Rogów Sobócki, dnia 07 lipca 2026

ZAWIADOMIENIE O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Szanowni Państwo,

Niniejsze zawiadomienie dotyczy sytuacji skutkującej naruszeniem ochrony danych osobowych, która miała miejsce w SSE Polska Spółka z ograniczoną odpowiedzialnością (dalej jako „**Spółka**") w czerwcu 2022 roku.

O tym naruszeniu informowaliśmy już Państwa między innymi w ogłoszeniu zamieszczonym na naszej stronie internetowej.

Naruszenie zgłoszono do Prezesa Urzędu Ochrony Danych Osobowych w dniu 23 czerwca 2022 r.

Ponowne zawiadomienie jest wynikiem zalecenia, które do Spółki skierował Prezes Urzędu Ochrony Danych Osobowych. Prezes wskazał w nim, by ponownie zawiadomić Państwa o tamtym incydencie – tym razem z uwzględnieniem szerszego zestawu informacji.

1. Co się wydarzyło – charakter naruszenia

W dniu 13 czerwca 2022 roku Spółka stwierdziła, że stała się ofiarą ataku z użyciem złośliwego oprogramowania typu ransomware. Atak objął serwer Spółki, na którym przechowywane było oprogramowanie do obsługi kadrowo-płacowej i dane z nim związane.

Wskutek działania złośliwego oprogramowania pliki zgromadzone na serwerze lokalnym zostały zaszyfrowane, co uniemożliwiło dostęp do danych.

Naruszenie potwierdzono w zakresie dostępności danych (zaszyfrowanie plików). Spółka przeprowadziła analizę ruchu sieciowego z okresu ataku i **nie stwierdziła wzmożonego ruchu wskazującego na nieautoryzowany transfer danych poza jej systemy informatyczne.**

Niemniej Spółka nie jest w stanie z całkowitą pewnością wykluczyć naruszenia poufności danych.

2. Jakie kategorie danych osobowych oraz osób, których dane dotyczą, zostały objęte naruszeniem

Zgodnie z ustaleniami Spółki naruszenie dotyczyło następujących kategorii danych osobowych: imiona i nazwiska, imiona rodziców, daty urodzenia, numery ewidencyjne PESEL, serie i numery dowodów osobistych, adresy zamieszkania lub pobytu, numery rachunków bankowych, numery telefonu, adresy e-mail, nazwy użytkownika i/lub hasła do systemów, dane dotyczące zarobków i/lub posiadanego majątku, nazwiska rodowe matki, dane dotyczące zdrowia, zaświadczenia z Krajowego Rejestru Karnego, dane dotyczące rozpoczęcia, przebiegu lub ustania zatrudnienia.

Naruszenie dotyczyło następujących kategorii osób: pracownicy, zleceniobiorcy, byli pracownicy i byli zleceniobiorcy Spółki oraz członkowie rodzin pracowników i byłych pracowników.

3. Możliwe konsekwencje naruszenia ochrony danych osobowych

Mając na uwadze szeroki zakres danych objętych naruszeniem - w ślad za wskazaniami Prezesa Urzędu Ochrony Danych - wskazujemy poniżej konsekwencje, z którymi powinni się Państwo liczyć.

A. Ryzyko wyłudzenia i kradzieży tożsamości

W związku z naruszeniem obejmującym taki zestaw danych jak imię i nazwisko oraz numer PESEL, osoby trzecie (osoby nieuprawnione) mogą:

- uzyskać kredyty lub pożyczki w instytucjach pozabankowych (parabankach) z wykorzystaniem Państwa danych,
- podszywać się pod Państwa osobę np. przy zawieraniu umów, rejestracji kont internetowych lub logowaniu do systemów,
- dokonywać innych czynności prowadzących do kradzieży tożsamości i naruszenia Państwa interesów finansowych.

B. Ryzyko dyskryminacji i naruszenia dóbr osobistych

W związku z naruszeniem obejmującym taki zestaw danych jak imię, nazwisko, adres zamieszkania, dane dotyczące zdrowia oraz zaświadczenia z Krajowego Rejestru Karnego, istnieje ryzyko:

- dyskryminacji w życiu zawodowym lub prywatnym,
- ostracyzmu społecznego,
- naruszenia dóbr osobistych.

4. Co mogą Państwo zrobić – zalecane działania ochronne

A. Działania mające na celu ochronę przed wyłudzeniem i kradzieżą tożsamości

W przypadku wycieku danych obejmującego numery PESEL zaleca się zastrzeżenie numeru w stosownym rejestrze – jest to możliwe np. za pośrednictwem portalu *obywatel.gov.pl* lub aplikacji *mObywatel*. Zastrzeżenie numeru PESEL skutecznie utrudni zawarcie w Państwa imieniu umów kredytowych lub pożyczkowych przez osoby nieuprawnione.

Rekomendujemy Państwu ponadto:

- regularne monitorowanie swojej historii kredytowej, w szczególności za pośrednictwem Biura Informacji Kredytowej (BIK) pod adresem *www.bik.pl*, w tym ustawienie alertów BIK powiadamiających o każdym zapytaniu o Państwa dane.
- szczególną ostrożność wobec podejrzanych wiadomości e-mail, SMS lub telefonów, w których ktokolwiek prosi o podanie danych osobowych lub danych dostępowych.
- zmianę haseł do systemów, w których używali Państwo tych samych danych logowania, jakie mogły być przechowywane w systemach Spółki.

B. Działania mające na celu ochronę dóbr osobistych oraz ochronę przed dyskryminacją i ostracyzmem społecznym

W przypadku naruszenia Państwa dóbr osobistych (dobrego imienia, prywatności, godności) w związku z ujawnieniem danych dotyczących zdrowia lub zaświadczeń z Krajowego Rejestru Karnego, przysługują Państwu środki ochrony przewidziane w Kodeksie cywilnym (przepisy o ochronie dóbr osobistych) oraz w Kodeksie postępowania cywilnego.

Zgodnie z art. 23 kodeksu cywilnego, dobra osobiste pozostają pod ochroną prawa cywilnego. Jak stanowi art. 24 kodeksu cywilnego, każdy, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, żeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności żeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Jeżeli wskutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa, poszkodowany może żądać jej naprawienia na zasadach ogólnych przewidzianych w kodeksie cywilnym

W przypadku silnego stresu, niepokoju lub poczucia naruszenia prywatności w związku z opisanym incydentem, rekomendujemy rozważenie skorzystania ze wsparcia psychologicznego.

5. Działania Spółki po incydencie oraz istotne informacje dodatkowe

Po incydencie Spółka podjęła szereg działań mających na celu eliminację podobnych zdarzeń w przyszłości. W szczególności wdrożono następujące dodatkowe środki ochrony:

- system wykrywania i reagowania na zagrożenia na urządzeniach końcowych, który stale monitoruje aktywność w sieci Spółki,
- rozszerzone stosowanie uwierzytelniania wieloskładnikowego w przypadku kluczowych usług,
- politykę blokowania potencjalnie niebezpiecznych rozszerzeń plików w systemie poczty elektronicznej,
- dodatkowe rozwiązania w zakresie tworzenia i przywracania danych z kopii zapasowych.

Ponadto należy podkreślić, że Spółce udało się odtworzyć zaszyfrowane dane.

Jednocześnie analizy ruchu sieciowego nie dostarczyły dowodów, że dane były skopiowane lub pobrane przez nieuprawnione osoby.

Dodatkowo warto wskazać, że mimo upływu czterech lat od incydentu do Spółki nie dotarły informacje, aby osoby, których dane dotyczą, doświadczyły negatywnych następstw związanych z incydentem.

6. Dane kontaktowe

We wszelkich kwestiach związanych z opisanym wyżej zdarzeniem można kontaktować się ze Spółką pod adresem SSE Polska Sp. z o.o., Rogów Sobócki, ul. Wrocławska 58, 55-050 Sobótka oraz numerem telefonu: +48 71 390 41 22 lub adresem email: *sse-polska@sse-polska.pl*.

Z poważaniem,

Zarząd SSE Polska Sp. z o.o.