnicą zawodową.
 - b. Ujawnienie danych osobowych w sposób nieuprawniony, np. w Internecie.
5. Szkody emocjonalne i niemajątkowe
 - a. Stres, niepokój i poczucie zagrożenia związane z możliwością wykorzystania danych.
 - b. Naruszenie dobrego imienia i reputacji.
6. Ograniczenie praw i wolności
 - a. Wykorzystanie danych w sposób, który może prowadzić do dyskryminacji.
 - b. Ograniczenie możliwości korzystania z przysługujących praw obywatelskich lub społecznych.

Jakie działania zalecamy?

W związku z naruszeniem ochrony danych osobowych, rekomendujemy zachowanie szczególnej czujności i ostrożności, zwracania uwagi na nietypowe zdarzenia i sygnały mogące świadczyć o wykorzystywaniu danych osobowych członków rodziny byłego pracownika Spółki niezgodnie z przepisami, a także podjęcie następujących działań zabezpieczających we własnym zakresie:

- Skorzystanie z możliwości założenia konta w systemie informacji kredytowej celem monitorowania prób uzyskania kredytu.
- Zachowanie ostrożności przy próbie kontaktu z nieznanymi numerów lub adresów e-mail, szczególnie przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem Internetu czy telefonu.
- Skorzystanie z możliwości zastrzeżenia dokumentu tożsamości w systemie dokumenty zastrzeżone (więcej informacji: www.dokumentyzastrzezone.pl).
- Skorzystanie z możliwości zastrzeżenia numeru PESEL (więcej informacji: <https://www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie>).
- W razie stwierdzenia podszywania się - zgłoszenie podejrzenia popełnienia przestępstwa na Policję.
- Skorzystanie ze środków ochrony dóbr osobistych określonych w przepisach Kodeksu Cywilnego w razie stwierdzenia naruszenia dóbr osobistych poprzez wykorzystanie danych osobowych.
- Zmiana danych logowania lub zastosowanie uwierzytelniania dwuskładnikowego do systemów, w których numer PESEL służył jako login lub hasło.
- Monitorowanie bezpieczeństwa danych za pośrednictwem strony: <https://bezpiecznedane.gov.pl/>

Zalecenia dotyczące rozmowy z dzieckiem w związku z naruszeniem ochrony jego danych osobowych

(Dotyczy wyłącznie osób, które udostępniły Spółce dane małoletnich dzieci, w związku ze zgłoszeniem ich do ubezpieczenia zdrowotnego i/lub realizacją uprawnień pracowniczych)

W związku z naruszeniem ochrony danych osobowych dziecka, rekomendujemy przeprowadzenie z nim spokojnej, świadomej i dostosowanej do jego wieku rozmowy. Celem takiej rozmowy powinno być wyjaśnienie dziecku sytuacji, w jakiej się znalazło, a także przygotowanie go na możliwe konsekwencje oraz nauczanie odpowiednich postaw i zachowań związanych z ochroną prywatnych informacji.

Poniżej przedstawiamy zestaw zaleceń, które mogą pomóc w przeprowadzeniu tej rozmowy w sposób konstruktywny, wspierający i bez wywoływania niepotrzebnego lęku.

1. Zadbanie o odpowiednie warunki rozmowy

Rekomendujemy, aby rozmowa odbyła się w spokojnych warunkach, w miejscu, w którym dziecko czuje się bezpiecznie. Warto wybrać moment, w którym zarówno dziecko, jak i rodzic, nie są rozproszeni innymi obowiązkami i posługiwać się prostym językiem dostosowanym do wieku oraz poziomu rozumienia dziecka.

2. Rzeczowe wyjaśnienie sytuacji

Podczas rozmowy warto w sposób zwięzły i zrozumiały poinformować dziecko, że doszło do sytuacji, w której jego dane osobowe, takie jak imię, nazwisko, adres zamieszkania, numer PESEL, mogły zostać ujawnione osobom nieuprawnionym. Warto podkreślić, że dziecko nie ponosi żadnej winy za zaistniałą sytuację. Należy również wyjaśnić, że w niektórych przypadkach osoby trzecie mogą próbować wykorzystać te dane w niewłaściwy sposób, np. podszywając się pod dziecko w Internecie lub próbując się z nim skontaktować.

3. Przekazanie podstawowych zasad ostrożności

Dziecku należy przekazać podstawowe zasady, które powinno stosować w codziennym życiu, aby chronić swoje dane osobowe. Zaleca się, aby omówiono z dzieckiem między innymi następujące kwestie:

- Dziecko nie powinno samodzielnie przekazywać swoich danych osobowych żadnym osobom, zwłaszcza za pośrednictwem Internetu.
- W przypadku otrzymania nietypowej wiadomości, w szczególności związanej z danymi osobowymi lub kontaktu z nieznaną osobą, należy niezwłocznie poinformować o tym rodzica lub opiekuna i nie podejmować żadnych działań samodzielnie.
- Nie powinno się klikać w nieznane lub podejrzane linki ani instalować aplikacji bez wcześniejszej zgody osoby dorosłej.
- Wszelkie nietypowe sytuacje, takie jak wiadomości zawierające prośby o podanie danych lub próby nawiązania kontaktu przez obce osoby, powinny być natychmiast zgłaszane rodzicom.

4. Zapewnienie dziecka o wsparciu

Ważne jest, aby dziecko miało świadomość, że może liczyć na wsparcie i opiekę ze strony rodziców/opiekunów. Należy zapewnić je, że ma prawo zgłaszać wszelkie wątpliwości, pytania lub niepokojące sytuacje. Rekomendujemy również, aby w rozmowie podkreślić, że nie ma „głupich pytań”, a odpowiedzialne zachowanie polega właśnie na tym, aby informować dorosłych o swoich obawach i nie podejmować ryzykownych działań na własną rękę.

Jak można się z nami skontaktować?

W razie jakichkolwiek pytań lub wątpliwości, prosimy o kontakt z naszym Inspektorem Ochrony Danych: Karoliną Nowak, pod adresem email: abi@pwn.pl oraz Bogusławą Trawińską, pod adresem email: komunikacjaPR@pwn.pl

Przepraszamy za wszelkie niedogodności i dziękujemy za zrozumienie - Wasze bezpieczeństwo jest dla nas priorytetem.

Niniejsze powiadomienie zostało przygotowane przez Administratora zgodnie z wymaganiami RODO.

Z poważaniem, w imieniu Spółki,

Zarząd ePWN sp. z o.o.