
LEX ARTIST

RODO - aktualności

22 lutego 2021 r.

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 Prezes UODO upomina za nieaktualne oprogramowanie

02 KSSIP z karą pieniężną za naruszenie przepisów RODO

03 Kara nałożona przez Prezesa UODO uchylona

04 W indywidualnej sprawie należy złożyć skargę do UODO

05 Hiszpański Urząd Ochrony Danych nakłada grzywnę w wysokości 6 mln EUR

01 Prezes UODO upomina za nieaktualne oprogramowanie

- organ nadzorczy nałożył karę upomnienia na spółkę, która straciła dostęp do danych osobowych w wyniku ataku złośliwego oprogramowania szyfrującego typu ransomware
- postępowanie UODO wykazało, że administrator danych dobrał nieskuteczne środki ochrony swoich systemów informatycznych – nie przeprowadzał też testów ich podatności na różnego rodzaju zagrożenia
- w ocenie organu nadzoru nie były sprawdzane w pełnym zakresie zabezpieczenia techniczne i organizacyjne systemów, w których przetwarzano dane osobowe
- administrator dysponował przestarzałymi systemami operacyjnymi i innym oprogramowaniem, które nie było aktualizowane, gdyż producenci tych rozwiązań nie oferowali już dla nich wsparcia technicznego – w efekcie nie były one aktualizowane m.in. pod kątem zabezpieczeń w tych programach
- w wyniku ataku złośliwego oprogramowania, które skutkowało zaszyfrowaniem danych osobowych, spółka utraciła dostęp do tych danych - nie doszło jednak do naruszenia atrybutu poufności danych osobowych
- w ocenie UODO naruszenie nie powodowało więc wysokiego ryzyka dla osób dotkniętych naruszeniem

Źródło: https://uodo.gov.pl/pl/138/1896

02 KSSIP z karą pieniężną za naruszenie przepisów RODO

- UODO stwierdził naruszenie przepisów RODO i nałożył administracyjną karę pieniężną w wysokości 100 tys. zł na Krajową Szkołę Sądownictwa i Prokuratury za niezrealizowanie ciążących na niej obowiązków administratora
- zdaniem UODO administrator nie zastosował odpowiednich środków technicznych i organizacyjnych, które pozwoliłyby zapewnić poufność usług przetwarzania
- KSSIP nie przetestowała i nie dokonała oceny skuteczności środków technicznych i organizacyjnych, mających na celu zapewnienie bezpieczeństwa danych osobowych znajdujących się w kopii bazy danych platformy szkoleniowej Krajowej Szkoły Sądownictwa i Prokuratury, a tym samym niewłaściwe uwzględniła ryzyka, jakie wiąże się ze zmianami w procesie przetwarzania danych osobowych
- administrator powierzył przetwarzanie danych osobowych podmiotowi przetwarzającemu bez umownego zobowiązania go do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora
- KSSIP zgłosiła UODO naruszenie ochrony danych osobowych, w związku z powiadomieniem o pojawieniu się w Internecie danych osobowych związanych z domeną kssip.gov.pl - incydent polegał na uzyskaniu przez nieznane osoby dostępu do kopii bazy danych witryny szkoleniowej KSSIP powstałej w trakcie testowej migracji do nowej platformy szkoleniowej

Źródło: https://uodo.gov.pl/pl/138/1909

03 Kara nałożona przez Prezesa UODO uchylona

- to pierwszy wyrok uchylający w pełni decyzję UODO – chodzi o karę 20 tys. zł nałożoną w lutym 2020 r. na Szkołę Podstawową nr 2 w Gdańsku za zainstalowanie czytników linii papilarnych przed wejściem do szkolnej stołówki
- uczeń przykładał palec, skaner porównywał odcisk i identyfikował dziecko – po przesłaniu informacji do systemu ten weryfikował, czy posiłek został opłacany
- szkoła twierdziła, że podstawę prawną stanowią dobrowolne zgody rodziców – UODO nie zgodził się, uznając, że chodziło o realizację zadań opiekuńczych i w tej sytuacji podstawą przetwarzania danych jest ustawa, a wówczas zgoda nie wchodzi w grę
- WSA w Warszawie nie miał wątpliwości, że chodzi o dane biometryczne, a więc szczególne, ale jego zdaniem nawet ich przetwarzanie szkoła mogła oprzeć na pisemnej zgodzie rodziców.
- dodatkowo sąd przyznał, że pogodzenie wymogu adekwatności i minimalizacji może nie być łatwe, ale jego zdaniem jest to możliwe i nie można zasadzie minimalizacji przyznawać pierwszeństwa – zdaniem sądu warunkiem jest to, aby przetwarzane dane miały ścisły związek z realizowanym celem – wystarczy, by ułatwiały jego osiągnięcie
- Prezes UODO nie zgadza się z orzeczeniem WSA w Warszawie i zapowiada złożenie kasacji do NSA

Źródło: https://prawo.gazetaprawna.pl/artykuly/8099344,za-zgoda-rodzicow-mozna-skanowac-linie-papilarne.html

04 W indywidualnej sprawie należy złożyć skargę do UODO

- co zrobić jeśli uznamy, że konkretny administrator danych naruszył nasze prawa albo przetwarza jej dane z naruszaniem przepisów o ochronie danych osobowych? – wtedy mamy prawo do złożenia skargi zarówno do Prezesa UODO, jak i skierować sprawę na drogę sądową
- poszkodowany może ponadto w oparciu o regulacje RODO dochodzić sądownie odszkodowania
- co w przypadku, gdy administrator danych nie jest nam znany? – wtedy urząd stara się ustalić administratora, a gdy nie jest to możliwe to zawiadamia organy ścigania
- bez wiedzy kto jest administratorem nie jest możliwe wszczęcie postępowania z urzędu - wyjaśnia UODO.
- *Urząd Ochrony Danych Osobowych nie jest organem ściągania i nie ma kompetencji śledczych, by w niektórych przypadkach zidentyfikować sprawcę takiego naruszenia. Takie uprawnienia oraz narzędzia do tego mają jedynie organy ścigania, jak policja czy prokuratura* - czytamy na stronie UODO.

Źródło: https://www.rp.pl/Dane-osobowe/302219978-Dane-osobowe-w-indywidualnej-sprawie-nalezy-zlozyc-skarge-do-UODO.html https://uodo.gov.pl/pl/138/1914

05 Hiszpański Urząd Ochrony Danych nakłada grzywnę w wysokości 6 mln EUR

- Hiszpański Urząd Ochrony Danych nałożył grzywnę o łącznej wysokości 6 mln EUR na CAIXABANK, SA za niezgodne z prawem przetwarzanie danych osobowych klientów i niedostarczenie wystarczających informacji dotyczących przetwarzania
- organ uznał, że dokument mający na celu przekazanie podmiotom danych informacji o przetwarzaniu ich danych nie zawiera wystarczających informacji dotyczących kategorii danych, których dotyczy, ani informacji o celach przetwarzania, a także o podstawie prawnej przetwarzania, zwłaszcza w odniesieniu przetwarzania opartego na uzasadnionym interesie firmy
- w konsekwencji organ uznał, że CAIXABANK naruszył art. 13 i 14 RODO za co nałożono karę w wysokości 2 000 000 EUR
- decydując o wysokości grzywny, organ uwzględnił m.in. charakter, wagę i czas trwania naruszenia, niedbały charakter naruszenia, związek między działalnością firmy a przetwarzaniem danych osobowych oraz obroty firmy
- dalej, organ stwierdził, że CAIXABANK nie zapewnia żadnego mechanizmu zbierania zgody osoby, której dane dotyczą i uznał, że stanowiło to naruszenie art. 6 RODO za co nałożono karę administracyjną w wysokości 4 000 000 EUR
- przy ustalaniu wysokości grzywny organ uwzględnił, m.in. charakter, wagę i czas trwania naruszenia; niedbały charakter naruszenia, stopień odpowiedzialności z uwzględnieniem środków technicznych i organizacyjnych, korzyści uzyskane z naruszenia, kategorie danych, związek między działalnością firmy a przetwarzaniem danych osobowych; oraz obroty firmy

Źródło: https://edpb.europa.eu/news/national-news/2021/spanish-data-protection-authority-aepd-imposes-fine-6000000-eur-caixabank-sa_en