





RODO - aktualności

[26.02.2024]

UWAGA!

Tezy przedstawione w artykułach, zamieszczone w niniejszym materiale i niebędące wytycznymi organu nadzorczego albo orzeczeniami sądów lub organów administracji publicznej, stanowią wyłącznie opinię ich autorów i nie są oficjalnym stanowiskiem Lex Artist Sp. z o.o.

01

NSA: Dane kandydatów do pracy można przechowywać 3 lata!

02

UODO: Zbyt szeroki zakres danych ujawnianych w oświadczeniach majątkowych budzi wątpliwości

03

Kontrola NIK w samorządach wykazała wieloletnie zaniedbania dot. ochrony danych

04

Rzecznik TSUE: Baza danych osobowych może być sprzedana w postępowaniu egzekucyjnym

05

Incydent w BNP Paribas GSC pokazał spory problem z systemem PUE ZUS

01 NSA: Dane kandydatów do pracy można przechowywać 3 lata

- Przechowywanie danych osobowych kandydatów do pracy, którzy nie uzyskali zatrudnienia jest dozwolone, aż do upływu terminu przedawnienia potencjalnych roszczeń związanych z dyskryminacją w procesie rekrutacji, czyli przez maksymalnie 3 lata. Tak orzekł NSA w sprawie skargi niedosłej pracownicy znanej firmy wysyłkowej A. Pani K. składała dokumenty aplikacyjne drogą elektroniczną, a firma, zgodnie z wewnętrznymi zasadami, utworzyła jej profil kandydata do pracy, przetwarzając i wykorzystując przekazane przez kandydatkę dane.
- Kobieta nie dostała pracy w firmie, wobec tego poprosiła o wykasowanie jej danych z bazy. Jednak firma odpowiedziała odmownie, wskazując, że po pierwsze zablokowała jej profil kandydatki, a po drugie, musi dysponować nadal jej danymi nawet po zakończeniu procesu rekrutacji (zakończonego dla kandydatki negatywnie), z uwagi na potencjalne roszczenia związane z naruszeniem zasad równości w zatrudnieniu.
- Pani K. skierowała skargę do Urzędu Ochrony Danych Osobowych. Prezes UODO, w odpowiedni na nią wydał decyzję, w której udzielił upomnienia firmie A. za naruszenie przepisów prawa ochrony danych osobowych poprzez bezpodstawne przetwarzanie danych po zakończeniu rekrutacji.
- WSA stwierdził, że firma A. jako administrator danych ale i pracodawca, musi respektować regulacje Kodeksu pracy dotyczące zakazu dyskryminacji ze względu nie tylko na zatrudnienie, ale i na takie same zakazy dyskryminacji dotyczące przyjmowania do pracy. Tym samym firma A. ma uzasadniony interes w przechowywaniu tych danych właśnie przez ten okres (wynoszący zgodnie z k.p. -3 lata).
- NSA w oparciu o art. 6 ust. 1 pkt f RODO wskazał, że przetwarzanie danych osobowych musi być oparte o trzy zasadnicze przesłanki: administrator musi wykazać cele, do których osiągnięcia przetwarzanie danych jest niezbędne, po drugie, cele te są uzasadnione interesem prawnym administratora danych, a interes prawny administratora ma charakter nadrzędny w stosunku do praw i wolności osoby której dane są przetwarzane. Zdaniem NSA wszystkie te przesłanki zostały spełnione.

02 UODO: Zbyt szeroki zakres danych ujawnianych w oświadczeniach majątkowych budzi wątpliwości

- Mirosław Wróblewski, prezes UODO, ma zastrzeżenia do poselskiego projektu nowelizacji ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne oraz niektórych innych ustaw, nad którym pracuje Sejm.
- Zdaniem prezesa Urzędu Ochrony Danych Osobowych informacja o sytuacji majątkowej małżonka osoby pełniącej funkcję publiczną nie stanowi informacji o działalności tej osoby, lecz o sytuacji osoby z jej rodziny. Zwraca uwagę, że informacja ta, zgodnie z projektem, stanie się publiczną.
- Dlatego zdaniem UODO projektodawca powinien wziąć pod uwagę zasadę minimalizacji danych, określoną w RODO, przepisy Konstytucji RP i przeanalizować to zagadnienie pod kątem wykazania niezbędności pozyskiwania i dalszego przetwarzania takich danych.
- Rozwiązania zaproponowane w projekcie ustawy, mimo, że opierają się na uzasadnionym założeniu zagwarantowania większej przejrzystości sytuacji osób sprawujących funkcje publiczne, stwarzają jednocześnie potencjalne poważne ryzyko naruszenia zasad przetwarzania danych osobowych.
- Przedstawiony projekt przewiduje odpowiedzialność karną osoby pełniącej funkcję publiczną także w sytuacji wypełniania oświadczenia majątkowego w części dotyczącej majątku odrębnego małżonka. Tymczasem na odpowiedzialność z tego tytułu i w tym aspekcie – zgodnie z założeniami projektu – wpływać będą również potencjalnie okoliczności braku czy niepełnej, co do zgodności ze stanem prawnym i faktycznym, wiedzy na temat majątku odrębnego małżonka.
- Wątpliwości budzi też zakres czasowy, jaki zgodnie z projektem, trzeba będzie wziąć pod uwagę, ujawniając dane w oświadczeniu majątkowym, który ma wynieść 10 lat. Wyznaczenie obowiązku przedstawiania oraz weryfikacji informacji i dokumentacji z okresu 10 lat poprzedzających złożenie oświadczenia godzi w zasadę niedziałania prawa wstecz, także w kontekście prawa do autonomii informacyjnej jednostki.

Źródło: [Ujawnienie w oświadczeniach majątkowych majątku małżonków opinia UODO \(prawo.pl\)](#)

03 Kontrola NIK w samorządach wykazała wieloletnie zaniedbania dot. ochrony danych osobowych

- Najwyższa Izba Kontroli skontrolowała 12 jednostek samorządu terytorialnego w województwie podlaskim. Wyniki kontroli były zatrważające. NIK wykazał wieloletnie zaniedbania związane z ochroną danych osobowych – wybrane elementy systemu ochrony danych osobowych w jednostkach samorządowych były złym stanie.
- W wielu samorządach korzystano z adresów mailowych utworzonych w domenach komercyjnych. Nie zawierano przy tym umów powierzenia przetwarzania danych osobowych.
- W niektórych Biuletynach Informacji Publicznej stwierdzono publikowanie oświadczeń majątkowych ponad wymagany prawem okres. Ze względu na systemowy charakter nieprawidłowości NIK rozszerzy kontrole na wszystkie jednostki samorządu terytorialnego w Polsce.
- W rezultacie kontroli wyeliminowano korzystanie z adresów mailowych utworzonych w domenach komercyjnych bez zawarcia wymaganych przez RODO umów powierzenia przetwarzania danych osobowych. Zmieniono też adresy mailowe w 45 jednostkach samorządowych oraz zrezygnowano z używania blisko 250 adresów mailowych wykorzystywanych do celów służbowych, a zlokalizowanych na domenach komercyjnych bez zawarcia stosownych umów gwarantujących odpowiedni poziom bezpieczeństwa.
- Po kontroli NIK usunięto ponad 1,3 tys. dokumentów z Biuletynów Informacji Publicznej. Dokumenty te zawierały oświadczenia majątkowe. Mimo że okres ich publikacji wynosi 6 lat, niektóre z nich dotyczyły 2002 r.
- Ponadto w niektórych samorządach zmieniono zasady transmitowania i publikowania posiedzeń organów stanowiących. Pierwotnie były one transmitowane na niezabezpieczonych portalach społecznościowych. Po kontroli 7 samorządów musiało zawrzeć umowy na przetwarzanie danych podczas transmisji obrad sesji.

04 Rzecznik TSUE: Baza danych osobowych może być sprzedana w postępowaniu egzekucyjnym

- Baza danych osobowych może być pod pewnymi warunkami sprzedana w postępowaniu egzekucyjnym, nawet jeśli osoby, których te dane dotyczą, nie wyraziły na to zgody - ocenił w opublikowanej w czwartek opinii rzecznik generalny Trybunału Sprawiedliwości UE w Luksemburgu Priit Pikamae. Sprawa dotyczy procesu toczącego się w Polsce.
- Warszawski sąd w trybie prejudycjalnym zwrócił się do Trybunału z pytaniem, czy przedmiotem postępowania egzekucyjnego może być baza danych klientów spółki oraz czy przepisy RODO stoją na przeszkodzie sprzedaży takiej bazy danych przez komornika.
- W rozpatrywanej przez warszawski sąd sprawie wierzyciel, mimo prawomocnego nakazu zapłaty, nie mógł odzyskać pieniędzy od pewnej firmy, ponieważ komornik stwierdził, że spółka nie ma majątku i umorzył postępowanie.
- Wierzyciel nie dał za wygraną i wytoczył proces członkowi zarządu firmy, ponieważ zgodnie z Kodeksem spółek handlowych, jeśli nie da się spłacić wierzyciela z majątku przedsiębiorstwa, to odpowiedzialność odszkodowawcza spada właśnie na członka zarządu.
- Pozwany wniósł o oddalenie sprawy i przyznał, że firma posiada majątek: dwie bazy danych z informacjami o setkach tysięcy użytkowników. Jak relacjonuje portal prawo.pl polski sąd ma wątpliwości, czy przepisy RODO pozwalają na to, aby takie bazy sprzedawać bez zgody osób, których dane się w nich znajdują. Dlatego skierował sprawę do TSUE.
- W opublikowanej w czwartek opinii rzecznik generalny przekonuje, że baza danych osobowych może być pod pewnymi warunkami sprzedana w postępowaniu egzekucyjnym, nawet jeśli osoby, których te dane dotyczą, nie wyraziły na to zgody.
- "Jest tak, jeżeli przetwarzanie danych, związane z taką sprzedażą, jest niezbędne i proporcjonalne w demokratycznym społeczeństwie w celu zagwarantowania egzekucji roszczenia cywilnoprawnego" - podkreślił Priit Pikamae.

05

Incydent w BNP Paribas GSC pokazał spory problem z systemem PUE ZUS

- W firmie BNP Paribas GSC miał miejsce incydent ochrony danych dotyczący pracowników, który 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.
- W PUE ZUS znajdują się takie dane pracowników, jak m.in.: imiona i nazwiska, adresy (zamieszkania i zameldowania), numery PESEL, numery dokumentów, informacje o zwolnieniach lekarskich, informacje o członkach rodziny zgłoszonych do ubezpieczenia.
- Spółka powiadomiła UODO o incydencie 15 września 2023 r. i zwróciła się do ZUS z prośbą o ustalenie, czy były pracownik mógł wykorzystać swój nieodwołany dostęp w celu obejrzenia lub pobrania danych pracowników.
- 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. Zatem informacje o tym, jakie dane wyświetla osoba zalogowana do ZUS PUE nie są zapisywane, a system nie odróżnia logowania w sprawie prywatnej od wykonywania działań na mocy upoważnienia.
- BNP Paribas GSC poinformowała pracowników o tym incydencie dopiero na początku roku 2024. Ze względu na rodzaj danych przetwarzanych w ZUS-PUE ryzyko naruszenia praw i wolności dla podmiotów danych zostało ocenione jako wysokie.
- Zdaniem ZUS to na pracodawcy 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.

Źródło: [Wyciek danych osobowych z ZUS. Teraz radź sobie sam \(aktualizacja\) - TELEPOLIS.PL](#); » [Incydent w BNP Paribas GSC pokazał spory problem z systemem ZUS -- Niebezpiecznik.pl](#) –

*Niniejszy dokument bez zezwolenia nie może być w żaden sposób wykorzystywany,
w szczególności rozpowszechniany i kopiowany.*