Incydent w BNP Paribas GSC pokazał spory problem z systemem ZUS

Ten problem nie dotyczy tylko BNP Paribas GSC. To sprawa, z której powinni zdać sobie sprawę **wszyscy pracodawcy**, zarówno duże firmy, osoby prowadzące JDG (Jednoosobową Działalność Gospodarczą), jak również wszyscy "**zwykli pracownicy**", którzy niekoniecznie muszą wiedzieć, że ich dane są na platformie PUE-ZUS.

Na czym polega problem?

> *Jeśli Wasz pracodawca nadał któremuś z pracowników dostęp do PUE-ZUS (co jest dość popularną praktyką), a potem zwolnił tę osobę (lub ta osoba sama się zwolniła), to jest spora szansa, że **zapomniano tej osobie odebrać uprawnienia w PUE-ZUS**. To oznacza, że **ta osoba wciąż ma dostęp do Waszych danych** i – o czym nie wszyscy wiedzą – w niektórych przypadkach **także danych członków Waszych rodzin** (!).*
>
> *Co gorsza, nawet jeśli firma zorientuje się, że na liście "uprawnionych" do PUE-ZUS ma kogoś, kto już w firmie nie pracuje i będzie chciała się dowiedzieć, czy ta osoba "podglądała to czego nie powinna", to **ZUS nie udzieli firmie odpowiedzi w tym zakresie**. ZUS **nie posiada logów**, które są w stanie stwiedzić, czy konkretne logowanie nieuprawnionego ex-pracownika było "prywatne" czy "służbowe" (czyli, co ktoś przeglądał na platformie PUE).*

Jenym słowem, mamy w Polsce poważny problem RODO… A dokładniej, wiele firm i pracowników go ma, ale część z Was dowie się o nim dopiero z tego artykułu.

BNP Paribas GSC informuje pracowników o incydencie

Ale zacznijmy od początku. A dokładniej, początku lutego, bo wtedy dowiedzieliśmy się od pewnej osoby, że w firmie BNP Paribas GSC miał miejsce incydent ochrony danych dotyczący pracowników. Tu wyjaśnijmy, że nie chodzi o bank BNP Paribas, ale o BNP Paribas Group Service Center, czyli spółkę grupy BNP Paribas, która świadczy m.in. usługę wynajmu długoterminowego urządzeń.

Incydent polegał na tym, że **byłemu pracownikowi spółki nie odwołano skutecznie dostępu do PUE ZUS**. Okres, w którym ten pracownik mógł mieć dostęp do danych to **1 stycznia – 25 sierpnia 2023**.

Inne istotne fakty:

- spółka powiadomiła UODO o incydencie 15 września 2023 r.,
- spółka zwróciła się do ZUS z prośbą o ustalenie, czy były pracownik mógł wykorzystać swój nieodwołany dostęp w celu **obejrzenia lub pobrania** danych pracowników,
- **w grudniu 2023 spółka dowiedziała się, że ZUS nie ma możliwości sprawdzenia co wyświetlał w PUE-ZUS pracownik spółki.**

Przypomnijmy tutaj, że w PUE ZUS znajdują się takie dane pracowników jak:

- imiona i nazwiska,
- adresy (zamieszkania i zameldowania),
- numery PESEL,

- numery dokumentów,
- informacje o zwolnieniach lekarskich,
- **informacje o członkach rodzin**y zgłoszonych do ubezpiecznia.

BNP Paribas GSC poinformowała pracowników o tym incydencie dopiero na początku roku 2024. Warto jednak podkreślić, że wcześniej firma starała się ocenić ryzyko naruszenia. Nie było pewne, czy były pracownik nadużył nieskutecznie odwołanego dostępu. Tak przynajmniej wywnioskowaliśmy z informacji o incydencie, jaka dotarła do pracowników. Oczywiście chcieliśmy dowiedzieć się czegoś więcej.

Nie wyciek, a "potencjalny dostęp"

Z prośbą o skomentowanie sprawy zwróciliśmy do BNP Paribas GSC. Odpowiedzi udzielił nam Maciej Kawecki, dyrektor finansowy.

Tu wyjaśnijmy, że nie chodzi o tego dra Macieja Kaweckiego, który niegdyś pracował w GIODO i był współodpowiedzialny za reformę ochrony danych, ale o Macieja Kaweckiego z BNP Paribas GSC, której to spółki nie powinniście mylić z bankiem BPN Paribas. ZUS jest jednak w tej historii tym ZUS-em, o którym myślicie, a konto w PUE-ZUS, nawet jeśli tego nie wiecie, możecie mieć. Proste, nie?

Maciej Kawecki potwierdził w oświadczeniu dla naszej redakcji, że opisany incydent był bardziej "nieodwołanym dostępem" niż "wyciekiem":

> *Przedmiotem zawiadomienia do PUODO było naruszenie ochrony danych osobowych polegające na potencjalnym dostępie byłego pracownika BNP Paribas GSC S.A. do danych osobowych innych pracowników BNP Paribas GSC S.A. w wyniku opóźnienia w odwołaniu pełnomocnictwa w ZUS dla tego byłego pracownika BNP Paribas GSC S.A., co skutkowało pozostawieniem aktywnego dostępu do danych w PUE-ZUS, co do których pracownik*

> *wcześniej miał dostęp na mocy upoważnienia.* ***Spółka nie ma podstaw by twierdzić, że doszło do jakiegokolwiek wycieku danych osobowych pracowników BNP Paribas GSC S.A.****, ani by były pracownik faktycznie miał dostęp do tych danych (…)*
> *Nie zauważono żadnych niepokojących sytuacji mogących świadczyć o tym, że dane pracowników mogły zostać wykorzystane.*

Skoro nie ma podstaw to dlaczego jednak poinformowano pracowników? I dlaczego w rozesłanych do nich ostrzeżeniach wspomniano o możliwości podjęcia pewnych działań ochronnych? Jak wyjaśnił Maciej Kawecki, potencjalne ryzyko zidentyfikowano w sierpniu 2023r. Wtedy spółka zwróciła się z prośbą o informację do ZUS. W tym czasie UODO już wiedział o incydencie, ale:

- Dopiero w grudniu 2023 r. BNP Paribas GSC S.A. otrzymała odpowiedź, w której ZUS poinformował o datach logowań byłego pracownika na jego profilu ZUS-PUE, jednak również o **braku możliwości ustalenia, czy i jakie dane były przez niego przeglądane**
- Ze względu na **rodzaj danych przetwarzanych w ZUS-PUE** ryzyko naruszenia praw i wolności dla podmiotów danych zostało ocenione jako **wysokie**.
- Co ważne, spółka otrzymała od UODO pismo informujące, że w wyniku analizy zawiadomienia w ocenie PUODO BPN Paribas GSC S.A. wdrożyła adekwatne środki bezpieczeństwa i środki zaradcze oraz podjęła działania mające na celu zminimalizowanie negatywnych skutków naruszenia i ryzyka jego ponownego wystąpienia.

I tu dochodzimy do senda problemu.

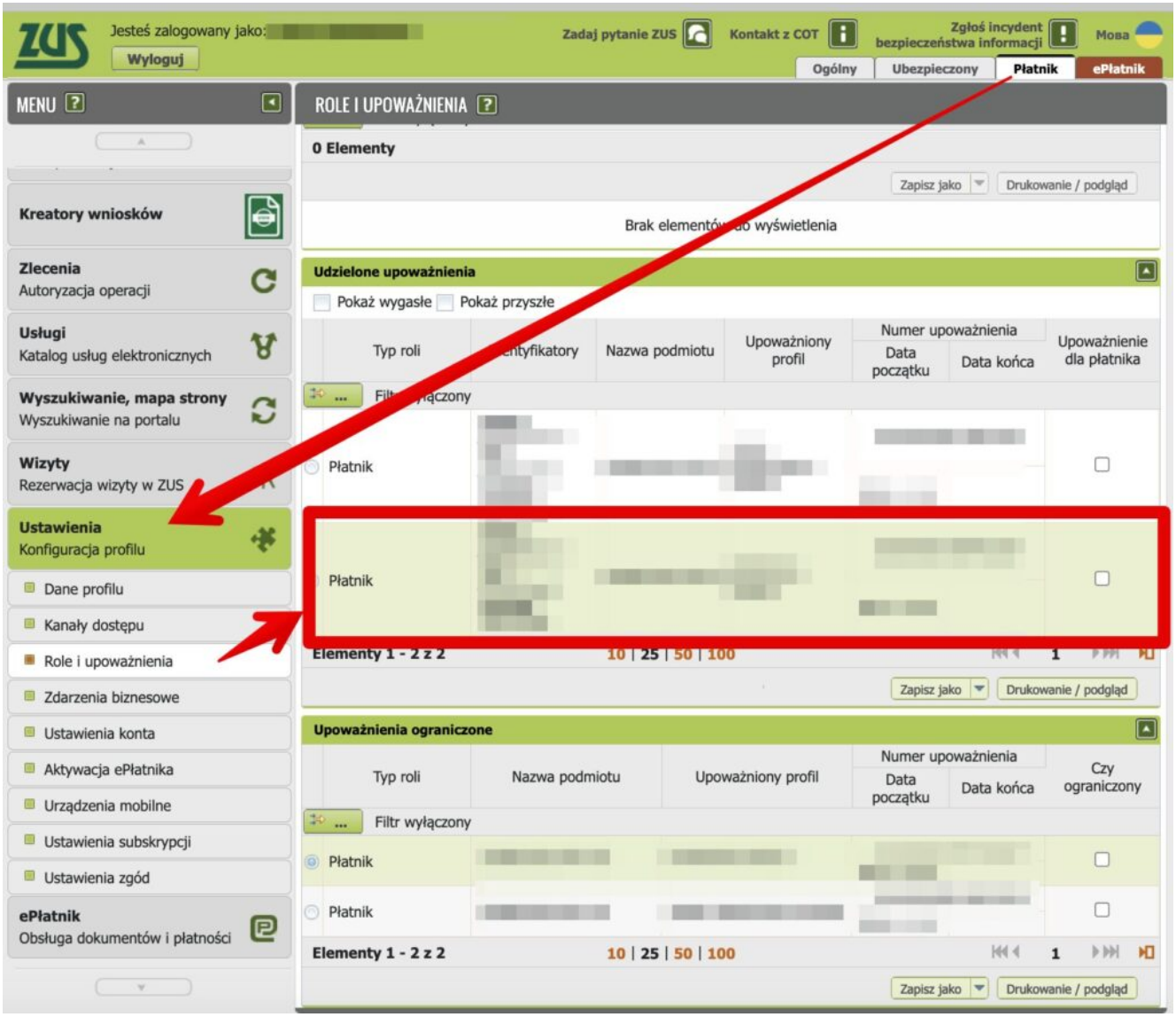
Poważne braki w PUE i ZUS

Powtórzmy jeszcze raz – ZUS przekazał spółce informacje o

logowaniach byłego pracownika, ale nie był w stanie stwierdzić, co ten pracownik widział (bo ZUS tego nie wie).

> *Czy sam fakt logowania się pracownika do PUE ZUS nie świadczy o wycieku danych? Nie, ponieważ w systemach ZUS-u nie ma czegoś takiego jak "konto pracownika". Jest prywatny profil, który dostaje upoważnienie do danych pracodawcy. Równie dobrze, ta osoba mogła się logować w swoich prywatnych sprawach i jest niejeden powód aby to robiła.*

Teoretycznie ZUS wie kiedy ktoś się logował, ale nie wie co robił na koncie. ZUS-PUE nie ma czegoś, co można by nazwać odpowiednim "audit logiem". I to, w kontekście tego, jak ta platforma jest wykorzystywana, jest dość zaskakujące, żeby nie powiedzieć, smutne.



W tym miejscu spółkę BNP Paribas GSC można nawet pochwalić. Incydent został zgłoszony, wykryty, zbadany. Ostatecznie powiadomiono też pracowników. Sytuacja trochę podobna jak kiedyś opisany u nas incydent w Twisto. Firma założyła, że ryzyko istniało i wolała poinformować, *że coś ryzykownego mogło się wydarzyć*, choć w podobnych sytuacjach wiele innych firm powiedziałoby, że **skoro nie ma dowodu nadużycia to ryzyko jest niskie**.

Przerażające w tej historii są trzy kwestie.

1. To, że ZUS potrzebował **kilku miesięcy**, aby przekazać wykaz logowań.
2. To, że ZUS nie ma wystarczająco precyzyjnych logów dla dość istotnej z punktu widzenia prywatności funkcji

3. I wreszcie to, że **pewnie wielu z Was pracuje w firmach, gdzie nikt po zwolnieniu pracownika (lub ustaniu stosunku pracy) nie odebrał mu dostępu do firmowego konta PUE-ZUS.** I ta osoba wciąż widzi dane Wasze, Waszych kolegów i Waszych rodzin.

No cóż, kontakty z ZUS-em to nigdy nie są "szybkie akcje", ale też i rozwijana przez nich platforma do najprostszych nie należy. Sami kiedyś zgłaszaliśmy do ZUS naprawdę poważne dziury i wolno to szło. Ba! Zdarzało nam się zgłaszać dziury jeszcze poważniejsze niż te poważne (też związane z rolami i uprawnieniami na platformie) i też na samą zapowiedź ich łatania czekaliśmy miesiącami.

Czy możemy liczyć na to, że Zakład Ubezpieczeń Społecznych poprawi architekturę systemu np. dodając pełniejsze logowanie zdarzeń związanych z przeglądaniem danych, do których uzyskało się upoważnienie, czyli w zasadzie coś, co powinno być dostępne do automatycznego pobrania za jednym kliknięciem na koncie każdego pracodawcy? Już zwróciliśmy się do ZUS z pytaniami i cierpliwie czekamy, ale ewentualne zmiany raczej nie będą szybkie. Mamy jednak nadzieję, że odpowiedź dostaniemy przed wakacjami. Tego roku

Co robić, jak żyć?

Do tego czasu, upewnijcie się, że na liście upoważnionych na PUE-ZUS nie ma ex-pracowników, a jak są, to ich usuńcie i zgłoście incydent do UODO oraz poinformujcie pracowników. Upewnijcie się też, że inne z danych, które trzeba skasować/zanonimizować macie pokasowane z firmowych zasobów lub poanonimizowane. A jak nie wiecie co trzeba regularnie kasować, to przypominamy instrukcje autorstwa Michała Kluski i kod PUE, który jest ważny do końca dnia i da Wam na te instrukcje 50% zniżkę. Prześlijcie ją do Waszych księgowych, kadrowych, dyrektorów IT i oczywiście prawników, zwłaszcza tych od RODO.

Aktualizacja 26.02.2024 8:36

Rzecznik ZUS Paweł Żebrowski przesłał nam oświadczenie następującej treści.

> *Zgodnie z obowiązującymi przepisami uprawnienia do logowania się do PUE-ZUS dla pracownika nadawane są przez pracodawcę. Pracodawca może również cofnąć pełnomocnictwo byłemu pracownikowi wypełniając specjalny formularz. ZUS nie weryfikuje danych o zwolnieniu pracownika.* ***Podkreślenia wymaga, że ZUS jest w stanie ustalić czy osoba loguje się na swoim koncie ubezpieczonego (co może być traktowane jako dostęp w celu prywatnym), a kiedy logowanie następuje na profilu pracodawcy, do którego obsługi posiada pełnomocnictwo (dostęp w celu służbowym).*** *To na pracodawcy jednak ciąży ciężar odwołania pełnomocnictwa i poinformowania o tym ZUS. W sytuacji zaniechania realizacji tego obowiązku przez pracodawcę nie można mówić o wycieku danych z ZUS. Możliwość nieuprawnionego dostępu do danych jest w takim przypadku wyłącznym efektem postępowania pracodawcy. Zakład Ubezpieczeń Społecznych będzie pracował z przedsiębiorcami, aby usprawnić proces administracji PUE-ZUS.*

Czyli sytuacja wymaga dalszego wyjaśnienia. Dlaczego firmie BNP Paribas GSC odpowiedziano, że ZUS nie ma możliwości sprawdzenia co widział pracownik? Możliwości są trzy:

1. Jedna ze stron mówi nieprawdę (ZUS albo spółka),
2. doszło do jakiegoś nieporozumienia, albo…
3. …ZUS wie kto i co widział, ale nie powie bo to na pracodawcy ciąży zarządzanie tym wszystkim.

O ile w 100% można się zgodzić, że to pracodawca ma zarządzać uprawnieniami to nadal uważamy, że powinien istnieć jakiś audyt log do ustalenia kto co widział. Przesłaliśmy dodatkowe pytania rzecznikowi ZUS i czekamy na odpowiedzi.

Źródło