

Warszawa, dnia 23.07.2025r.

ZAWIADOMIENIE OSOBY, KTÓREJ DANE DOTYCZĄ O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Szanowni Państwo,

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**”), z przykrością informujemy, że w dniu 21 lipca 2025 r. w Spółce doszło do incydentu z zakresu cyberbezpieczeństwa, który skutkował naruszeniem ochrony danych osobowych.

Incydent polegał na nieautoryzowanym dostępie do infrastruktury informatycznej Spółki, w wyniku czego doszło do utraty dostępu do danych w wybranych systemach informatycznych. Zdarzenie to mogło również skutkować naruszeniem poufności Waszych 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, obejmujących również dane osobowe. Zdarzenie mogło również skutkować naruszeniem poufności Waszych danych osobowych.

Co zrobiliśmy?

Niezwłocznie po zidentyfikowaniu naruszenia podjęliśmy następujące działania w celu usunięcia/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.

Informujemy, że wdramy wszelkie niezbędne działania w celu wyjaśnienia przyczyn incydentu, ograniczenia potencjalnych negatywnych jego konsekwencji oraz eliminacji ryzyka wystąpienia podobnych incydentów w przyszłości.

Jakie dane zostały naruszone?

Naruszenie objęło następujące kategorie danych osobowych:

- imię i nazwisko,
- numer PESEL,
- adres zamieszkania,
- numer telefonu,
- adres e-mail,
- dane dotyczące Państwa wynagrodzenia, w tym numer rachunku bankowego,
- informacje dotyczące umów, które zostały przez Was zawarte ze Spółką.

Jakie są możliwe konsekwencje naruszenia?

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

1. Utrata kontroli nad danymi osobowymi
 - a. Nieuprawnione wykorzystanie danych przez osoby trzecie.
 - b. Podszycie 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. Wyłudzenie świadczeń ubezpieczeniowych.
 - c. Wykorzystanie danych do manipulacji lub wyłudzenia 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 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 z przysługujących Wam środków ochrony dóbr osobistych określonych w przepisach Kodeksu Cywilnego w razie stwierdzenia naruszenia Waszych dóbr osobistych poprzez wykorzystanie Waszych danych osobowych.
- Zmiana danych logowania lub zastosowanie uwierzytelniania dwuskładnikowego do systemów, w których Wasz numer PESEL służył jako login lub hasło.
- Monitorowanie bezpieczeństwa Waszych danych za pośrednictwem strony: <https://bezpiecznedane.gov.pl/>.

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,

Zarząd ePWN