Polecamy Państwu lekturę opracowań decyzji Prezesa Urzędu Ochrony Danych Osobowych, które są źródłem wskazówek dla administratorów m.in. w zakresie doboru środków technicznych i organizacyjnych przy przetwarzaniu danych osobowych oraz zagadnień z obszaru analizy ryzyka. Prezes w swoich decyzjach wskazuje szczegółowo, na czym polega analiza ryzyka zarówno na potrzeby zastosowania adekwatnych środków technicznych i organizacyjnych – aby przetwarzanie odbywało się zgodnie z RODO, jak również na potrzeby zgłaszania naruszeń ochrony danych. W newsletterze przytaczamy także okoliczności nałożenia najwyższej jak dotychczas kary finansowej nałożonej, co ciekawe, nie tylko na administratora, ale również na podmiot przetwarzający. Zachęcamy do lektury.

Utrata danych osobowych w wyniku włamania

W decyzji o sygnaturze DKN.5131.11.2020 z dnia 30 czerwca 2021 r. Prezes UODO nałożył na Fundację Promocji Mediacji i Edukacji Prawnej LEX NOSTRA z siedzibą w Warszawie, karę pieniężną w kwocie **13.644** złotych z tytułu:

- niezgłoszenia naruszenia ochrony danych osobowych Prezesowi UODO,
- a także niezawiadomienia o tym fakcie osób, których dane dotyczą.

Okoliczności sprawy:

Prezes UODO wszczął postępowanie wobec Fundacji w związku z zawiadomieniem o podejrzeniu naruszenia przepisów o ochronie danych osobowych polegającego na kradzieży teczek z danymi 96 beneficjentów Fundacji, takich jak imię i nazwisko, adres do korespondencji, numer telefonu oraz prawdopodobnie numer ewidencyjny PESEL. Teczki z dokumentami zostały skradzione pomimo stosowania licznych procedur bezpieczeństwa i zabezpieczeń lokalu. W efekcie Prezes UODO

stwierdził naruszenie przepisów dotyczących obowiązku zgłoszenia naruszenia ochrony danych do organu, jak również obowiązku powiadomienia osób fizycznych, których dotyczyło zdarzenie, z uwagi na wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Wnioski dla administratorów:

1. W przypadku wysokiego ryzyka dla osób fizycznych, których dotyczyło naruszenie – administrator zobowiązany jest do **szybkiego poinformowania** tych osób o naruszeniu ich danych osobowych. Brak szybkiego działania po stronie administratora może skutkować pozbawieniem tych osób możliwości przeciwdziałania potencjalnym szkodom.
2. Ryzyko należy oszacować na podstawie obiektywnej i rzeczowej analizy (z perspektywy osoby której dotyczyło naruszenie). **Stosowanie gotowych kalkulatorów oceny poziomu ryzyka może mieć charakter pomocniczy, nie powinno natomiast stanowić wyłącznej podstawy oceny poziomu ryzyka.**
3. Dla oceny ryzyka znaczenie może mieć fakt, że administrator nie jest w stanie dokładnie wskazać kategorii danych osobowych zawartych w utraconej dokumentacji, co mogło przyczynić się do niewłaściwego oszacowania przez niego ryzyka naruszenia (zaniżenia oceny).
4. Stosowanie procedur bezpieczeństwa oraz zabezpieczeń lokalu siedziby nie stanowi przesłanki wyłączającej odpowiedzialność za naruszenie ochrony danych osobowych. Podobnie zgłoszenie sprawy karnej w związku z włamaniem, w wyniku którego utracone zostały dane osobowe, **nie stanowi podstawy do zaniechania zgłoszenia naruszenia organowi nadzorczemu w zakresie ochrony danych osobowych.**

Treść decyzji Prezesa UODO znajdą Państwo pod linkiem:

https://uodo.gov.pl/decyzje/DKN.5131.11.2020

Utrata danych przechowywanych na niezabezpieczonym nośniku pamięci zewnętrznej

W decyzji o sygnaturze DKN.5131.22.2021 z dnia 13 lipca 2021 r. Prezes UODO nałożył karę w wysokości **10.000** złotych na Prezesa Sądu Rejonowego w Zgierzu w związku z niewdrożeniem odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania danych osobowych. W konsekwencji doszło do naruszenia ochrony danych osobowych polegającego na utracie danych z zagubionego nośnika.

Okoliczności sprawy:

Prezes Sądu Rejonowego z Zgierzu dokonał zgłoszenia naruszenia ochrony danych osobowych do UODO, wskazując na utratę danych osobowych 400 osób podlegających nadzorowi kuratorskiemu w zakresie imion i nazwisk, dat urodzenia, adresów zamieszkania lub pobytu, numerów PESEL, danych dotyczących zarobków i/lub posiadanego majątku, serii i numerów dowodów osobistych, numerów telefonów, danych dotyczących zdrowia oraz danych dotyczących wyroków skazujących. **Naruszenie spowodowane było zagubieniem nośnika przez kuratora, na którym przechowywane były dane.**

Wnioski dla administratorów:

1. Administrator nie może powoływać się na brak stosowania odpowiednich zasad bezpieczeństwa obowiązujących w organizacji administratora przez osobę, która spowodowała naruszenie ochrony danych, **gdyż to on jest odpowiedzialny za wprowadzenie i stosowanie zabezpieczeń zapewniających bezpieczeństwo przetwarzanych danych osobowych.**
2. Prezes UODO uznał, że do naruszenia zasady poufności i integralności danych doszło już poprzez wydanie przez administratora do użytku służbowego kuratorom sądowym **niezabezpieczonego przenośnego nośnika pamięci oraz zobowiązanie ich do wdrożenia zabezpieczeń tej pamięci we własnym zakresie.**
3. Administrator danych osobowych jest zobowiązany nie tylko do wprowadzenia i stosowania odpowiednich zabezpieczeń, **ale również sprawdzania ich skuteczności.**
4. Zorganizowanie szkoleń dla pracowników nie jest środkiem organizacyjnym, który pozwoli zminimalizować lub wyeliminować ryzyka zagubienia nośnika. Szkolenie nie zastąpi również rozwiązań o charakterze technicznym.
5. Wymaga się prowadzenia **cyklicznej weryfikacji** całego systemu ochrony danych osobowych **pod kątem prawidłowości, jak i skuteczności** implikowanych rozwiązań technicznych i organizacyjnych. Jak wskazano w decyzji UODO, **dokonywanie doraźnych kontroli jest niewystarczające**, a prowadzenie działań kontrolnych powinno mieć charakter zaplanowany.

Treść decyzji Prezesa UODO znajdą Państwo pod linkiem:

https://www.uodo.gov.pl/decyzje/DKN.5131.22.2021

Odpowiedzialność za utratę przesyłki

Prezes UODO w decyzji o sygnaturze DKN.5131.16.2021 z dnia 14 października 2021 r. nałożył na Bank Millennium S.A. karę pieniężną w wysokości **363.822** złotych. Powodem wydania decyzji było naruszenie polegające na:

- zaniechaniu zgłoszenia naruszenia ochrony danych osobowych w terminie 72h po stwierdzeniu naruszenia oraz
- niezawiadomieniu o naruszeniu osób, których dane dotyczą.

Okoliczności sprawy:

Skarga, na podstawie której wszczęto postępowanie, została wniesiona w wyniku utraty danych podczas procedury zakładania konta w Banku. W toku postępowania ustalono, że dane dwóch osób w zakresie imienia i nazwiska, numeru PESEL, adresu zameldowania, numerów rachunków bankowych, numeru CIF (numer identyfikacyjny nadawany klientom Banku) zostały utracone w trakcie transportu kurierskiego pomiędzy oddziałami Banku. Administrator ocenił poziom ryzyka tego naruszenia jako średni (metodologia ENISA), w związku z powyższym nie dokonał samodzielnego zawiadomienia osób, których dane zostały utracone, ani nie powiadomił Prezesa UODO.

Wnioski dla administratorów:

1. Administrator zwolniony jest z obowiązku powiadamiania organu nadzorczego o naruszeniu, jeśli w wyniku przeprowadzonego badania okaże się, że **nie ma prawdopodobieństwa wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych. Organ nadzorczy będzie mógł zwrócić się do administratora o uzasadnienie decyzji o niezgłaszaniu naruszenia.**
2. Dokonanie skrupulatnej oceny ryzyka pozwala na właściwą reakcję organu nadzorczego, zwiększając tym samym szansę na uniknięcie negatywnych skutków naruszenia dla osób fizycznych. Ocena naruszenia przeprowadzona przez administratora pod kątem ryzyka naruszenia praw lub wolności osób fizycznych powinna być dokonana przez pryzmat osoby dotkniętej naruszeniem.
3. Obowiązek zawiadomienia osoby fizycznej o naruszeniu jej danych osobowych nie jest uwarunkowany od występowania dla niej negatywnych skutków, lecz już od samej możliwości wystąpienia takiego ryzyka.

4. **Przy ocenie ryzyka na potrzeby obowiązków administratora związanych z naruszeniem nie jest istotne to, czy nieuprawniony odbiorca faktycznie wszedł w posiadanie i zapoznał się z danymi osobowymi innych osób, lecz to, że wystąpiło takie ryzyko,** a w konsekwencji również potencjalnie wystąpiło ryzyko naruszenia praw lub wolności podmiotów danych, które z uwagi na zakres danych należy uznać jako wysokie.
5. Operator pocztowy jest jedynie pośrednikiem działań podjętych przez administratora, **nie powoduje to zatem zdjęcia odpowiedzialności za utratę przetwarzanych danych przez administratora.**

Treść decyzji Prezesa UODO znajdą Państwo pod linkiem:

https://www.uodo.gov.pl/decyzje/DKN.5131.16.2021

Politechnika Warszawska

W decyzji o sygnaturze DKN.5130.2559.2020 z dnia 9 grudnia 2021 r Prezes UODO nałożył karę pieniężną w wysokości **45.000** złotych na Politechnikę Warszawską. Naruszenie przepisów o ochronie danych osobowych dotyczyło w szczególności:

- niezastosowania odpowiednich środków technicznych i organizacyjnych w celu zapewnienia poufności usług przetwarzania danych w systemie informatycznym,
- braku właściwego uwzględnienia ryzyka związanego z przetwarzaniem haseł użytkowników w aplikacji.

Okoliczności sprawy:

Politechnika Warszawska, będąca administratorem danych studentów, wykładowców oraz kandydatów na studia umieszczonych w systemie informatycznym uczelni, dopuściła do naruszenia danych osobowych 5013 osób w zakresie imienia i nazwiska, imion rodziców, daty urodzenia, adresu zamieszkania lub pobytu, numeru PESEL, adresu e-mail, nazwy użytkownika i/lub hasła, nazwiska rodowego matki, serii i numeru dowodu osobistego oraz numeru telefonu. Administrator, stwierdzając wysokie ryzyko naruszenia praw i wolności osób, powiadomił odpowiednie organy ścigania oraz zabezpieczył zasoby informatyczne będące przedmiotem naruszenia. Utrata danych była spowodowana zastosowaniem złośliwego narzędzia (pliku typu backdoor), które nieuprawnionemu umożliwiło uzyskanie dostępu do danych osobowych. W toku postępowania ustalono, że pomimo stosowania środków technicznych, okazały się one niewystarczające w zabezpieczeniu danych.

Wnioski dla administratorów:

1. Każdorazowo wprowadzanie środków technicznych powinno następować z dokonaniem **uprzedniej analizy ryzyka** dla procesu przetwarzania danych osobowych. W innym wypadku zachodzi wysoka wątpliwość co do skuteczności i adekwatności stosowanych środków.
2. Stosowanie funkcji skrótu (inaczej też: haszowanie) w stosunku do haseł przechowywanych w systemach teleinformatycznych **jest jednym z najczęściej spotykanych środków mających zapewnić poufność hasła i ograniczyć jego znajomość wyłącznie do osoby, która się nim posługuje.** Ogranicza się w ten sposób negatywne konsekwencje związane z potencjalnym ryzykiem wykorzystania takiego hasła przez osobę, która w sposób nieuprawniony uzyskuje do niego dostęp.

Treść decyzji Prezesa UODO znajdą Państwo pod linkiem:

https://www.uodo.gov.pl/decyzje/DKN.5130.2559.2020%20

Santander Bank Polska S.A.

19 stycznia 2022 roku Prezes UODO wydał decyzję DKN.5131.33.2021, w której nałożył karę pieniężną w wysokości **545.748** złotych na Santander Bank Polska S.A. z siedzibą w Warszawie za niezawiadomienie, bez zbędnej zwłoki, o naruszeniu poufności danych osobowych osób, których dane dotyczą.

Okoliczności sprawy:

Pracownik Banku po ustaniu stosunku pracy nadal miał dostęp do platformy PUE ZUS, która zawierała dane osobowe pracowników Banku takie jak numery PESEL, wraz z imionami i nazwiskami, adresami zamieszkania lub pobytu oraz informacjami o zwolnieniach lekarskich, tj. danymi dotyczącymi zdrowia. W trakcie postępowania ustalono, że były pracownik nie tylko miał dostęp, ale również korzystał z bazy danych kilkukrotnie, także po ustaniu stosunku pracy.

Wnioski dla administratorów:

1. Jak wskazuje Prezes UODO, s**tatus odbiorcy zaufanego posiadają podmioty, które działają w strukturach danej organizacji albo są np. dostawcą, z którego usług administrator stale korzysta. Pomiędzy podmiotami istnieje więź faktyczna, a nierzadko prawna, która pozwala na ocenę stopnia zaufania stron.** W przypadku takiego odbiorcy administrator może przyjąć domniemanie, że zna on obowiązujące

procedury w zakresie ochrony danych osobowych i że zachowa się w odpowiedni sposób.
2. Nie można uznać, że były pracownik zachowa się w sposób adekwatny do okoliczności – zatem nie można go uznać za podmiot zaufany.
3. Administrator nie może uchylać się od obowiązku zawiadamiania o naruszeniu ochrony danych osobowych osób, których dane dotyczą z uwagi na brak ściśle określonego kręgu takich osób, gdyż w takim przypadku administrator może przekazać informacje w formie np. komunikatu publicznego.

Treść decyzji Prezesa UODO znajdą Państwo pod linkiem:

https://uodo.gov.pl/decyzje/DKN.5131.33.2021

Rekordowa kara za nienależytą kontrolę nad przetwarzaniem danych osobowych

Prezes UODO w decyzji DKN.5130.2215.2020 z dnia 19 stycznia 2022 roku nałożył kary pieniężne w wysokości:

- **4.911.732** złotych na administratora danych Fortum Marketing and Sales Polska S.A. z siedzibą w Gdańsku za niewdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych oraz niezweryfikowanie podmiotu przetwarzającego w zakresie zapewnienia wdrożenia odpowiednich środków technicznych i organizacyjnych spełniających wymogi z RODO,

- **250.135** złotych na podmiot przetwarzający PIKA Sp. z o.o. z siedzibą w Gdańsku za niewdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych.

Okoliczności sprawy:

Procesor dokonywał zmian w systemie teleinformatycznym. W wyniku tych zmian utworzono dodatkową bazę danych klientów. Okazało się, że serwer, na którym znajdowała się baza nie został odpowiednio zabezpieczony, w wyniku czego doszło do jej skopiowania przez nieuprawnione osoby. Warto dodać, że administrator dowiedział się o tym fakcie od internautów, którzy stwierdzili, że mają nieuprawniony dostęp do bazy. Ujawnione dane dotyczyły ponad 120.000 osób.

Wnioski dla administratorów:

1. Administrator zobowiązany jest do **wymagania** od podmiotu przetwarzającego **analizy ryzyka oraz koncepcji zmian projektów funkcjonalnych i technicznych oraz alternatywnych rozwiązań** w przypadku wprowadzania przez procesora czynności poprawiających wydajność usługi.
2. Mimo stosowanych przez administratora procedur bezpieczeństwa jest on zobligowany **do sprawowania nadzoru nad procesem wprowadzania zmian w zakresie obowiązujących standardów**.
3. Wdrożenie środków bezpieczeństwa przez administratora nie może mieć charakteru jednorazowego. Jest to ciągły proces, w którym administrator powinien dokonywać weryfikacji i uaktualnień przyjętych rozwiązań.
4. Zawarcie w umowie powierzenia danych osobowych postanowienia o dokonywaniu przez administratora cyklicznych **audytów** u podmiotu przetwarzającego w trakcie przetwarzania danych osobowych powinno mieć **charakter rzeczywisty**, tzn. administrator nie może powoływać się jedynie na postanowienie umowne, ale musi wykazać, że takie kontrole przeprowadzał.

Treść decyzji Prezesa UODO znajdą Państwo pod linkiem:

https://www.uodo.gov.pl/decyzje/DKN.5130.2215.2020

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

Krzysztof Bąk
Radca prawny
Associate
krzysztof.bak@jdp-law.pl