

Zawiadomienie o naruszeniu ochrony danych osobowych

Szanowni Państwo,

niniejszym w trybie art. 34 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), Zakład Gospodarki Komunalnej w Gorzycach będący Administratorem Państwa danych osobowych informuje, że w dniu 14 marca 2025 r., wystąpił incydent związany z cyberatakami, który spowodował naruszenie ochrony danych osobowych. Atak polegał na uzyskaniu kopii korespondencji e-mail ZGK w Gorzycach, co wiąże się z wysokim ryzykiem ich nieuprawnionego dostępu i potencjalnej kradzieży.

W wyniku tego zdarzenia z dużym prawdopodobieństwem doszło do naruszenia ich poufności. Dotyczy to informacji zawartych w korespondencji e-mail.

W związku z powyższym podjęto działania zmierzające do likwidacji skutków ataku oraz ustalenia zakresu szkód. Jednocześnie ZGK w Gorzycach dokonał zgłoszenia naruszenia do Prezesa Urzędu Ochrony Danych Osobowych oraz poinformował uprawnione instytucje (Policja i CERT Polska).

W dalszej części przekazujemy Państwu:

1. Opis charakteru naruszenia.
2. Możliwe konsekwencje z jakimi możecie się Państwo zetknąć w związku z naruszeniem.
3. Działania i środki, jakie zostały podjęte i jakie obecnie nadal są podejmowane w celu zaradzenia naruszeniu a także w celu zminimalizowania jego ewentualnych skutków.
4. Informacje o możliwych działaniach, jakie mogą Państwo podjąć samodzielnie.

1. Opis charakteru naruszenia

Naruszenie ochrony danych osobowych miało charakter incydentu cybernetycznego polegającego na włamaniu na skrzynki mailowe oraz ustawienie na nich nietypowych przekierowań, co może skutkować nieautoryzowanym dostępem do danych oraz potencjalnym naruszeniem ich poufności. Istnieje wysokie prawdopodobieństwo, że dane osobowe zostały przejęte w sposób nieuprawniony. Może to oznaczać możliwość ich dalszego wykorzystania w sposób nieautoryzowany, np. poprzez sprzedaż, nielegalne rozpowszechnianie lub wykorzystanie do oszustw i kradzieży tożsamości.

Atak dotknął szeroki zakres danych osobowych, obejmujących m.in. informacje pracowników, kontrahentach oraz innych osobach, których dane były przetwarzane w systemach ZGK w Gorzycach. W wyniku incydentu naruszona została poufność danych.

Naruszenie to może prowadzić do negatywnych konsekwencji dla osób, których dane zostały objęte incydem, w tym ryzyka nieuprawnionego wykorzystania Państwa danych w celach oszustw, nadużyć finansowych, czy naruszenia prywatności.

Rodzaje danych objętych atakiem:

1. Dane identyfikacyjne (m.in. imię, nazwisko, PESEL, nr dokumentu stwierdzającego tożsamość, organ wydający oraz data ważności, data urodzenia, obywatelstwo).
2. Dane adresowe (adres zamieszkania, zameldowania, korespondencyjny).
3. Dane kontaktowe (nr telefonu, adres e-mail).

Kategorie osób objętych atakiem:

1. Pracownicy.
2. Kontrahenci/podwykonawcy.

Obecnie nie możemy jednoznacznie potwierdzić, czy Państwa dane zostały skradzione, jednak istnieje wysokie prawdopodobieństwo. Wciąż trwa analiza skali incydentu, dlatego w trosce o bezpieczeństwo zalecamy dokładne zapoznanie się z poniższymi wskazówkami oraz regularne sprawdzanie aktualnych komunikatów na stronie głównej www.zgkgorzyce.pl.

2. Możliwe konsekwencje naruszenia

Administrator informuje, że niniejsze prawdopodobne naruszenie poufności w/w danych powoduje bardzo wysokie ryzyko naruszenia praw i wolności osób fizycznych, i zdecydował się zawiadomić Prezesa Urzędu Ochrony Danych Osobowych oraz opublikować niniejszy komunikat o naruszeniu ochrony danych osobowych.

W związku z naruszeniem możliwe jest wystąpienie następujących, negatywnych konsekwencji:

1. Naruszenie prawa do prywatności, w związku z incydem polegającym na ujawnieniu osobie nieupoważnionej danych osobowych zwykłych (tj. imię, nazwisko, adres zamieszkania i nr PESEL);
2. Naruszenie dóbr osobistych wynikające z możliwości ujawnienia imienia i nazwiska, oraz nr PESEL wraz z pozostałymi danymi;
3. Ograniczenie możliwości korzystania z praw obywatelskich i usług kierowanych do ogółu obywateli, w związku z ujawnieniem imienia, nazwiska i nr PESEL (np. głosowania w ramach budżetu obywatelskiego, internetowej rejestracji wizyt w urzędach itp.);
4. Uzyskanie przez osoby trzecie pożyczek w instytucjach pozabankowych z użyciem imienia, nazwiska i nr PESEL osoby dotkniętej naruszeniem (np. przez Internet, bez konieczności okazywania dokumentu tożsamości);
5. Uzyskanie przez osoby trzecie dostępu do systemów obsługujących udzielanie świadczeń medycznych osoby dotkniętej naruszeniem (czasami w takich systemach tożsamość potwierdza się za pomocą numeru PESEL);
6. Próby zawarcia umów cywilnoprawnych na szkodę osoby, której dane ujawniono, w związku z ujawnieniem imienia, nazwiska i nr PESEL, np. umów z operatorami telekomunikacyjnymi czy dostawcami sygnału RTV;
7. Uzyskanie przez osoby trzecie możliwości podjęcia próby założenia firmy z wykorzystaniem Państwa danych osobowych, która następnie może posłużyć do wyłudzeń podatkowych, narażając Państwa na nieprzyjemności i konieczność wykazania Państwa braku związku ze sprawą;
8. Uzyskanie przez osoby trzecie możliwości złożenia fałszywej deklaracji podatkowej w Państwa imieniu, powodując tym działaniem wszczęcie postępowania wyjaśniającego w Urzędzie Skarbowym;
9. Ryzyko otrzymania wezwania do zwrotu środków, których faktycznie Państwo nie otrzymaliście;
10. Ryzyko podjęcia próby zamiany Państwa adresu korespondencyjnego, numeru telefonu lub adresu e-mail powiązanego z kontem bankowym oraz z innymi kontami (np. kontem kredytowym, leasingowym, kontem rozliczeniowym za dostarczone media (gaz, prąd, wodę etc.), czy wszelkiego rodzaju abonamenty i subskrypcje), co może utrudnić Państwu dostęp do tych internetowych kont a także ryzyko przejęcia istotnych dokumentów w korespondencji z tymi podmiotami;
11. Ryzyko uzyskania dostępu do Państwa świadczeń w ZUS lub NFZ;
12. Ryzyko otrzymania wezwania do złożenia wyjaśnień w sprawie, z którą nie macie Państwo nic wspólnego;

13. Ryzyko wystąpienia ukierunkowanych ataków socjotechnicznych, oszustw metodą "na wnuczka" czy "na policjanta";
14. Wzrost zagrożenia fizycznego (np. włamania, stalking, niechciane wizyty);
15. Możliwość fałszowania historii zawodowej i wykorzystania danych do nielegalnych celów;
16. Ryzyko oszustw rekrutacyjnych, w tym podszywania się pod pracowników;

Informujemy, że obecnie istnieją wysokie ryzyka związane z ewentualnym wykorzystaniem Państwa danych osobowych w sposób nieuprawniony, narażające Państwa na ewentualne naruszenia praw i wolności.

3. Zastosowane środki zaradcze

Aktualnie trwają czynności prowadzone przez uprawnione służby, mające na celu oszacowanie zakresu ataku a także szereg innych czynności mających na celu minimalizację skutków naruszenia.

4. Proponowane środki zaradcze – jakie działania możecie Państwo podjąć?

Zalecamy zachowanie szczególnej czujności i ostrożności, zwracania szczególnej uwagi na nietypowe zdarzenia czy na jakiegokolwiek sygnały mogące świadczyć o wykorzystywaniu Państwa danych niezgodnie z przepisami prawa.

W związku z ujawnieniem Państwa danych osobowych, możecie Państwo zminimalizować wystąpienie opisanych wyżej ryzyk m.in. poprzez:

1. Zastrzeżenie numeru PESEL. Od 1 czerwca 2024 r. instytucje finansowe (np. banki) będą miały obowiązek weryfikować, czy numer PESEL jest zastrzeżony przy zawieraniu np. umowy kredytu lub pożyczki. W dowolnym momencie mogą Państwo cofnąć zastrzeżenie, wykonać przysługujące Państwu czynności a następnie zastrzec numer ponownie. Zastrzeżenie numeru PESEL w żaden sposób nie zablokuje Państwa możliwości rejestracji do lekarza, realizacji recepty czy załatwienia sprawy urzędowej, ale zabezpiecza Państwa przed zawarciem umowy kredytu/pożyczki w Państwa imieniu przez osoby do tego nieuprawnione. Zastrzec numer PESEL można na wiele sposobów, w tym elektronicznie, za pośrednictwem Internetu oraz osobiście w urzędzie. Wszelkie szczegóły tego jak to zrobić znajdują się na rządowej stronie: <https://www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie>
2. Wykupienie rocznego abonamentu tzw. Alertów w BIK (Biurze Informacji Kredytowej) Alerty takie, przychodzą w postaci krótkich wiadomości SMS wysyłanych na Państwa nr telefonów komórkowych zawsze, gdy ktoś złoży wniosek o kredyt/pożyczkę na Państwa dane lub spróbuje podpisać w Państwa imieniu umowę np. na świadczenie usług telekomunikacyjnych z operatorem sieci komórkowej lub usług RTV z dostawcą sygnału telewizyjnego.
3. Przejrzenie dostępnych informacji w Internecie na swój temat i usunięcie tych, które mogą wykorzystać przestępcy do nielegalnej działalności, w szczególności nr telefonów komórkowych, adresy e-mail, wizerunek, adresy zamieszkania, ale także zbędne informacje o miejscach pobytu czy zainteresowaniach i wszelkie inne szczegóły, które mogą zostać wykorzystane przez przestępców do podszywania się pod Państwa.
4. Zachowanie szczególnej rozwagi podczas umieszczania jakichkolwiek prywatnych danych na swój temat w Internecie. Obecnie zakres przestępczej działalności internetowej jest bardzo szeroki i aktywny.
5. Weryfikację swoich haseł wykorzystywanych w różnych portalach, sklepach internetowych, kontach pocztowych i ich zmianę w taki sposób by były w każdym takim miejscu niepowtarzalne.
6. Weryfikację występowania Państwa danych w bazie znanych wycieków danych, za pośrednictwem rządowego portalu <https://bezpiecznedane.gov.pl>.

Jeżeli dowiedzą się Państwo o upublicznieniu, wykorzystaniu lub o jakimkolwiek dalszym ujawnieniu danych osobowych, bardzo proszę o niezwłoczne przekazanie tej informacji do Inspektora Ochrony Danych ZGK Gorzyce, korzystając z danych podanych w niniejszym zawiadomieniu, i/lub o kontakt z najbliższą jednostką Policji lub o zgłoszenie na numer alarmowy 112. Ponadto mają Państwo prawo złożyć zawiadomienie do prokuratury o możliwości popełnienia przestępstwa w związku z wejściem nieuprawnionej osoby w posiadanie Państwa danych osobowych i wykorzystywanie ich w jakikolwiek niedozwolony sposób. Mają Państwo również prawo złożyć skargę do Prezesa Urzędu Ochrony Danych Osobowych (00-193 Warszawa, ul. Stawki 2).

5. Dane kontaktowe

Inspektor Ochrony Danych:

W razie jakichkolwiek pytań, proszę o kontakt z Inspektorem Ochrony Danych, panem Mateuszem Siembab, telefonicznie: 733 – 337 – 421, za pośrednictwem poczty elektronicznej: mateusz.siembab@hebenpolska.pl lub listownie, pisząc na adres siedziby Administratora danych, z dopiskiem „Inspektor Ochrony Danych”.

Administrator danych osobowych:

Zakład Gospodarki Komunalnej w Gorzycach, 39 – 432 Gorzyce, ul. Wrzawska 9,
NIP 8670003482, REGON 001093618,
Kontakt telefoniczny: + 48 15 644-68-39
Kontakt mailowy: biuro@zgkgorzyce.pl

ZAKŁAD GOSPODARKI KOMUNALNEJ
ul. Wrzawska 9
39-432 GORZYCE
tel. (15)644 68 39
NIP: 867-000-34-82 REGON: 001093618

DYREKTOR
Zakładu Gospodarki Komunalnej
inż. Przemysław Świergul