ALERT JDP | DECYZJE PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH

Prezes Urzędu Ochrony Danych Osobowych („**PUODO**") nałożył w grudniu i styczniu szereg kar za naruszenia przepisów Rozporządzenia o Ochronie Danych Osobowych („**RODO**").

Poniżej przedstawiamy zestawienie nałożonych kar, wraz z komentarzem, jak w danej sytuacji powinien zachować się administrator, aby zminimalizować skutki potencjalnego naruszenia przepisów RODO.

Virgin Mobile Polska

3 grudnia 2020 r. Prezes UODO wydał decyzję DKN.5112.1.2020, w której nałożył na Virgin Mobile Polska z siedzibą w Warszawie karę pieniężną w kwocie **1.968.524 złotych**, z tytułu naruszenia przepisów RODO, polegających na niewdrożeniu odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych za pomocą systemów informatycznych służących do rejestracji danych osobowych abonentów usług przedpłaconych, co doprowadziło do uzyskania przez osobę nieuprawnioną dostępu do tych danych.

Okoliczności nałożenia kary:

Spółka dokonała zgłoszenia ochrony danych osobowych do Prezesa UODO polegającego na uzyskaniu przez osobę nieuprawnioną dostępu do danych osobowych abonentów usług przedpłaconych. W związku ze zgłoszeniem Prezes UODO zdecydował o przeprowadzeniu kontroli w Spółce. Naruszenie skutkowało tym, że w wyniku wykorzystania podatności (luki) w systemie obsługującym rejestrację abonentów (osoba nieuprawniona uzyskała dostęp do danych abonentów pre-paid i pozyskała dane osobowe w postaci 123.391 imion i nazwisk, a także numerów PESEL, numerów dokumentu abonenta, w różnej konfiguracji tych danych. W wyniku kontroli stwierdzono naruszenie przepisów oraz nałożono karę.

Wnioski dla administratora:

1. Administratorzy zobowiązani są do dokonywania przeglądu i aktualizacji zastosowanych środków technicznych i organizacyjnych w sposób kompleksowy i regularny (planowany). Nie jest wystarczającym dokonywanie

testów zabezpieczeń (w tym podatności systemów informatycznych) wyłącznie w sytuacji pojawiającego się zagrożenia („w miarę potrzeb, w sytuacji wystąpienia zmian organizacyjnych lub prawnych").
2. Zmiana istotnych okoliczności w procesie przetwarzania takich jak zmiany prawne, organizacyjne czy techniczne (np. zmiana operatora obsługującego system informatyczny) powinna pociągać za sobą obowiązek ponownej oceny skuteczności wdrożonych rozwiązań technicznych i informatycznych.
3. Administratorzy zobowiązani są do wdrożenia i stosowania procedur określających regularne testowanie, mierzenie i ocenianie skuteczności wdrożonych środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych.

Treść decyzji dostępna pod linkiem:
https://www.uodo.gov.pl/decyzje/DKN.5112.1.2020

Smart Cities

9 grudnia 2020 r. Prezes UODO wydał decyzję DKE.561.13.2020, w której nałożył na Smart Cities sp. z o.o. z siedzibą w Warszawie karę pieniężną w kwocie **12.838,20 złotych**, z tytułu naruszenia przepisów RODO, polegającym na braku współpracy z Prezesem Urzędu Ochrony Danych Osobowych oraz na niezapewnieniu dostępu do danych osobowych i innych informacji niezbędnych Prezesowi Urzędu Ochrony Danych Osobowych do realizacji jego zadań.

Okoliczności nałożenia kary:

Do UODO wpłynęła skarga na nieprawidłowości w procesie przetwarzania danych osobowych skarżącego przez Smart Cities. Prezes UODO zwrócił się do Smart Cities o ustosunkowanie się do treści skargi oraz o udzielenie odpowiedzi na szczegółowe pytania dotyczące sprawy. Administrator udzielił dalece niepełnych informacji, a następnie nie odbierał żadnej dalszej korespondencji. Prezes UODO bezskutecznie wzywał spółkę do udzielenia wyjaśnień, a następnie wszczął postępowanie ws. nałożenia kary i wydał w tym przedmiocie decyzję.

Wnioski dla administratora:

1. Brak współpracy z Prezesem UODO stanowi samodzielną podstawę do podjęcia decyzji o nałożeniu kary w osobnym postepowaniu odmiennym od postępowania, w którym UODO wzywał administratora do złożenia wyjaśnień.
2. Naruszenie, w postaci braku współpracy z Prezesem UODO, polegające na braku odpowiedzi na wezwania UODO, jest kwalifikowane przez UODO jako umyślne, mające dużą wagę i naganny charakter.
3. Gdy administrator dopuszcza się rażących zaniedbań w obszarze ochrony danych osobowych i składanie wyjaśnień mogłoby spowodować poczynienie przez UODO ustaleń co do zaistnienia takich istotnych zaniedbań (co do których UODO nie ma wiedzy), uzasadniających wysoki wymiar kary, brak współpracy z UODO może stanowić instrumentalnie używany środek mitygowania wysokości kary finansowej, niezależnie od oceny skuteczności takiego środka.

Treść decyzji dostępna pod linkiem:
https://www.uodo.gov.pl/decyzje/DKE.561.13.2020%20

TUiR Warta

9 grudnia 2020 r. Prezes UODO wydał decyzję DKN.5131.5.2020, w której nałożył na TUiR Warta z siedzibą w Warszawie karę pieniężną w wysokości **85.588 złotych** za niezgłoszenie Prezesowi Urzędu Ochrony Danych Osobowych naruszenia ochrony danych osobowych oraz niezawiadomienie o naruszeniu ochrony danych osobowych, bez zbędnej zwłoki, osób, których dane dotyczą.

Okoliczności nałożenia kary:

O naruszeniu ochrony danych osobowych organ nadzorczy został poinformowany przez nieuprawnionego adresata, który wszedł w posiadanie nieprzeznaczonych dla niego dokumentów zawierających ww. dane osobowe. Naruszenie polegało na **jednokrotnym wysłaniu pocztą elektroniczną** przez agenta ubezpieczeniowego (P. U. J. K. z siedzibą w O.), będącego podmiotem przetwarzającym dla TUiR WARTA S.A. z siedzibą w W., **polisy ubezpieczeniowej zawierającej dane osobowe dwóch osób do nieuprawnionego adresata**,

w wyniku czego doszło do naruszenia poufności danych dwóch osób w zakresie imion, nazwisk, adresów zamieszkania lub korespondencyjnych, numerów PESEL, numerów telefonów, adresów poczty elektronicznej oraz informacji dotyczących przedmiotu ubezpieczenia (samochód osobowy), zakresu ubezpieczenia, płatności, cesji, a także dodatkowych zapisów wynikających z umowy.

Co istotne Warta przesłała polisę na adres e-mail, który podała osoba ubezpieczana. To sama osoba ubezpieczana podała omyłkowo błędny adres e-mail, w wyniku czego polisa trafiła do osoby trzeciej.

Wnioski dla administratora:

1. Naruszenie dotykające nawet pojedynczych osób może być przyczyną nałożenia kary niebagatelnej wysokości przez UODO.
2. Administrator posługujący się pocztą mailową, powinien wdrożyć system weryfikacji umożliwiający wychwycenie błędu klienta przy podawaniu swojego adresu mailowego (np. robocza weryfikacja adresów mailowych) lub system uniemożliwiający zapoznanie się z danymi przez nieuprawnionego odbiorcę (np. szyfrowanie komunikacji mailowej). W przypadku, gdy taki system nie został wdrożony, a klient błędnie podał swój własny adres, w wyniku czego dane osobowe zostały przesłane przez administratora do innej osoby niż klient, to wówczas dojdzie do naruszenia ochrony danych osobowych, za które odpowiada administrator.
3. Nawet w przypadku otrzymania przez administratora deklaracji od osób, które przypadkowo otrzymały dane, iż osoby te usunęły otrzymane dane osobowe, administrator nie może traktować takich osób jako zaufane, z uwagi na brak relacji biznesowej z tymi osobami, a tym samym oceniać ryzyka naruszenia praw i wolności osób, których dane dotyczą, jako niższe, w oparciu o taką deklarację.
4. Każde nieuprawnione ujawnienie danych, o kategoriach takich jak w tej sprawie, należy traktować jako podlegające zgłoszeniu do UODO i wymagające poinformowania osób, których dane dotyczą. Wyjątkiem może być jedynie nieuprawnione ujawnienie do odbiorców zaufanych.

Treść decyzji dostępna pod linkiem:
https://uodo.gov.pl/decyzje/DKN.5131.5.2020

ID Finance Poland (MoneyMan.pl)

17 grudnia 2020 r. Prezes UODO wydał decyzję DKN.5130.1354.2020, w której nałożył na ID Finance Poland Sp. z o.o. w likwidacji z siedzibą w Warszawie karę pieniężną w wysokości **1.069.850 złotych** z tytułu naruszenia przepisów RODO, polegających na **niewdrożeniu przez ID Finance Poland Sp. z o.o. w likwidacji, zarówno w fazie projektowania procesu przetwarzania jak i w czasie samego przetwarzania, odpowiednich środków technicznych i organizacyjnych odpowiadających ryzyku naruszenia zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemu przetwarzania danych osobowych, a także zapewniających zdolność skutecznego i szybkiego stwierdzenia naruszenia ochrony danych osobowych oraz zapewniających regularną ocenę skuteczności tych środków, co skutkowało uzyskaniem przez osoby trzecie nieuprawnionego dostępu do przetwarzanych danych osobowych.**

Okoliczności nałożenia kary:

Spółka dokonała zgłoszenia naruszenia ochrony danych w postaci problemów związanych z działaniem serwera, a następnie dokonała zgłoszenia uzupełniającego. W wyniku naruszenia objętego zgłoszeniem **nieznana osoba uzyskała dostęp do bazy 140.699 klientów** w tym do danych takich jak imię i nazwisko, poziom wykształcenia, adres e-mail, dane dotyczące zatrudnienia, adres e-mail osoby, której klient chce polecić pożyczkę, dane dotyczące zarobków, dane dotyczące stanu cywilnego, numer telefonu (stacjonarnego, komórkowego, wcześniej używanego numeru telefonu), numer PESEL, narodowość, numer NIP, hasło, miejsce urodzenia, adres korespondencyjny, adres zameldowania, numer telefonu do miejsca pracy oraz numer rachunku bankowego. Dane były wykorzystane do szantażu spółki i żądania okupu.

W toku wszczętego postępowania okazało się, że **ID Finance Poland nie zareagowała odpowiednio na wiadomość mailową w języku angielskim od niezależnego badacza dotyczącą luk w zabezpieczeniach**. Luka powstała poprzez nieprawidłowe uruchomienie firewalla przez podwykonawcę ID Finance Poland w trakcie restartu serwera, w wyniku czego jeden z portów pozostał otwarty.

Dodatkowo hasła użytkowników przechowywane były w otwartym tekście, bez szyfrowania/hashowania. Uzyskanie dostępu przez nieznaną osobę nastąpiło w wyniku opóźnionej (10 dni) reakcji administratora na otrzymaną wiadomość o luce w zabezpieczeniach.

Wnioski dla administratora:

1. Każdy komunikat otrzymywany przez administratora dotyczący nieprawidłowego funkcjonowania systemu, który obejmuje przetwarzanie danych osobowych powinien być traktowany przez administratora poważnie i analizowany w takim czasie, który umożliwiłby zaraportowanie naruszenia do UODO w ciągu 72 godzin a także powiadomienie osób, których dane dotyczą.
2. W przypadku jakichkolwiek wątpliwości, mając w szczególności na względzie charakter i zakres przetwarzanych danych oraz ryzyko wiążące się z ich np. przypadkowym udostępnieniem, administrator powinien zgłosić naruszenie organowi nadzorczemu, nawet jeśli taka ostrożność mogłaby się okazać nadmierna.
4. Administrator powinien wdrożyć i stosować procedury umożliwiające sprawną obsługę zgłoszeń z uwzględnieniem kontaktu z podwykonawcami jak również procedury określających regularne testowanie, mierzenie i ocenianie skuteczności wdrożonych środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych.
3. Przechowywanie haseł użytkowników **w postaci jawnej, co w przypadku nie zastosowania innych środków technicznych i organizacyjnych mających na celu zapewnienie bezpiecznego przetwarzania w tym zakresie, stanowi również o naruszeniu ochrony danych osobowych.**

Treść decyzji dostępna pod linkiem: https://uodo.gov.pl/decyzje/DKN.5130.1354.2020

Śląski Uniwersytet Medyczny w Katowicach

5 stycznia 2021 r. Prezes UODO wydał decyzję DKN.5131.6.2020, w której nałożył na Śląski Uniwersytet Medyczny w Katowicach karę pieniężną w wysokości **25.000**

złotych za niezgłoszenie Prezesowi UODO naruszenia ochrony danych osobowych oraz niezawiadomienie o naruszeniu ochrony danych osobowych, bez zbędnej zwłoki, osób, których dane dotyczą. Ponadto Prezes UODO zobowiązał Uniwersytet do zawiadomienia studentów o naruszeniu.

Okoliczności nałożenia kary:

Do UODO wpłynęły od kilkunastu osób informacje o naruszeniu ochrony danych osobowych. W wyniku wszczętego postępowania ujawniono, że naruszenie polegało na **umieszczeniu na platformie e-learningowej nagrań egzaminów praktycznych z pediatrii z udziałem studentów**. Nagrania te były dostępne dla każdej osoby posiadającej link, bez konieczności logowania, jednak linki zostały udostępnione wyłącznie innym studentom i wykładowcom. **Nagrania utrwalały dane z dowodów osobistych i legitymacji studenckich studentów (w tym np. numer PESEL).**

Wnioski dla administratora:

1. W kontekście zgłoszenia naruszenia do UODO nie jest istotne czy nieuprawniona osoba faktycznie zapoznała się lub weszła w posiadanie danych osobowych, w przypadku gdy, w wyniku działania administratora, uzyskała taką możliwość. Uzależnianie reakcji administratora od ziszczenia się podejrzewanych ryzyk jest działaniem sprzecznym w RODO.
2. Ujawnienie nagrań na których widać wizerunki oraz głosy osób, jak również PESELE lub numery dowodów osobistych, w kontekście innych danych takich jak: rok studiów, grupa, etc. oznacza, że występuje wysokie ryzyko naruszenia praw i wolności i takie naruszenie należy zaraportować do UODO i powiadomić osoby, których dane dotyczą.
3. Fakt, że do danych miały dostęp wyłącznie osoby pozostające w związku z administratorem (studenci, wykładowcy) nie daje w tym przypadku podstaw do traktowania ich jako „odbiorców zaufanych", bo nie daje gwarancji co do intencji tych osób, a tym samym nie ocenić ryzyka naruszenia praw i wolności jako mniejsze.

Treść decyzji dostępna pod linkiem: https://uodo.gov.pl/decyzje/DKN.5131.6.2020

Kontakt

W przypadku dodatkowych pytań zachęcamy do bezpośredniego kontaktu z naszymi ekspertami.

Anna Matusiak-Wekiera
Radca prawny

Head of Data Protection/
Compliance Practice

anna.matusiak-wekiera@jdp-law.pl

AUTOR TEKSTU:

Krzysztof Bąk

Radca prawny
Associate

krzysztof.bak@jdp-law.pl