Rejestr kar pieniężnych Prezesa UODO

Ogólne rozporządzenie o ochronie danych (RODO) jest… ogólnym aktem prawnym. W wielu sytuacjach jego przepisy wymagają interpretacji.

Z pomocą przychodzi obserwowanie działań praktyków. W tej rubryce przyglądamy się karom Prezesa UODO, których nałożenie wzbudziło najwięcej emocji. Chodzi oczywiście o kary pieniężne.

Celem przypomnienia – RODO wyróżnia dwa przedziały kar pieniężnych:

- **do 10 mln euro**, a w przypadku przedsiębiorstwa do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego,
- **do 20 mln euro**, a w przypadku przedsiębiorstwa do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

Ustawa o ochronie danych osobowych przewiduje jednak mniejsze kary dla podmiotów sektora finansów publicznych:

- jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–12 i 14 *Ustawy o finansach publicznych*, instytuty badawcze i Narodowy Bank Polski – w wysokości **do 100 000 złotych** (tj. np. szkoły, uczelnie, szpitale, ZUS, gminy, NFZ, sądy),
- jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 13 *Ustawy o finansach publicznych* – w wysokości **do 10 000 złotych** (tj. np. teatry, opery, filharmonie, kina, muzea, biblioteki, domy kultury, galerie sztuki).

Nałożenie każdej kary łączy się z wydaniem decyzji administracyjnej wraz z uzasadnieniem.

Żebyście nie musieli sami przedzierać się przez gąszcz paragrafów i skomplikowanych uzasadnień, prowadzimy dla Was bieżącą analizę wszystkich kar pieniężnych nałożonych przez organ nadzorczy!

Ostatnia aktualizacja: 07.03.2022 r.

Decyzja	Decyzja Prezesa UODO z dnia 15 marca 2019 r. ZSPR.421.3.2018
Ukarany podmiot	Bisnode Polska sp. z o.o.
Kwota kary pieniężnej	943 470,00 PLN
Naruszone przepisy RODO	• art. 14 ust. 1 – 3 RODO – obowiązki związane z podawaniem informacji o przetwarzaniu danych osobowych w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą (tzw. obowiązek informacyjny wtórny)
Kontekst	Bisnode Polska sp. z o.o. jest globalnym dostawcą informacji gospodarczych i biznesowych. Spółka posiada dostęp do bazy danych firm krajowych i zagranicznych. Decyzja Prezes UODO dotyczyła postępowania związanego z działalnością spółki polegająca na pozyskiwaniu danych osobowych ze źródeł publicznie dostępnych, m.in. z Centralnej Ewidencji i Informacji Działalności Gospodarczej (CEiDG), i przetwarzaniu ich w celach zarobkowych. UODO weryfikował niedopełnienie obowiązku informacyjnego wobec osób fizycznych prowadzących działalność gospodarczą – przedsiębiorców, którzy aktualnie ją prowadzą bądź tę działalność zawiesili, jak i tych, którzy prowadzili ją w przeszłości. Spółka spełniła obowiązek informacyjny, podając informacje wymagane przepisami art. 14 ust. 1-3 RODO jedynie wobec tych osób, do których posiadała adresy e-mail. W przypadku pozostałych osób tego nie zrobiono. Bisnode Polska sp. z o.o. tłumaczyła to postępowanie zbyt wysokimi kosztami takiej operacji. Treść klauzuli informacyjnej została jedynie zamieszczona na stronie internetowej spółki. W ocenie Prezesa UODO takie działanie było niewystarczające. Mając dane kontaktowe do poszczególnych osób spółka powinna spełnić wobec nich obowiązek informacyjny, poinformować m.in. o: swoich danych, skąd ma dane tych osób, w jakim celu i jak długo zamierza je przetwarzać oraz o przysługujących osobom prawach na gruncie RODO. Zdaniem Prezesa UODO spółka dysponując adresami korespondencyjnymi i numerami telefonów mogła spełnić obowiązek informacyjny wobec osób, których dane przetwarza. UODO uznał, że naruszenie miało charakter umyślny, ponieważ spółka miała świadomość istnienia obowiązku podania stosownych informacji, jak i konieczności bezpośredniego informowania osób. Wymierzając karę, organ wziął pod uwagę również fakt, że spółka nie podjęła żadnych działań zmierzających do usunięcia naruszenia ani nie zadeklarowała takiego zamiaru.

	Bisnode Polska sp. z o.o. wskazuje, że działalność firmy kontrolowana była pod tym katem w dwóch innych krajach i nie dopatrzono się żadnych uchybień. Zapowiedziała też odwołanie się od decyzji.

Komentarz eksperta

Krystian Dobosz, starszy specjalista ds. ochrony danych osobowych

Decyzja UODO pozostawia pewien niedosyt. Szkoda, że nie wskazano metodologii badania możliwości zwolnienia się ze spełnienia wtórnego obowiązku informacyjnego, tj. kiedy występuje niewspółmiernie duży wysiłek. Uznano, że kwota prawie 30 mln złotych na wysyłkę listów drogą pocztową, nie stanowi niewspółmiernego wysiłku by Spółka mogła skorzystać ze zwolnienia–mimo, że wskazała, że jest inaczej.

Takie arbitralne podejście zawarte w decyzji może powodować brak jednoznacznych wytycznych dla uczestników rynku i pewności jak stosować zwolnienie z art. 14 RODO, co w przyszłości będzie kłopotem dla firm.

Decyzja	Decyzja Prezesa UODO z dnia 25 kwietnia 2019 r. ZSPR.440.43.2019
Ukarany podmiot	Dolnośląski Związek Piłki Nożnej
Kwota kary pieniężnej	55 750,50 PLN
Naruszone przepisy RODO	• art. 5 ust. 1 lit. f RODO – zasada integralności i poufności • art. 32 ust. 1 lit. b RODO – zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania • art. 32 ust. 2 RODO – obowiązek oceny stopnia bezpieczeństwa przetwarzania przy uwzględnieniu, w szczególności ryzyka wiążącego się z przetwarzaniem, w szczególności wynikającego z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych
Kontekst	Dolnośląski Związek Piłki Nożnej (DZPN) upublicznił w sieci dane osobowe sędziów, którym przyznano licencje sędziowskie w 2015 roku (585 osób). Podano jednak nie tylko ich imiona i nazwiska, ale także adresy zamieszkania oraz numery PESEL. Tymczasem nie ma żadnych podstaw prawnych, by w Internecie dostępny był aż tak szeroki zakres danych sędziów. Upubliczniając je, administrator stwarzał potencjalne ryzyko ich bezprawnego wykorzystania, np. do podszycia się pod te osoby w celu zaciągania pożyczek czy innych zobowiązań. Wprawdzie DZPN sam dostrzegł swój błąd, czego dowodzi zgłoszenie naruszenia ochrony danych osobowych Prezesowi UODO, to fakt, iż próby jego usunięcia były nieskuteczne, przesądził o nałożeniu kary. W zgłoszeniu DZPN wskazał bowiem, iż naruszenie trwało od października 2015 roku do lipca 2018 roku, natomiast w styczniu 2019 roku te dane były nadal dostępne, a definitywne usunięcie naruszenia nastąpiło dopiero po wszczęciu postępowania przez Prezesa UODO. Ustalając wysokość kary Prezes UODO wziął pod uwagę m.in. czas trwania naruszenia oraz fakt, że dotyczyło ono dużej grupy osób. Uznał, że mimo iż ostatecznie naruszenie zostało usunięte, to miało poważny charakter. Prezes UODO uwzględnił również okoliczności łagodzące, którymi były m.in. dobra współpraca administratora z organem nadzoru czy brak dowodów na to, że powstały szkody po stronie osób, których dane ujawniono.

Komentarz eksperta

Tomasz Wasilczyk, starszy specjalista ds. ochrony danych osobowych

Decyzja Prezesa UODO o nałożeniu kary na Dolnośląski Związek Piłki Nożnej nie budzi wątpliwości, gdyż ukarany podmiot nie dochował należytej staranności w zakresie usunięcia naruszenia.

Jednym z podstawowych obowiązków administratora jest zapewnienie bezpieczeństwa przetwarzanych danych. To bezpieczeństwo można osiągnąć wyłącznie za pomocą efektywnych działań poprzez wdrożenie odpowiednich środków organizacyjnych i technicznych. Liczy się skuteczność podjętych działań, a nie dobre intencje. Ma to szczególne znaczenie w sytuacji współpracy z podmiotami zewnętrznymi.

Warto również zwrócić uwagę na okoliczności, jakie Prezes UODO wziął pod uwagę ustalając wysokość kary. Organ wskazał, iż samodzielne zgłoszenie naruszenia nie stanowi okoliczności łagodzącej, gdyż jest to wymagane przepisami prawa. Z drugiej strony usunięcie naruszenia w trakcie postępowania może złagodzić jej wymiar.

Decyzja	Decyzja Prezesa UODO z dnia 10 września 2019 r. ZSPR.421.2.2019
Ukarany podmiot	Morele.net sp. z o.o.
Kwota kary pieniężnej	2 830 410,00 PLN
Naruszone przepisy RODO	• art. 5 ust. 1 lit. a RODO – zasada zgodności z prawem, rzetelności i przejrzystości • art. 5 ust. 1 lit. f RODO – zasada integralności i poufności • art. 5 ust. 2 RODO – zasada rozliczalności • art. 6 ust. 1 RODO – podstawy prawne przetwarzania danych osobowych • art. 7 ust. 1 RODO – obowiązek wykazania, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych • art. 24 ust. 1 RODO – obowiązek wdrażania odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO i wykazania podjętych działań w tym zakresie oraz w razie potrzeby poddawania tych środków przeglądom i uaktualnianiu • art. 25 ust. 1 RODO – zasada *privacy by design* • art. 32 ust. 1 lit. b RODO – zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania • art. 32 ust. 1 lit. d RODO – regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania • art. 32 ust. 2 RODO – obowiązek oceny stopnia bezpieczeństwa przetwarzania przy uwzględnieniu, w szczególności ryzyka wiążącego się z przetwarzaniem, w szczególności wynikającego z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych
Kontekst	Kara, to skutek wycieku danych klientów sklepów internetowych prowadzonych przez Morele.net. Pierwsze doniesienia sugerujące naruszenie pojawiły się już w listopadzie 2018 r. Hakerzy uzyskali wówczas dostęp do bazy danych ponad 2 milionów klientów. W grudniu 2018 r. spółka poinformowała o incydencie Prezesa UODO, policję, jak i osoby, których dane dostały się w niepowołane ręce. W styczniu 2018 r. organ rozpoczął postępowanie wyjaśniające, które zakończyła decyzja o ukaraniu spółki. Zdaniem UODO, zastosowane przez Morele.net środki organizacyjne i techniczne ochrony danych, nie były odpowiednie do istniejącego ryzyka związanego z ich

	przetwarzaniem. Zabrakło m.in. odpowiednich procedur reagowania na wypadek pojawiania się nietypowego ruchu w sieci. W swojej decyzji Prezes UODO wskazał, że tak wysoki wymiar kary wynika ze znacznej wagi czynu i liczby osób poszkodowanych, których bezpieczeństwo zostało poważnie narażone. Przedstawiciele Morele.net wskazują, że firma nie zgadza się z oceną zebranego materiału dowodowego i odwoła się od decyzji.

Komentarz eksperta

Przemysław Zegarek, Prezes Lex Artist sp. z o.o., ekspert ds. ochrony danych osobowych

Moją uwagę najbardziej zwróciło to, że jest to pierwsza kara dotycząca zastosowanych środków zabezpieczeń IT (ich odpowiedniości i proporcjonalności). W treści decyzji znajdziemy listę norm i wytycznych z obszaru Security IT, na której bazowali pracownicy Regulatora. Decyzja może być więc bardzo cennym źródłem informacji dla każdego IODa lub innej osoby, która chce zadbać o obszar zabezpieczeń IT.

Więcej o wytycznych i normach, na które powołał się Regulator przeczytasz tutaj: https://blog-daneosobowe.pl/co-to-sa-odpowiednie-srodki-zabezpieczen-wedlug-rodo/

Marcin Szkutnik, radca prawny, ekspert ds. ochrony danych osobowych

Decyzja Prezesa UODO w sprawie spółki Morele.net jest ważna dla polskiego systemu ochrony danych osobowych, nie tylko ze względu na najwyższą karę sięgającą blisko 3 mln zł. Przede wszystkim, decyzja ta, koncertuje się na kwestii stosowania środków technicznych i organizacyjnych, a więc tych zagadnień co do których RODO nie zawierają precyzyjnych wytycznych. W tej sprawie organ uznał, że spółka nie dochowała należytej staranności w doborze środków technicznych i organizacyjnych co skutkowało wystąpieniem ataku hakerskiego. Uzasadniając swoje stanowisko, Prezes UODO wskazał m.in. na normę PN – ISO/IEC 29115:2017 07, opracowanie NIST 800-63B czy dokument organizacji OWASP jako źródła wytycznych dla doboru właściwych środków. Tak wyraźne powołanie się na konkretne normy i dokumenty jest na pewno dużą wartością tej decyzji i może stanowić istotną wskazówkę w tym zakresie dla innych administratorów.

Małgorzata Zdunek, ekspert ds. ochrony danych osobowych

Decyzja wzbudziła duże emocje zarówno wśród ekspertów, jak i podmiotów, które na co dzień przetwarzają dane osobowe. Emocje są tym większe, że mówimy tu o prawie 3 mln złotych kary nałożonych na spółkę, która stała się ofiarą ataku hakerskiego. Nie było to zatem działanie umyślne. Naruszenie nie miało również charakteru wewnętrznego.

Spółka oszacowała ryzyko i wdrożyła odpowiednie według niej zabezpieczenia przetwarzanych danych. Postąpiła zatem zgodnie z zasadą wprowadzoną przez RODO, czyli „*zrób to sam*". W mojej

ocenie, niedopuszczenie do postępowania dowodu z opinii biegłego, w znacznym stopniu osłabia argumentację organu o zastosowaniu przez Morele.net niewystarczających zabezpieczeń technicznych.

Nie ulega wątpliwości, że za wystąpienie tego naruszenia, spółka jako administrator powinna ponieść odpowiedzialność. Pytanie tylko, czy aż w takim wymiarze.

Decyzja	Decyzja Prezesa UODO z dnia 18 października 2019 r. ZSPU.421.3.2019
Ukarany podmiot	Burmistrz Aleksandrowa Kujawskiego
Kwota kary pieniężnej	40 000,00 PLN
Naruszone przepisy RODO	• art. 5 ust. 1 lit. a RODO – zasada zgodności z prawem, rzetelności i przejrzystości • art. 5 ust. 1 lit. f RODO – zasada integralności i poufności • art. 5 ust. 1 lit. e RODO – zasada ograniczenia przechowywania danych • art. 5 ust. 2 RODO – zasada rozliczalności • art. 24 ust. 1 oraz 2 RODO – obowiązek wdrażania odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO i wykazania podjętych działań w tym zakresie oraz w razie potrzeby poddawania tych środków przeglądom i uaktualnianiu, a gdy jest to proporcjonalne wdrożenie w tym celu odpowiednich polityk ochrony danych • art. 28 ust. 3 RODO – obowiązek zawarcia umowy powierzenia danych osobowych w przypadku udostępnia danych podmiotom przetwarzającym • art. 30 ust. 1 lit. d oraz f RODO- obowiązek wskazania w rejestrze czynności przetwarzania odbiorców danych oraz terminów usunięcia danych • art. 32 ust. 1 lit. b RODO – zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania • art. 32 ust. 1 lit. c RODO – zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego
Kontekst	Kara jest efektem kontroli, której zakres obejmował sposób przetwarzania danych w ramach procesu wysyłki korespondencji i prowadzenia Biuletynu Informacji Publicznej (BIP) oraz sposób prowadzenia rejestru czynności przetwarzania oraz dokumentowania naruszeń ochrony danych. Po przeprowadzonej kontroli Prezes UODO stwierdził, że: - doszło do udostępniania danych osobowych bez podstawy prawnej tj. bez zawarcia umów powierzenia danych. Dotyczyło to współpracy z firmą, na której serwerach znajdowały się zasoby BIP oraz firmą zajmująca się obsługą serwisową BIP, - znajdujące się w BIP dane osobowe (zawarte w oświadczeniach majątkowych oraz informacjach o wynikach naboru na wolne stanowiska) były przechowywane przez okres dłuższy niż wynikało to z właściwych przepisów prawa lub dłużej niż wynikało z celów, dla których zostały one zgromadzone, co stanowiło naruszenie zasady ograniczenia przechowania danych,

	- nie zostały wdrożone procedury wewnętrzne w postaci odpowiednich polityk ochrony danych dotyczące przeglądu zasobów znajdujących się w BIP z punktu widzenia ich zgodności z zasadą ograniczenia przechowywania danych, - nie została wykonana analiza ryzyka związanego korzystaniem z kanału YouTube dla celów transmisji obrad rady miejskiej i związanego z tym przetwarzania danych osobowych uczestników obrad, - materiały z posiedzeń rady miejskiej były przechowane jedynie w serwisie YouTube, co zostało uznane przez organ jako brak wdrożenia odpowiednich środków technicznych i organizacyjnych, z uwagi na fakt, w ten sposób urząd nie dysponował kopią zapasową tych nagrań, - w rejestrze czynności przetwarzania danych nie zostały wskazane obligatoryjne elementy rejestru w postaci wskazania wszystkich odbiorców danych oraz terminów usunięcia danych dla czynności przetwarzania danych związanych z publikowaniem informacji na stronach BIP. Ponadto, wszystkie te naruszenia spowodowały także naruszenie zasady rozliczalności, która wymaga od administratora, aby ten był w stanie wykazać przestrzeganie zgodności z RODO. O wymierzeniu kary zadecydował przede wszystkim brak umów powierzenia oraz nieprzestrzeganie zasady rozliczalności. Natomiast, na sam wymiar kary wpływ miały m.in.: czas trwania naruszenia (w tym to, że nieprawidłowości nie zostały usunięte ani w trakcie trwania kontroli ani później – w toku postępowania administracyjnego), umyślność naruszenia (nie zostały podjęte żadne działania mające na celu przeciwdziałaniu w przyszłości podobnym naruszeniom) oraz brak współpracy z organem nadzorczym.

Komentarz eksperta

Marcin Szkutnik, radca prawny, ekspert ds. ochrony danych osobowych

Przede wszystkim, decyzja ta, pokazuje, że także organy administracji publicznej muszą bardzo poważnie traktować stosowanie przepisów RODO. Muszą liczyć się nie tylko z kontrolami, ale też i z potencjalnymi karami pieniężnymi. W decyzji, Prezes UODO wskazał na dwa bardzo ważne elementy systemu ochrony danych osobowych: zawieranie umów powierzenia danych osobowych oraz przestrzeganie „*zasady rozliczalności*". Jak wynika z uzasadniania decyzji, stwierdzone w tym zakresie naruszenia miały decydujący wpływ na wymierzenie kary pieniężnej. O tym powinni pamiętać wszyscy administratorzy, bez względu na to czy reprezentują sektor publiczny czy prywatny.

Decyzja	Decyzja Prezesa UODO z dnia 16 października 2019 r. ZSPU.421.7.2019
Ukarany podmiot	ClickQuickNow sp. z o.o.
Kwota kary pieniężnej	201 559,50 PLN
Naruszone przepisy RODO	• art. 5 ust 1 lit. a w zw. z art. 5 ust. 2 RODO – zasada zgodności z prawem, rzetelności i przejrzystości przetwarzania danych osobowych • art. 7 ust. 3 RODO – prawo osoby, której dane dotyczą do wycofania zgody na przetwarzanie danych osobowych w dowolnym momencie • art. 12 ust. 2 RODO – obowiązki związane z ułatwianiem wykonywania praw przysługujących na gruncie RODO osobie, której dane dotyczą • art. 17 ust. 1 lit. b RODO – prawo do usunięcia danych („prawo do bycia zapomnianym") • art. 24 ust. 1 RODO – obowiązek wdrażania odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO i wykazania podjętych działań w tym zakresie oraz w razie potrzeby poddawania tych środków przeglądom i uaktualnianiu • art. 6 ust. 1RODO – podstawy prawne przetwarzania danych osobowych
Kontekst	ClickQuickNow sp. z o.o. to podmiot zajmujący się realizacją kampanii marketingowych z wykorzystaniem e-maili, SMS-ów, telemarketingu i narzędzi digitalowych. Kara pieniężna została nałożona na spółkę m.in. za utrudnianie realizacji prawa do wycofania zgody na przetwarzanie danych osobowych. Zdaniem Prezesa UODO spółka nie wdrożyła odpowiednich środków technicznych i organizacyjnych, które umożliwiałyby łatwe i skuteczne wycofanie zgody na przetwarzanie danych osobowych oraz realizację prawa do żądania usunięcia danych osobowych (prawa do bycia zapomnianym). Naruszyła tym samym określone w RODO zasady zgodności z prawem, rzetelności i przejrzystości przetwarzania danych osobowych. Prezes UODO uznał, że spółka w procesie wycofania zgody stosowała skomplikowane rozwiązania organizacyjne i techniczne. Stosowany przez spółkę mechanizm wycofania zgody, polegający na użyciu linku zamieszczonego w treści informacji handlowej, nie skutkował szybkim wycofaniem zgody. Po uruchomieniu linku, komunikaty kierowane do osoby zainteresowanej wycofaniem zgody wprowadzały ją w błąd. Ponadto spółka wymuszała podanie

	przyczyny wycofania zgody, a prawo tego nie wymaga. Co więcej, brak wskazania przyczyny skutkował przerwaniem procesu wycofania zgody. Tym samym w ocenie Prezesa UODO Spółka nie ułatwiała realizacji praw osobom, których dane przetwarzała. W decyzji Prezes Urzędu wskazał również, że Spółka przetwarzała bez podstawy prawnej dane osób, które nie są jej klientami, a od których otrzymała żądania zaprzestania przetwarzania ich danych osobowych. Ustalając wysokość kary pieniężnej, Prezes UODO nie uwzględnił żadnej okoliczności łagodzącej mającej wpływ na ostateczny wymiar kary. Uznał też, że działanie spółki było umyślne, gdyż przekazywanie osobie zainteresowanej wycofaniem zgody sprzecznych ze sobą komunikatów skutkowało tym, że wycofanie zgody nie było skuteczne. W ten sposób spółka utrudniała, czy wręcz uniemożliwiała realizację praw osób, których dane dotyczą. Spółka nie zgadza się ustaleniami stanowiącymi podstawę wydania decyzji oraz jej błędnym uzasadnieniem prawnym i zamierza złożyć skargę wobec decyzji do sądu administracyjnego.

Komentarz eksperta

Małgorzata Zdunek, ekspert ds. ochrony danych osobowych

Decyzja dotyczy jednego z podstawowych obowiązków administratora w zakresie budowania relacji z osobami, których dane dotyczą, czyli podejmowania działań w celu ułatwiania wykonywania praw przysługujących im na gruncie RODO.

Stan faktyczny opisany w decyzji, pozwala stwierdzić, że ukarana spółka w rzeczywistości z tego obowiązku się nie wywiązywała. Dwustopniowy proces dojścia do informacji o sposobie odwołania zgody, niejasne komunikaty, czy wreszcie konieczność ujawnienia powodu skorzystania z prawa – to wszystko składa się na działanie, które można określić wręcz jako utrudnianie składania żądań. W mojej ocenie, organ miał słuszność w zakwestionowaniu tego typu praktyki.

Sam fakt gromadzenia informacji o przyczynach wycofania zgody nie byłby kontrowersyjny, gdyby ich podanie nie warunkowało możliwości skorzystania z prawa. Analiza powodów, dla których podmiot nie zgadza się na dalsze przetwarzanie jego danych, pozwala administratorowi dostrzec i naprawić nieprawidłowości w relacjach z osobami, których dane dotyczą.

Decyzja	Decyzja Prezesa UODO z dnia 18 lutego 2020 r. ZSZZS.440.768.2018
Ukarany podmiot	Szkoła Podstawowa nr 2 w Gdańsku
Kwota kary pieniężnej	20 000,00 PLN
Naruszone przepisy RODO	• art. 5 ust. 1 lit. c RODO – zasada minimalizacji danych • art. 9 ust. 1 RODO – zakaz przetwarzania szczególnych kategorii danych osobowych
Kontekst	Prezes UODO nałożył karę w związku z naruszeniem polegającym na przetwarzaniu danych biometrycznych dzieci podczas korzystania przez nie ze szkolnej stołówki. Szkoła przetwarzała dane szczególnych kategorii (dane biometryczne) 680 dzieci bez podstawy prawnej, mogąc jednocześnie zastosować inne formy identyfikacji uczniów. Prezes UODO po przeprowadzeniu z urzędu postępowania administracyjnego ustalił, że szkoła korzysta z czytnika biometrycznego przy wejściu do stołówki szkolnej, który identyfikuje dzieci w celu weryfikacji uiszczenia opłaty za posiłek. Postępowanie wykazało, że szkoła pozyskuje te dane i przetwarza je na podstawie pisemnej zgody rodziców lub opiekunów prawnych. Prezes UODO uznał, że przetwarzanie danych biometrycznych nie jest niezbędne dla osiągnięcia celu, jakim jest identyfikacja uprawnienia dziecka do odebrania obiadu. Szkoła może przeprowadzić identyfikację za pomocą innych środków, które nie ingerują tak dalece w prywatność dziecka. Prezes UODO w uzasadnieniu swojej decyzji podkreślił, że szczególnej ochrony danych osobowych wymagają dzieci. Dane biometryczne zaś, mają wyjątkowy charakter w świetle podstawowych praw i wolności, dlatego również też wymagają wyjątkowej ochrony. Ewentualny ich wyciek może skutkować dużym ryzykiem naruszenia praw i wolności osób fizycznych. Organ wskazał, że zastosowanie administracyjnej kary pieniężnej w tym przypadku jest niezbędne zważywszy także na to, że Szkoła całkowicie zignorowała fakt przetwarzania danych biometryczny dzieci poprzez stwierdzenie, że nie przetwarza danych w ww. zakresie. W ocenie Prezesa Urzędu Ochrony Danych Osobowych, administracyjna kara pieniężna spełni funkcję represyjną, jako że stanowić będzie odpowiedź na naruszenie przez Szkołę przepisów RODO, ale i prewencyjną, jako że sama Szkoła będzie skutecznie zniechęcona do naruszania w taki sposób przepisów ochrony danych osobowych w przyszłości.

Komentarz eksperta

Przemysław Zegarek, Prezes Lex Artist sp. z o.o., ekspert ds. ochrony danych osobowych

W decyzji PUODO widzę kontynuację linii decyzyjnej GIODO i sądów administracyjnych sprzed... 10 lat (!) (por. wyrok z 18 czerwca 2010 r., sygn. akt II SA/Wa 151/10). Jest jednak zasadnicza różnica. Dziesięć lat temu instalacja biometryki skończyła się nakazem usunięcia czytników przez Naczelnika Urzędu Skarbowego. Dzisiaj mamy dotkliwą finansowo karę. Nie oznacza to jednak zakazu stosowania biometryki w każdej sytuacji!

O nałożonej karze zaważyły następujące okoliczności:

1) doszło do dyskryminacji osób nie korzystających z biometryki,
2) cel, czyli dostęp do szkolnej stołówki wydaje się być zupełnie nieadekwatny do ingerencji w prywatność, jaką zawsze jest biometryka,
3) chodziło o dzieci.

Decyzja	Decyzja Prezesa UODO z dnia 9 marca 2020 r. ZSPR.421.19.2019
Ukarany podmiot	Vis Consulting Sp. z o.o. w likwidacji
Kwota kary pieniężnej	20 000,00 PLN
Naruszone przepisy RODO	• art. 31 RODO – obowiązek współpracy z organem nadzorczym w ramach wykonywania przez niego swoich zadań • art. 58 ust. 1 lit. e oraz f RODO – uprawnienia organu nadzorczego w zakresie uzyskiwania od administratora dostępu do wszelkich danych osobowych i informacji oraz wszystkich pomieszczeń w tym sprzętu i środków służących do przetwarzania danych osobowych
Kontekst	Prezes UODO nałożył karę za uniemożliwienie przeprowadzenia kontroli. Dodatkowo właścicielowi Spółki grozi za to odpowiedzialność karna. Prezes UODO podjął decyzję o przeprowadzeniu czynności kontrolnych w ukaranej Spółce, w związku z ustaleniami dokonanymi w toku innej przeprowadzonej kontroli. Kontrolerzy UODO, pod wskazanym w KRS adresem i po uprzednim zawiadomieniu o planowanej kontroli, nikogo nie zastali. Kontrolerom udało się jednak telefonicznie skontaktować z Vis Consulting, a jej pełnomocnik poinformował, że kontrola się nie odbędzie. Prezes UODO uznał więc, że Spółka ta w żaden sposób nie chce współpracować z organem. Przez dwa kolejne dni zaplanowanych czynności kontrolnych Spółka dwukrotnie uniemożliwiła jej przeprowadzenie. Ponadto, w dniu, w którym kontrolerzy próbowali ponownie skontrolować Vis Consulting Sp. z o.o., jej władze podjęły uchwałę o likwidacji tego podmiotu. W ocenie Prezesa Urzędu Spółka nie realizuje obowiązków związanych z przetwarzaniem danych osobowych oraz w co najmniej zamierzony sposób unika poddania się kontroli organu nadzorczego. Spółka naruszała tym samym przepisy RODO, mówiące o współpracy z organem nadzorczym i umożliwieniu temu organowi dostępu do wszystkich danych osobowych i wszelkich informacji. Prezes UODO uznał więc, że zostały spełnione przesłanki, by nałożyć na spółkę karę pieniężną. Ustalając jej wysokość organ nadzorczy nie dopatrzył się żadnych okoliczności łagodzących, mających wpływ na wysokość kary. W związku z podejrzeniem popełnienia przestępstwa z art. 108 ust. 1 ustawy o ochronie danych osobowych przez Prezesa Spółki, organ nadzorczy zawiadomił o tym Prokuraturę Rejonową w Katowicach. Zgodnie z tym przepisem za udaremnianie lub utrudnianie prowadzenie kontroli przestrzegania przepisów o

	ochronie danych osobowych, grozi grzywna, kara ograniczenia wolności albo pozbawienia wolności do lat dwóch. Prokuratura skierowała w tej sprawie akt oskarżenia przeciwko Prezesowi Spółki do sądu.

Komentarz eksperta

Małgorzata Zdunek, ekspert ds. ochrony danych osobowych

Patrząc na sam wymiar kary i porównując ją z poprzednimi karami finansowymi nałożonymi przez organ na podmioty prywatne, wydaje się ona być wręcz symboliczna. To co jednak najbardziej istotne w tej decyzji, to nie wysokość sankcji lecz to, za co ją nałożono. Prezes UODO dał jasny sygnał administratorom i innym podmiotom przetwarzającym dane osobowe – brak współpracy z organem nadzorczym nie popłaca. Wydaje się, że ukarana Spółka nie do końca przemyślała swoje działania. Z drugiej strony, jej postępowanie mogło być wynikiem przeprowadzonej kalkulacji, tj. bardziej opłaca się nam (oraz Prezesowi) ponieść karę za uniemożliwienie kontroli, niż w jej toku ujawnić, jakie dane osobowe i w jaki sposób przetwarzamy. Pojawia się zatem pytanie, co Vis Consulting Sp. z o.o. w likwidacji chciała ukryć i czy dane w jakich jest posiadaniu są bezpieczne?

Decyzja	Decyzja Prezesa UODO z dnia 10 lipca 2020 r. DKE.561.1.2020
Ukarany podmiot	East Power sp. z o.o.
Kwota kary pieniężnej	15 000,00 PLN
Naruszone przepisy RODO	• art. 58 ust. 1 lit. e RODO – uprawnienia organu nadzorczego w zakresie uzyskiwania od administratora dostępu do wszelkich danych osobowych i informacji
Kontekst	East Power sp. z o.o. zajmuje się na terenie Polski i Niemiec pośrednictwem pracy. Skargę na jej działania złożył obywatel Niemiec. Zdaniem skarżącego spółka przetwarzała jego dane osobowe w celach marketingowych bez podstawy prawnej. Skargę złożono w niemieckim organie nadzoru właściwym dla Nadrenii-Palatynatu. Skarga została następnie przejęta do rozpoznania przez Prezesa UODO, który był w tej sprawie tzw. organem wiodącym z uwagi na to, że spółka ma siedzibę w Polsce. Prezes UODO trzykrotnie skierował do spółki wezwania do złożenia wyjaśnień. Dwa z nich pozostały bez żadnej odpowiedzi. Na jedno z wezwań spółka udzieliła odpowiedzi, jednakże w ocenie organu były one niewystarczające do ustalenia stanu faktycznego sprawy. Prezes UODO uznał, że East Power sp. z o.o. celowo utrudnia bieg postępowania lub co najmniej lekceważy swoje obowiązki związane ze współpracą. Dopiero w reakcji na zawiadomienie o wszczęciu postępowania w sprawie nałożenia na nią administracyjnej kary pieniężnej spółka złożyła bardziej obszerne wyjaśnienia. Wyjaśnienia te również zdaniem UODO okazały się niepełne i wymagały prowadzenia dalszego postępowania wyjaśniającego. Ostatecznie Prezes UODO uznał, że spółka nie chce z nim współpracować i nie wywiązuje się z obowiązku zapewnienia mu dostępu do danych osobowych i innych informacji niezbędnych do realizacji jego zadań. Wydając decyzję o nałożeniu na East Power Sp. z o.o. administracyjnej kary pieniężnej oraz określając jej wysokość, Prezes UODO wziął pod uwagę jako okoliczności obciążające m.in. dużą wagę naruszenia, umyślny charakter naruszenia oraz niezadowalający stopień współpracy w celu usunięcia naruszenia oraz złagodzenia jego skutków.

Komentarz eksperta

Katarzyna Kmiecicka, ekspert ds. ochrony danych osobowych

Jest to pierwsza w Polsce kara nałożona w ramach postępowania transgranicznego. Skargę na działania firmy złożył obywatel Niemiec w niemieckim organie ochrony danych osobowych właściwym dla Nadrenii-Palatynatu, która z kolei została przejęta do rozpoznania przez polski organ z uwagi na siedzibę spółki znajdującą się na terenie Polski. Jest to także kolejna kara, nałożona za utrudnianie organowi przeprowadzenia czynności kontrolnych. W ramach postępowania Prezes UODO trzykrotnie skierował do spółki wezwania do złożenia wyjaśnień. Dwa z nich pozostały bez odpowiedzi, pomimo prawidłowego ich doręczenia, natomiast jedyne w sprawie złożone wyjaśnienie zostało uznane za niewystarczające. Pokazuje to po raz kolejny, że brak składanych wyjaśnień, granie na czas i unikanie kontroli nie jest odpowiednim wyjściem z sytuacji. Poprzez swoje działanie spółka uniemożliwiła organowi rozpatrzenie skargi złożonej przez obywatela Niemiec i wydanie odpowiedniej decyzji w tej sprawie.

Decyzja	Decyzja Prezesa UODO z dnia 16 lipca 2020 r. DKE.561.2.2020
Ukarany podmiot	Osoba fizyczna prowadząca działalność gospodarczą
Kwota kary pieniężnej	5 000,00 PLN
Naruszone przepisy RODO	• art. 58 ust. 1 lit. e RODO – uprawnienia organu nadzorczego w zakresie uzyskiwania od administratora dostępu do wszelkich danych osobowych i informacji
Kontekst	Przedsiębiorca prowadzący niepubliczny żłobek i przedszkole nie zapewnił Prezesowi UODO dostępu do danych osobowych i innych informacji niezbędnych do realizacji jego zadań – w tym przypadku do oceny czy administrator w sposób zgodny z przepisami RODO zawiadomił osoby, których dane dotyczą, o naruszeniu (czym naruszył art. 58 ust. 1 lit. e RODO). Przedsiębiorca zgłosił do Prezesa UODO naruszenia ochrony danych osobowych, polegające na utracie dostępu do danych osobowych przechowywanych w prowadzonym niepublicznym żłobku i przedszkolu. W związku z brakiem w ww. zgłoszeniu informacji niezbędnych do oceny tego naruszenia, organ nadzorczy trzykrotnie skierował do przedsiębiorcy wezwania do złożenia stosownych wyjaśnień – przedsiębiorca nie udzielił Prezesowi UODO żadnej odpowiedzi na wezwania. Wydając decyzję o nałożeniu administracyjnej kary pieniężnej oraz określając jej wysokość, Prezes UODO wziął pod uwagę jako okoliczności obciążające przedsiębiorcę, m.in. charakter, wagę i czas trwania naruszenia, umyślny charakter naruszenia oraz brak współpracy z organem nadzorczym. Nałożona kara jest w ocenie Prezesa UODO proporcjonalna do wagi stwierdzonego naruszenia oraz do możliwości jej poniesienia przez przedsiębiorcę bez dużego uszczerbku dla prowadzonej przez niego działalności.

Komentarz eksperta

Tomasz Wasilczyk, starszy specjalista ds. ochrony danych osobowych

Decyzja Prezesa UODO o nałożeniu kary na przedsiębiorcę prowadzącego niepubliczny żłobek oraz przedszkole nie budzi wątpliwości. Ukarany przedsiębiorca ewidentnie nie współpracował z organem nadzorczym w zakresie usunięcia naruszenia.

Analizując treść uzasadnienia do decyzji, przede wszystkim należy zauważyć, iż mniejsze podmioty również mogą zostać ukarane administracyjną karę pieniężną, szczególnie, że w niniejszym stanie

faktycznym działalność przedsiębiorcy obejmuje przetwarzanie danych osobowych dzieci, które wymagają szczególnej ochrony.

Po drugie, w ocenie organu obowiązkiem przedsiębiorcy, czyli podmiotu profesjonalnie działającego w obrocie prawno-gospodarczym, jest odbieranie korespondencji związanej z prowadzoną działalnością. Analizowane rozstrzygnięcie Prezesa UODO potwierdza zatem fakt, iż istotną okolicznością w danym postępowaniu jest dobra współpraca z organem, co zostało również podkreślone w poprzednich decyzjach Prezesa UODO, np. tej z dnia 10 lipca 2020 roku nakładającej karę na spółkę East Power z Jeleniej Góry.

Decyzja	Decyzja Prezesa UODO z dnia 2 lipca 2020 r. DKE.561.3.2020
Ukarany podmiot	Główny Geodeta Kraju
Kwota kary pieniężnej	100 000,00 PLN
Naruszone przepisy RODO	• art. 58 ust. 1 lit. e oraz f RODO – uprawnienia organu nadzorczego w zakresie uzyskiwania od administratora dostępu do wszelkich danych osobowych i informacji oraz wszystkich pomieszczeń w tym sprzętu i środków służących do przetwarzania danych osobowych
Kontekst	Kara pieniężna w kwocie 100 tys. zł. została nałożona przez Prezesa UODO po przeprowadzeniu wszczętego z urzędu postępowania administracyjnego. Organ nadzoru stwierdził naruszenie przez Głównego Geodetę Kraju przepisów RODO, polegające na niezapewnieniu organowi nadzorczemu w trakcie kontroli dostępu do pomieszczeń, sprzętu i środków służących do przetwarzania danych osobowych oraz dostępu do danych osobowych i informacji niezbędnych Prezesowi UODO do realizacji jego zadań. Ponadto GGK nie współpracował z Prezesem UODO w trakcie tej kontroli. Na początku marca 2020 r. Prezes UODO zdecydował o konieczności przeprowadzenia kontroli przetwarzania przez Głównego Geodetę Kraju na portalu GEOPORTAL2 danych osobowych pochodzących z powiatowych ewidencji gruntów i budynków, o czym poinformował go pismem, w którym wskazał zakres kontroli oraz termin jej przeprowadzenia. W celu przeprowadzenia czynności kontrolnych, kontrolujący upoważnieni przez Prezesa UODO, okazali Głównemu Geodecie Kraju swoje legitymacje służbowe oraz przedłożyli upoważnienia imienne zawierające informację o zakresie kontroli. GGK nie dopuścił do przeprowadzenia czynności kontrolnych w pełnym zakresie wynikającym z przedłożonych upoważnień, gdyż według jego oceny z zakresu wskazanego w upoważnieniach wynika, że kontrola ma dotyczyć numerów ksiąg wieczystych, które według niego nie stanowią danych osobowych w rozumieniu przepisów Prawa geodezyjnego i kartograficznego. Ostatecznie GGK podpisał upoważnienia, na których zamieścił pisemną adnotację, z której wynika, że odmawia przeprowadzenia kontroli w zakresie ustalenia m.in.: podstawy przetwarzania (także udostępniania w GEOPRTALU2) danych osobowych, źródeł pozyskiwania tych danych, zakresu i rodzaju udostępnianych danych osobowych oraz sposobu i celu tego udostępniania. Z uwagi na powyższe, w toku kontroli ustalono jedynie, jakie środki organizacyjne zastosował GGK dla bezpieczeństwa danych oraz czy powołany został inspektor ochrony danych.

	Przed Prezesem UODO toczy się osobne postępowanie w przedmiocie naruszenia polegającego na przetwarzaniu danych osobowych w postaci numerów ksiąg wieczystych na portalu internetowym GEOPORTAL2 bez podstawy prawnej.

Komentarz eksperta

Małgorzata Zdunek, ekspert ds. ochrony danych osobowych

To już czwarta kara pieniężna nałożona przez Prezesa UODO w związku z brakiem współpracy ze strony administratora. 100 tys. zł. to maksymalny wymiar sankcji finansowej, jaką organ nadzoru może nałożyć na podmiot publiczny. Warto jednak w tym kontekście zwrócić uwagę nie na postępowanie, które zostało zakończone wskazaną decyzją, ale na to, które się jeszcze toczy. Dotyczy ono kwestii udostępniania numerów ksiąg wieczystych na GEOPORTAL2 bez podstawy prawnej. UODO nie ma wątpliwości, że numery te pozostają danymi osobowymi. Główny Geodeta Kraju twardo stoi jednak na stanowisku, że nie mają one takiego charakteru. Stąd właśnie niedopuszczenie przez niego pracowników UODO do kontroli, która w ocenie GGK była bezprzedmiotowa.

Warto zauważyć, że pomimo tego, że numer księgi wieczystej sam w sobie odnosi się do nieruchomości, to pozwala on zgromadzić wiedzę już o konkretnych osobach. Za dane osobowe uznaje natomiast informacje, które pozwalają nam zidentyfikować osobę fizyczną nie tylko w sposób bezpośredni, ale również pośrednio. Trudno się zatem nie zgodzić ze stanowiskiem Prezesa UODO. Biorąc jednak pod uwagę działania GGK, sprawa zapewne ostatecznie zakończy się w sądzie. Pozostaje nam zatem czekać na rozstrzygnięcie tego zagadnienia przez WSA.

Decyzja	Decyzja Prezesa UODO z dnia 24 sierpnia 2020 r. DKN.5112.13.2020
Ukarany podmiot	Główny Geodeta Kraju
Kwota kary pieniężnej	100 000,00 PLN
Naruszone przepisy RODO	• art. 5 ust. 1 lit. a RODO – zasady zgodności z prawem przetwarzania danych osobowych • art. 6 ust. 1 RODO – podstawy prawne przetwarzania danych osobowych
Kontekst	Powodem nałożenia administracyjnej kary pieniężnej na Głównego Geodetę Kraju w wysokości 100 tys. złotych jest naruszenie zasady zgodności z prawem przetwarzania danych osobowych oraz udostępnianie w sposób umyślny bez podstawy prawnej na portalu GEOPORTAL2 danych osobowych w postaci numerów ksiąg wieczystych pozyskanych z ewidencji gruntów i budynków. Prezes UODO wskazał ponadto, że GGK musi dostosować operacje przetwarzania danych osobowych do przepisów RODO poprzez zaprzestanie udostępniania na portalu GEOPORTAL2 (www.geoportal.gov.pl) danych osobowych w zakresie numerów ksiąg wieczystych pozyskanych z ewidencji gruntów i budynków (prowadzonej przez starostów). O przeprowadzeniu czynności kontrolnych u Głównego Geodety Kraju, Prezes UODO zadecydował na początku marca 2020 r. Poprzez brak współpracy z organem, GGK udaremnił możliwość zbadania legalności publikowania na GEOPORTAL2 informacji o numerach ksiąg wieczystych. Mimo odmowy przeprowadzenia kontroli, GGK złożył jednak zeznania, które posłużyły za materiał dowodowy w prowadzonym przez organ nadzorczy postępowaniu. GGK w trakcie przeprowadzonego postępowania nie wskazał przepisu prawa, który stanowiłby podstawę prawną jego działania. Prezes UODO stwierdził również, że żaden z przepisów regulujących kwestie związane z działalnością Głównego Geodety Kraju nie pozwala na udostępnianie przez niego w ramach GEOPORTAL2 danych pozyskanych ze starostw. W ocenie Prezesa UODO, Główny Geodeta Kraju, zdając sobie sprawę z braku wyraźnej podstawy prawnej do przetwarzania numerów ksiąg wieczystych, zawarł porozumienia ze starostami, na postawie których pozyskał informacje z ewidencji gruntów i budynków (w tym numerów ksiąg wieczystych) prowadzonych przez starostów celem ich publikacji na GEOPORTAL2. Organ nadzorczy uznał, że porozumienia te nie stanowiły podstawy prawnej do udostępniania danych, w tym numerów ksiąg wieczystych. Tym samym Prezes UODO uznał, że doszło do udostępniania danych osobowych w postaci numerów ksiąg wieczystych na GEOPORTAL2 bez podstawy prawnej.

	Nakładając karę pieniężną, organ nadzorczy wziął pod uwagę nie tylko wagę naruszenia, jego charakter oraz czas trwania, ale także umyślny charakter działania.

Komentarz eksperta

Małgorzata Zdunek, ekspert ds. ochrony danych osobowych

Główny Geodeta Kraju rozbija bank. To już druga kara nałożona na ten podmiot w przeciągu dwóch miesięcy. Tak jak poprzednio mamy do czynienia z maksymalnym wymiarem sankcji finansowej, jaką organ nadzorczy może nałożyć na podmiot publiczny. Tym razem decyzja dotyczy meritum przeprowadzonej kontroli, a więc udostępniania numerów ksiąg wieczystych bez podstawy prawnej. Prezes UODO twardo stoi na stanowisku, że są to dane osobowe i ich udostępnienie na GEOPORTAL2 było bezprawne. Biorąc pod uwagę, że z dostępnych w Internecie ksiąg wieczystych każdy ostatecznie może poznać nawet numer PESEL i imiona rodziców właściciela oraz osób mających prawa czy roszczenia do nieruchomości, trudno się z organem w tym zakresie spierać.

Co ciekawe, w Internecie udostępniono petycję do Prezesa UODO o wycofanie kar UODO dla GGK. Jej autorem jest geodeta z Polic Paweł Myłka, a podpisało się pod nią już ponad sto osób. Myłka podkreśla, że nie chce rozstrzygać meritum samego sporu, ale w jego ocenie jego strony powinny ze sobą współpracować i rozwiązać go w oparciu o merytoryczną i jednocześnie na uwadze dobro społeczne i interes obywateli. Trudno się w tym zakresie z autorem petycji nie zgodzić. Niewątpliwie w tej sprawie woli współpracy zabrakło u każdej ze stron.

Nam pozostaje czekać na orzeczenie WSA, które, mamy nadzieję, ostatecznie zakończy trwający spór.

Decyzja	Decyzja Prezesa UODO z dnia 21 sierpnia 2020 r. ZSOŚS.421.25.2019
Ukarany podmiot	Szkoła Główna Gospodarstwa Wiejskiego w Warszawie
Kwota kary pieniężnej	50 000,00 PLN
Naruszone przepisy RODO	• art. 5 ust. 1 lit. e RODO – zasada ograniczenia przechowywania • art. 5 ust. 1 lit. f RODO – zasada integralności i poufności • art. 5 ust. 2 RODO – zasada rozliczalności • art. 25 ust. 1 RODO – zasada *privacy by design* • art. 32 ust. 1 lit. b RODO – zapewnienie zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania • art. 32 ust. 1 lit. d RODO – regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania • art. 32 ust. 2 RODO – ocena stopnia bezpieczeństwa przy uwzględnieniu ryzyka wiążącego się z przetwarzaniem • art. 38 ust. 1 RODO – zapewnienie, że inspektor ochrony danych jest właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych • art. 39 ust. 1 lit. b RODO – zadania inspektora ochrony danych – monitorowanie przestrzegania przepisów o ochronie danych oraz polityk administratora, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty • art. 39 ust. 2 RODO – wypełnianie przez inspektora ochrony danych swoich zadań z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania
Kontekst	W listopadzie 2019 r. Prezes UODO otrzymał zgłoszenie naruszenia ochrony danych osobowych kandydatów na studia w Szkole Główną Gospodarstwa Wiejskiego w Warszawie. Zgłoszenie było związane z kradzieżą przenośnego prywatnego komputera pracownika uczelni, który używał tego urządzenia także do celów służbowych, w tym do przetwarzania danych osobowych kandydatów na studia w SGGW. Po kontroli przeprowadzonej na uczelni w związku z naruszeniem ochrony danych, organ wszczął z urzędu postępowanie administracyjne. Na podstawie zebranego materiału dowodowego Prezes UODO nałożył na uczelnię administracyjną karę pieniężną w wysokości 50 tys. zł.

	Decydując o wysokości kary, organ nadzorczy wziął pod uwagę, że naruszenie ochrony danych osobowych dotyczyło kandydatów na studia za okres ostatnich pięciu lat, obejmowało szeroki zakres danych, a liczba osób dotkniętych naruszeniem może wynosić do 100 tys. Ponadto, administrator nie miał wiedzy o przetwarzaniu danych osobowych na prywatnym komputerze pracownika, a także nie kontrolował procesu przetwarzania danych poprzez brak weryfikacji na jakich nośnikach są przetwarzane dane osobowe. W wyniku przeprowadzonego postępowania ustalono, że uczelnia nie wdrożyła odpowiednich środków organizacyjnych i technicznych, które pozwalają na zapewnienie bezpieczeństwa przetwarzania danych osobowych kandydatów na studia. Jednocześnie Prezes UODO stwierdził, że w przedmiotowej sprawie inspektor ochrony danych wypełniał swoje zadania bez należytego uwzględnienia ryzyka związanego z operacjami przetwarzania. Powołany IOD nie był angażowany przez uczelnię w proces rekrutacji na studia obejmujący funkcjonowanie systemu informatycznego przeznaczonego do tego działania. Wymierzając karę pieniężną, Prezes UODO wziął pod uwagę okoliczności łagodzące, takie jak: dobrą współpracę z organem nadzorczym, podjęcie działań mających na celu usunięcie naruszenia oraz zapewnienie bezpieczeństwa w procesie przetwarzania danych w przyszłości.

Komentarz eksperta

Przemysław Zegarek, Prezes Lex Artist sp. z o.o., ekspert ds. ochrony danych osobowych

Moją uwagę zwróciła łączna kwota kary. Z jednej strony, 50 tys. zł to niedużo w porównaniu do słynnej, prawie 3 mln kary dla Morele.net. Z drugiej strony, 50 tys. zł to aż 50% górnego pułapu kary, która może zostać nałożona na państwową instytucję!

UODO wskazuje, że naruszono, aż 10 różnych artykułów RODO. Jeśli każde z naruszeń potraktujemy jako równorzędne, to taryfikator będzie przedstawiał się następująco: 5 tys. zł za każde naruszenie (takie ujęcie sprawi już mniej szokujące wrażenie).

Pamiętajmy też o tym, że naruszenie dotyczyło około 100 tys. rekordów. Skala naruszenia również odegrała dużą rolę przy ostatecznej decyzji UODO.

Uzasadnienie decyzji to prawdziwa kopalnia wiedzy dla każdego Inspektora Ochrony Danych. Lektura uzasadnienia obrazuje, jak zdaniem UODO powinna wyglądać współpraca na linii IOD – Administrator Danych Osobowych. Jak więc powinna wyglądać ta relacja?

Przede wszystkim, IOD powinien być włączany we wszelkie nowe i bieżące operacje na danych osobowych. To cenna lekcja dla każdego Administratora Danych. Niewłączanie IOD w procesy związane z ochroną danych osobowych, może skutkować nałożeniem kary. Dla Inspektorów Ochrony Danych może być to ważny argument za angażowaniem ich w bieżące procesy biznesowe.

Z własnego doświadczenia wiem, że zdarzają się sytuacje, kiedy IOD np. o uruchomieniu sklepu internetowego, dowiaduje się ostatni. I to w momencie, kiedy sklep, przetwarzający duże ilości danych osobowych, już funkcjonuje.

Ponadto, UODO daje również wskazówki, jak sam IOD powinien organizować swoją pracę. Organ podkreśla konieczność ustalania priorytetów, które wiążą się z indywidualnym i samodzielnym określaniem środków oraz metod działania. Zarówno środki, jak i metody powinny zostać dostosowane do specyfiki konkretnego Administratora Danych.

Decyzja pokazuje również wagę szacowania ryzyka dla UODO. Pokazuje też, jak dużą, zdaniem organu, rolę w jej przeprowadzeniu odgrywa IOD. Z niektórych fragmentów uzasadnienia można wręcz odczytać, że to IOD powinien zająć się szacowaniem ryzyka. Z tym w mojej opinii trudno się zgodzić. Oczywiście IOD może pomagać czy nadzorować szacowanie ryzyka, jak i wskazywać obszary, które takiej oceny wymagają. Realizacja oceny, to już jednak co najmniej wspólne zadanie IOD oraz Administratora Danych (a właściwie jego pracowników).

UODO położył mocny nacisk na konieczność wykonywania przez IOD audytów i monitorowania aktualnej sytuacji. To właśnie brak bieżącej kontroli nad procesami ochrony danych osobowych, był jedną z głównych przyczyn naruszenia do którego doszło w SGGW.

Decyzja	Decyzja Prezesa UODO z dnia 3 grudnia 2020 r. DKN.5112.1.2020
Ukarany podmiot	Virgin Mobile Polska sp. z o.o.
Kwota kary pieniężnej	1 968 524,00 PLN
Naruszone przepisy RODO	• art. 5 ust. 1 lit. f RODO – zasada integralności i poufności • art. 5 ust. 2 RODO – zasada rozliczalności • art. 25 ust. 1 RODO – zasada *privacy by design* • art. 32 ust. 1 lit. b RODO – zapewnienie zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania • art. 32 ust. 1 lit. d RODO – regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania • art. 32 ust. 2 RODO – ocena stopnia bezpieczeństwa przy uwzględnieniu ryzyka wiążącego się z przetwarzaniem
Kontekst	UODO stwierdził, że Virgin Mobile Polska sp. z o.o. naruszyła określone w RODO zasady poufności danych i rozliczalności. Spółka nie przeprowadzała regularnych i kompleksowych testów, pomiarów i oceny skuteczności zastosowanych środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych. Działania w tym zakresie były podejmowane jedynie przy okazji pojawiających się podejrzeń zaistnienia podatności, czy w związku ze zmianami organizacyjnymi. Ponadto, nie były przeprowadzone testy weryfikujące zabezpieczenia związane z przekazywaniem danych między aplikacjami, które związane były z obsługą osób kupujących usługi przedpłacone. Oprócz tego, podatność związaną z wymianą danych w tych systemach, wykorzystała osoba nieuprawniona do pozyskania danych niektórych klientów spółki. W efekcie naruszenia ochrony danych, w wyniku którego nieuprawniona osoba uzyskała dane klientów z jednej z baz, Prezes UODO przeprowadził kontrolę. W wyniku stwierdzonych nieprawidłowości wszczął następnie postępowania administracyjne zakończone nałożeniem kary. Organ nadzoru uznał m.in., że wdrożenie systemu służącego do przetwarzania danych do użytku bez poprawnie działającej walidacji zakładanych parametrów jest rażącym naruszeniem administratora.

	UODO nakładając karę wziął pod uwagę, że naruszenie do którego doszło u operatora ma poważny charakter, gdyż stwarza wysokie ryzyko negatywnych skutków ochrony prawnej dla dużej liczby osób (np. ryzyko kradzieży tożsamości). Urząd wziął pod uwagę również okoliczności łagodzące, jak np. dobrą współpracę administratora, szybkie usunięcie naruszenia po jego wykryciu, ale i wdrożenie dodatkowych rozwiązań, które mają dodatkowo podnieść bezpieczeństwo przetwarzanych danych. Biorąc jednak pod uwagę skalę naruszeń i ich wagę UODO uznał, że zastosowanie innych środków naprawczych niż administracyjnej kary pieniężnej byłoby nieproporcjonalne. Kara pieniężna w wysokości 1,9 mln zł ma zaś sprawić, że spółka w przyszłości nie dopuści już do podobnych zaniedbań.

Komentarz eksperta

Przemysław Zegarek, Prezes Lex Artist sp. z o.o., ekspert ds. ochrony danych osobowych

Widzę duże podobieństwo w przyczynach nałożenia kar przez UODO na Virgin Mobile oraz Morele.net.

W obu przypadkach, główną przyczyną nałożenia kary był brak odpowiednich środków zabezpieczeń IT. To dopiero druga kara UODO, w której obszar Cybersecurity odgrywa kluczową rolę. Jednak kwoty kar dla Virgin Mobile i Morele net. robią duże wrażenie. To odpowiednio 1,9 mln zł dla Virgin Mobile i 2,8 mln zł dla Morele.net.

W obu przypadkach kara była konsekwencją postępowania wyjaśniającego, związanego z zaistnieniem RODO incydentu.

Są i różnice. W przypadku Virgin Mobile, szczególną uwagę zwrócono na brak bieżącego monitorowania zabezpieczeń IT. Pewne zabezpieczenia funkcjonowały w spółce, jednak nikt ich regularnie nie kontrolował. Brak kontroli nad zabezpieczeniami, doprowadził do dopuszczenia do działania nienależycie zabezpieczonej aplikacji.

Kara może pomóc podjąć dobre, długofalowe decyzje administratorom danych osobowych. Chodzi o poważniejsze traktowanie obszaru Cybersecurity. Wielu administratorów danych, do dzisiaj nie wyznaczyło konkretnych osób odpowiadających za obszar Cybersecuiry. W mojej opinii, w każdej organizacji, korzystającej z infrastruktury informatycznej, powinien działać ktoś odpowiedzialny za ten obszar.

Decyzja	Decyzja Prezesa UODO z dnia 9 grudnia 2020 r. DKN.5131.5.2020
Ukarany podmiot	Towarzystwo Ubezpieczeń i Reasekuracji WARTA S.A.
Kwota kary pieniężnej	85 588,00 PLN
Naruszone przepisy RODO	• art. 33 ust. 1 RODO – zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu • art. 34 ust. 1 RODO – zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych
Kontekst	W maju 2020 r. do Urzędu Ochrony Danych Osobowych wpłynęła informacja od osoby postronnej o naruszeniu ochrony danych osobowych, które polegało na wysłaniu pocztą elektroniczną przez agenta ubezpieczeniowego, będącego podmiotem przetwarzającym dla Towarzystwa Ubezpieczeń i Reasekuracji WARTA S.A., polisy ubezpieczeniowej do nieuprawnionego adresata. Załączony dokument zawierał dane osobowe w zakresie m.in. imion, nazwisk, adresów zamieszkania, numerów PESEL oraz informacji dotyczących przedmiotu ubezpieczenia (samochód osobowy). Organ nadzorczy został poinformowany o naruszeniu ochrony danych osobowych przez nieuprawnionego adresata, który wszedł w posiadanie nieprzeznaczonych dla niego dokumentów. Prezes UODO zwrócił się do Spółki o wyjaśnienie, czy w związku z wysyłką korespondencji elektronicznej do nieuprawnionego odbiorcy została dokonana analiza pod kątem ryzyka naruszenia praw i wolności osób fizycznych niezbędna do oceny, czy doszło do naruszenia ochrony danych skutkującego koniecznością zawiadomienia UODO oraz osób, których dotyczy naruszenie. Spółka potwierdziła, że doszło do incydentu oraz, że została dokonana ocena pod kątem ryzyka naruszenia praw i wolności osób fizycznych. Na jej podstawie ukarana Spółka uznała, iż zaistniałe naruszenie nie wymaga zawiadomienia UODO. Spółka uznała, że naruszenie powstało na skutek wysłania dokumentu polisy ubezpieczeniowej na błędny adres poczty elektronicznej, który wskazał sam klient. Ponadto nieuprawniony odbiorca zwrócił się do Spółki, a ta poprosiła o trwałe usunięcie wiadomości wraz z prośbą o informację zwrotną potwierdzającą jej usunięcie. Pomimo pisma UODO z prośbą o wyjaśnienia, Spółka nadal nie zgłosiła naruszenia ochrony danych osobowych oraz nie powiadomiła o incydencie osób, których dotyczyło naruszenie. Organ nadzoru wszczął więc postępowanie administracyjne. Dopiero w wyniku wszczęcia postępowania Spółka zgłosiła naruszenie ochrony danych osobowych oraz zawiadomiła dwie osoby, których dotyczy naruszenie.

	Takie działanie Spółki spowodowało, że czas trwania naruszenia był długi, co uznano za okoliczność obciążającą. Tym bardziej, że od powzięcia informacji o naruszeniu ochrony danych osobowych do powiadomienia o nim organ nadzorczy upłynęło pięć miesięcy. W toku postępowania UODO uznał, że fakt, iż do naruszenia doszło w wyniku błędu klienta, który przekazał nieprawidłowy adres mailowy, nie może mieć wpływu na niezakwalifikowanie zdarzenia jako naruszenia ochrony danych osobowych. Również fakt zwrócenia się z prośbą do niewłaściwego odbiorcy o trwałe usunięcie otrzymanej korespondencji nie może stanowić o tym, że ryzyko dla praw i wolności osób, których dane dotyczą nie jest wysokie. Administrator nie ma pewności, że nieuprawniony adresat nie wykonał np. kserokopii dokumentów lub też ich nie utrwalił. Prezes UODO nakładając administracyjną karę pieniężną wziął pod uwagę również okoliczności łagodzące jak fakt, że naruszenie dotyczyło danych osobowych dwóch osób oraz, że Spółka zwróciła się do niewłaściwego odbiorcy z prośbą o trwałe usunięcie otrzymanej korespondencji.

Komentarz eksperta

Małgorzata Zdunek, ekspert ds. ochrony danych osobowych

To, na co należy zwrócić uwagę w pierwszej kolejności, to fakt, że naruszenie ochrony danych osobowych, którego dotyczy nałożona na kara, miało miejsce u podmiotu przetwarzającego. To agent, działając jako procesor Towarzystwa Ubezpieczeń i Reasekuracji WARTA S.A. nieumyślnie ujawnił dane osobowe osobom nieuprawnionym. Za jego działanie, przed organem nadzoru oraz przed osobami, których dane dotyczą, odpowiada jednak Spółka, która jest administratorem tych danych. To pokazuje, jak ważna jest relacja podmiot przetwarzający – administrator. Wybór procesora nigdy nie może być przypadkowy, a zawarta umowa powierzenia przetwarzania danych osobowych powinna zawierać odpowiednie zapisy o informowaniu administratora o ewentualnych naruszeniach.

Dokonanie analizy i oceny stwierdzonego naruszenia ochrony danych osobowych (lub jego podejrzenia) jest obowiązkiem administratora. Analiza ta powinna być szczegółowa i uwzględniać wszystkie okoliczności zdarzenia. Ciężko nie zgodzić się ze stwierdzeniem organu, że w przypadku tego incydentu, Spółka dokonała błędnej oceny naruszenia. Biorąc pod uwagę sam zakres danych, ich ujawnienie osobie nieuprawnionej może powodować wiele negatywnych konsekwencji dla podmiotu danych. Kradzież tożsamości, nadużycia finansowe, utrata kontroli nad własnymi danymi osobowymi, ograniczenie możliwości realizacji praw, to tylko niektóre z nich. Dziwi zatem początkowe stanowisko Spółki, że naruszenie nie powoduje ryzyka naruszenia praw lub wolności osoby fizycznej.

Decyzje Prezesa UODO (nie tylko ta komentowana, nakładająca karę finansową) pokazują, że w przypadku naruszenia, zawsze lepiej jest zawiadomić o nim organ i osoby, których dane dotyczą, niż z tego zrezygnować. Odkładając obowiązki wynikające z RODO na bok, zwyczajnie, po ludzku,

podmiotowi danych należą się informacje, że jego dane osobowe w tak szerokim zakresie zostały przekazane osobom nieuprawnionym. Bez tych informacji nie może on bowiem podjąć żadnych działań zabezpieczających swoje interesy, jak np. monitorowanie aktywności kredytowej, zastrzeżenie dowodu osobistego, etc.

Decyzja	Decyzja Prezesa UODO z dnia 17 grudnia 2020 r. DKN.5130.1354.2020
Ukarany podmiot	ID Finance Poland Sp. z o.o.
Kwota kary pieniężnej	1 069 850,00 PLN
Naruszone przepisy RODO	• art. 5 ust. 1 lit. f RODO – zasada integralności i poufności • art. 25 ust. 1 RODO – zasada *privacy by design* • art. 32 ust. 1 lit. b RODO – zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania • art. 32 ust. 1 lit. d RODO – regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania • 32 ust. 2 RODO – obowiązek oceny stopnia bezpieczeństwa przetwarzania przy uwzględnieniu, w szczególności ryzyka wiążącego się z przetwarzaniem, w szczególności wynikającego z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych
Kontekst	Spółka ID Finance Poland sp. z o.o. (właściciel portalu pożyczkowego MoneyMan.pl) nie zareagowała odpowiednio na sygnał o lukach w jej zabezpieczeniach. Nie sprawdziła odpowiednio szybko informacji o tym, że na jednym z jej serwerów dostępne są dane jej klientów. Zawiadomienia nie potraktowała z odpowiednią powagą, przez co kilka dni po otrzymanym sygnale, osoba nieuprawniona skopiowała te dane, a następnie usunęła je z serwera. Za zwrot wykradzionych informacji zażądała okupu. Dopiero wtedy spółka rozpoczęła analizowanie zabezpieczeń i jednocześnie zgłosiła naruszenie ochrony danych organowi nadzoru. W toku postępowania UODO ustalił, że do naruszenia doszło po tym, jak po restarcie jednego z serwerów obsługiwanego przez podmiot przetwarzający (firmę hostingową) nie przywrócono odpowiedniej konfiguracji zabezpieczeń. Administrator został powiadomiony o tym przez jednego ze specjalistów zajmujących się cyberbezpieczeństwem. Administrator zamiast rzetelnie sprawdzić jego doniesienia i monitorować podmiot przetwarzający, miał wątpliwości, czy nie jest to próba wyłudzenia od niego innych danych. Przez to nie zajęto się od razu sprawdzeniem wskazanych luk w systemie i kilka dni później doszło do wykradzenia danych z tego serwera. Do tego naruszenia nie doszłoby, gdyby administrator od razu odpowiednio zareagował na informację o tym, iż dane na jego serwerze są niezabezpieczone. Zdaniem UODO administrator powinien utrzymywać zdolność do szybkiego i skutecznego stwierdzenia wystąpienia wszelkich naruszeń, aby mieć możliwość

	podjęcia odpowiednich działań. Ponadto administrator powinien być w stanie szybko zbadać dany incydent pod kątem tego, czy doszło do naruszenia ochrony danych oraz podjąć odpowiednie działania zaradcze. UODO, nakładając karę w wysokości ponad 1 mln zł za to, że w wyniku szeregu zaniedbań administratora doszło do naruszenia poufności danych osobowych, wziął pod uwagę skalę naruszenia, jak i zakres wykradzionych danych. Ponadto z uwagi na fakt, że wyciekły też niezaszyfrowane hasła, istnieje możliwość posłużenia się tymi danymi do zalogowania się na różnych kontach klientów, jeżeli w innych serwisach posługiwali się tym samym loginem (np. e-mail) i hasłem. Przy wymierzaniu wysokości kary organ wziął też pod uwagę zwłokę administratora w podjęciu działań zapobiegawczych.

Komentarz eksperta

Przemysław Zegarek, Prezes Lex Artist sp. z o.o., ekspert ds. ochrony danych osobowych

Kara nałożona na administratora danych jest bardzo wysoka. To jedna z trzech najwyższych kar nałożonych do tej pory przez UODO. Nastąpiła kumulacja trzech ważnych czynników, które zadecydowały o wysokiej karze:

1) Brak natychmiastowej reakcji na naruszenie. Ukarana spółka miała czas i możliwości zareagować szybciej. Gdyby nastąpiła szybka reakcja, to nie doszłoby do eskalacji naruszenia.

2) Duża ilość danych osobowych. Z treści decyzji Prezesa UODO wynika, że naruszenie dotyczyło ponad 100 tys. osób.

3) Dane które wyciekły są bardzo szerokie, dotyczą między innymi numerów pesel i treści haseł. Taki zestaw informacji jest wyjątkowo niebezpieczny w kontekście skutków, które może wywołać.

W mojej opinii, pierwotną przyczyną naruszenia były nieprawidłowości w funkcjonowaniu struktury organizacyjnej ochrony danych osobowych – brak odpowiedniej reakcji i przerzucanie się odpowiedzialnością.

Na naszym blogu pisaliśmy już o tym, jak wdrożyć strukturę, która zapewni rozliczalność RODO w organizacji i pozwoli zapobiec sytuacjom, które mogą doprowadzić do nałożenia kary przez organ nadzorczy.

Decyzja	Decyzja Prezesa UODO z dnia 5 stycznia 2021 r. DKN.5131.6.2020
Ukarany podmiot	Śląski Uniwersytet Medyczny
Kwota kary pieniężnej	25 000,00 PLN
Naruszone przepisy RODO	• art. 33 ust. 1 RODO – zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu • art. 34 ust. 1 RODO – zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych
Kontekst	Na początku czerwca 2020 roku Prezes UODO otrzymał sygnały o tym, że na Śląskim Uniwersytecie Medycznym doszło do naruszenia ochrony danych. Z informacji tych, jak i opisu skargi wynikało, że podczas egzaminów odbywających się pod koniec maja 2020 r. w formie wideokonferencji, miała miejsce identyfikacja studentów. Po zakończonym egzaminie nagrania z nich były dostępne nie tylko dla osób egzaminowanych, ale i innych osób mających dostęp do systemu. Ponadto wykorzystując bezpośredni link każda osoba postronna mogła mieć dostęp do nagrań z egzaminów i przedstawionych podczas identyfikacji danych egzaminowanych studentów. Ponieważ informacje wskazywały na to, że mogło dojść do wysokiego ryzyka dla praw i wolności osób, które przystąpiły do egzaminu, UODO zwrócił się do administratora danych o wyjaśnienie sytuacji. Ten w odpowiedzi na pismo utrzymywał, że w związku z naruszeniem nie było konieczności zawiadamiania organu, gdyż w jego ocenie ryzyko dla praw lub wolności osób, których dotyczył incydent było niskie. Ponadto po tym zdarzeniu system został zmodyfikowany, by nie dochodziło do omyłkowego udostępniania plików z zarejestrowanym przebiegiem egzaminów. Administrator wskazał też, że zidentyfikował osoby, które pobrały plik z egzaminem i powiadomił je o odpowiedzialności za posługiwanie się tymi danymi. Uczelnia w dalszym ciągu jednak nie zgłosiła naruszenia ochrony danych i nie powiadomiła osób dotkniętych tym zdarzeniem. Nie uczyniła tego, pomimo kolejnego pisma z UODO, w którym wskazano sytuacje, w jakich należy naruszenie ochrony danych zgłosić organowi nadzoru i w jakich trzeba też powiadomić o tym zdarzeniu osoby, których ono dotyczyło. W związku z tym wszczęto postępowanie administracyjne. Urząd uznał, że doszło do naruszenia ochrony danych, a administrator nie dopełnił obowiązków związanych z powiadomieniem o tym fakcie zarówno organu nadzoru i osób, których dotyczyło naruszenie. Administrator niewłaściwie ocenił bowiem zaistniałe ryzyko.

	Prezes Urzędu wymierzając karę 25 tys. zł za niezgłoszenie naruszenia organowi nadzoru i niepowiadomienie o nim osób, których dotyczył ten incydent, wziął pod uwagę m.in. czas trwania naruszenia (od naruszenia do wydania decyzji minęło kilka miesięcy), umyślne działanie administratora, który podjął decyzję, by nie zawiadamiać o naruszeniu i nie informować o nim studentów, niezadowalającą współpracę administratora z organem (nie zgłosił naruszenia pomimo wysyłanych pism i wszczętego postępowania). Organ nadzoru oprócz nałożonej kary, nakazał również uczelni powiadomienie osób, których dotyczyło naruszenie, do jakiego doszło w związku z egzaminami przeprowadzanymi w formie wideokonferencji na specjalnej do tego platformie e-learningowej.

Komentarz eksperta

Małgorzata Zdunek, ekspert ds. ochrony danych osobowych

To już druga kara Prezesa UODO nałożona w związku z niedopełnieniem przez administratora obowiązków związanych z powiadomieniem o naruszeniu ochrony danych osobowych.

Podobnie jak w przypadku TUiR WARTA S.A. tak i tutaj zabrakło rzetelnej analizy zdarzenia pod kątem jego wpływu na prawa i wolności osób, których dane dotyczą. To co rzuca się w oczy w przedmiotowej decyzji, to brak reakcji administratora na wskazówki, jakich organ udzielił mu w jednym z pierwszych pism w sprawie. Jeszcze przed wszczęciem postępowania administracyjnego Prezes UODO wprost wskazał uczelni, jak powinna wyglądać analiza incydentu pod kątem ryzyka naruszenia praw i wolności osób fizycznych, tj. przede wszystkim jakimi kryteriami należy się kierować podczas jej przeprowadzania. Pytanie, czy administrator dokonał ponownej kalkulacji ryzyka i jaki wynik uzyskał, od razu powinno zasugerować administratorowi, że organ z wcześniejszą oceną administratora się nie zgadza.

Jak zatem można było uniknąć kary? Należałoby zacząć od prawidłowej analizy zdarzenia, ze szczególnym uwzględnieniem zakresu danych, których ono dotyczy. Biorąc pod uwagę stosunek Prezesa UODO do naruszeń obejmujących numer PESEL, w każdym przypadku, kiedy incydent dotyczy tego typu informacji, administratorowi powinna zapalić się czerwona lampka.

Dodatkowo, kiedy już dochodzi do wymiany korespondencji z organem nadzoru, warto uważnie analizować kierowane do nas informacje. Mogą się tam znaleźć cenne wskazówki dotyczące naszej sytuacji oraz oczekiwań urzędu.

O tym, jak radzić sobie z naruszeniami, w tym m.in. jak prawidłowo dokonywać ich analizy, kiedy i jak zgłaszać je organowi lub osobom fizycznym, pisaliśmy na naszym blogu w cyklu poświęconym incydentom ochrony danych osobowych.

Decyzja	Decyzja Prezesa UODO z dnia 9 grudnia 2020 r. DKE.561.13.2020
Ukarany podmiot	Smart Cities Sp. z o.o.
Kwota kary pieniężnej	12 838,20 PLN
Naruszone przepisy RODO	• art. 31 RODO – obowiązek współpracy z organem nadzorczym w ramach wykonywania przez niego swoich zadań • art. 58 ust. 1 lit. e oraz f RODO – uprawnienia organu nadzorczego w zakresie uzyskiwania od administratora dostępu do wszelkich danych osobowych i informacji oraz wszystkich pomieszczeń w tym sprzętu i środków służących do przetwarzania danych osobowych
Kontekst	Do Urzędu Ochrony Danych Osobowych wpłynęła skarga na nieprawidłowości w procesie przetwarzania jego danych osobowych przez Smart Cities Sp. z o.o. Prezes UODO w ramach wszczętego postępowania administracyjnego prowadzonego celem rozpatrzenia wniesionej skargi zwrócił się do Spółki o ustosunkowanie się do treści skargi oraz o udzielenie odpowiedzi na szczegółowe pytania dotyczące sprawy. W odpowiedzi na wezwanie, Prezes Zarządu Spółki złożył organowi wyjaśnienia, które były niepełne przez co zatem nie dały podstawy do rozpatrzenia ww. skargi. Prezes UODO, uznając wyjaśnienia Spółki za niewystarczające, zwrócił się o ich uzupełnienie. Do dnia wydania decyzji Spółka nie udzieliła informacji niezbędnych do rozpatrzenia sprawy. W związku z powyższym, Smart Cities Sp. z o.o. z Warszawy ukarana została karą pieniężną w wysokości ponad 12 tys. zł za brak współpracy z UODO poprzez nieudzielanie odpowiedzi na jego pisma oraz niezapewnienie dostępu do danych osobowych i innych informacji niezbędnych do realizacji jego zadań. Utrudnianie i uniemożliwianie uzyskania dostępu do informacji, których UODO żądał od Spółki, a które niewątpliwie są w jej posiadaniu, świadczy o rażącym lekceważeniu swoich obowiązków dotyczących współpracy z organem nadzoru w ramach wykonywania przez niego zadań.

Komentarz eksperta

Marcin Szkutnik, radca prawny, ekspert ds. ochrony danych osobowych

Współpraca z organem nadzorczym jest jednym z podstawowych obowiązków jakie RODO nakłada na administratorów oraz podmioty przetwarzające. Obowiązek ten nabiera szczególnego znaczenia wtedy, gdy organ zwraca się o udzielenie informacji w ramach prowadzonych przez siebie postępowań. Z uzasadnienia decyzji wynika, że ukarana spółka nie udzieliła organowi

pełnych informacji, a później przestała nawet odbierać kierowanie do niej pisma. Dotychczasowa praktyka Prezesa UODO w podobnych przypadkach pokazuje, że brak współpracy z organem prowadzi do nałożenia kary pieniężnej (np. decyzja DKE.561.1.2020, decyzja DKE.561.2.2020). W tym kontekście, nie dziwi więc nałożenie kary pieniężnej na spółkę. Jak zawsze w takich przypadkach, do dyskusji pozostaje natomiast jej wysokość, a przede wszystkim to czy była ona adekwatna do skali naruszenia.

Decyzja	Decyzja Prezesa UODO z dnia 5 stycznia 2021 r. DKE.561.11.2020
Ukarany podmiot	Osoba fizyczna prowadząca działalność gospodarczą
Kwota kary pieniężnej	85 588,00 PLN
Naruszone przepisy RODO	• nieprzestrzeganie nakazu orzeczonego przez organ nadzorczy
Kontekst	Przedsiębiorca, prowadzący działalność gospodarczą w zakresie ochrony zdrowia, z administracyjną karą pieniężną w wysokości ponad 85 tys. zł za niewykonanie nakazu nałożonego wobec niego w decyzji administracyjnej. Urząd Ochrony Danych Osobowych nakazał przedsiębiorcy prowadzącemu działalność gospodarczą w zakresie ochrony zdrowia, zawiadomienie jego pacjentów o naruszeniu ich danych osobowych oraz przekazanie tym osobom zaleceń dotyczących zminimalizowania potencjalnych negatywnych skutków zaistniałego incydentu. Administrator tego nie zrobił, co wykazało postępowanie, którego celem było sprawdzenie, czy nałożone w decyzji UODO obowiązki zostały zrealizowane. W konsekwencji osoby, których dotyczyło naruszenie nic o nim nie wiedziały. Zdaniem organu, właściwe wywiązanie się z tego obowiązku pozwoliłoby zrozumieć osobom, których dane dotyczą, na czym polegało naruszenie ochrony ich danych osobowych, poznać możliwe konsekwencje takiego zdarzenia oraz jakie działania mogą podjąć w celu zminimalizowania jego ewentualnych negatywnych skutków. UODO zdecydował o wszczęciu z urzędu postępowania w sprawie nałożenia administracyjnej kary pieniężnej. Przedsiębiorca pomimo udzielenia mu przez organ szczegółowych wskazówek, m.in. dotyczących prawidłowego sformułowania zawiadomień i formy ich przekazania pacjentom, a także sposobu udokumentowania tych czynności, nawet na etapie postępowania w sprawie nałożenia kary nie przedstawił kompletnych dowodów, które pozwoliłyby uznać, że obowiązek wynikający z nakazu decyzji został przez niego wykonany. Niezastosowanie się przez przedsiębiorcę do udzielanych wskazówek, zdaniem organu świadczy o rażącym lekceważeniu przez niego obowiązków związanych z ochroną danych osobowych. Prezes UODO nakładając karę wziął pod uwagę czynniki obciążające tj.: długotrwały okres trwania naruszenia, co spowodowało zwiększone ryzyko zaistnienia negatywnych konsekwencji po stronie osób dotkniętych naruszeniem oraz umyślny charakter naruszenia i niezadowalający stopień współpracy z organem nadzorczym w celu usunięcia naruszenia.

Komentarz eksperta

Przemysław Zegarek, Prezes Lex Artist sp. z o.o., ekspert ds. ochrony danych osobowych

To kolejna kara z serii: UODO pokazuje, że nie można go lekceważyć. Przez wiele lat poprzednik UODO (Generalny Inspektor Ochrony Danych Osobowych), rzadko weryfikował realizację wydanych przez siebie decyzji. Teraz to się zmienia. Organ nadzorczy nie tylko sprawdza czy decyzje zostały wykonane. Jeśli decyzji nie wykonano, nakłada kary. Taka praktyka UODO wydaje się słuszna. Bez zdecydowanych działań regulatora w podobnych sytuacjach, nie ma co liczyć na respektowanie naszego prawa do prywatności.

Decyzja	Decyzja Prezesa UODO z dnia 11 lutego 2021 r. DKN.5130.2024.2020
Ukarany podmiot	Krajowa Szkoła Sądownictwa i Prokuratury
Kwota kary pieniężnej	100 000,00 PLN
Naruszone przepisy RODO	• art. 5 ust. 1 lit. f RODO – zasada integralności i poufności • art. 25 ust. 1 RODO – zasada *privacy by design* • art. 28 ust. 3 RODO – przetwarzanie przez podmiot przetwarzający na podstawie umowy lub innego instrumentu prawnego • art. 32 ust. 1 RODO – wdrożenie odpowiednich środków technicznych i organizacyjnych • art. 32 ust. 2 RODO – ocena stopnia bezpieczeństwa przy uwzględnieniu ryzyka wiążącego się z przetwarzaniem
Kontekst	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, 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 przez Komendę Główną Policji o pojawieniu się w Internecie danych osobowych związanych z domeną kssip.gov.pl. Zgłoszony incydent polegał na uzyskaniu przez nieznane osoby nieupoważnionego dostępu do kopii bazy danych witryny szkoleniowej KSSIP. Naruszenie dotyczyło danych osobowych ponad 50 tys. osób. Na zasobach informatycznych KSSiP znajdowała się kopia bazy danych, której istnienie i bezpieczeństwo, po wykonaniu czynności migracyjnych, w żaden sposób nie zostało zweryfikowane przez administratora, co jest jego prawnym obowiązkiem wynikającym z przepisów o ochronie danych osobowych. KSSIP, w związku ze zmianami w procesie przetwarzania, nie podjęła wystarczających działań mających

	na celu zweryfikowanie bezpieczeństwa środowiska przetwarzania przed rozpoczęciem działań migracyjnych, jak i po ich zakończeniu. Treść umowy powierzenia w tej sprawie w sposób niewystarczający określała zakres powierzanych danych. KSSiP, powierzając przetwarzanie danych osobowych podmiotowi przetwarzającemu, nie zawarła w umowie powierzenia przetwarzania danych osobowych kategorii osób oraz nie doprecyzowała rodzaju danych osobowych przez wskazanie ich kategorii. Ponadto ukarany podmiot nie zawarł w umowie zobowiązania podmiotu przetwarzającego do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora. Model współpracy administratora z podmiotem przetwarzającym był nieskuteczny. Brak zrozumienia przez administratora roli, jaką on pełni w relacji z podmiotem przetwarzającym, doprowadziły do naruszenia ochrony danych osobowych. KSSiP, zarówno przed naruszeniem ochrony danych, jak i po jego stwierdzeniu, nie miała pełnej świadomości, jak kształtują się prawa i obowiązki, pomiędzy administratorem a podmiotem przetwarzającym. Zdaniem organu podmiot przetwarzający wypełniał obowiązki wynikające z umowy powierzenia i umowy głównej, a także stosował przyjęte przez siebie środki organizacyjne mające na celu zapewnienie bezpieczeństwa systemów informatycznych. To administrator nie podjął się analizy, czy wskazując podmiotowi przetwarzającemu miejsce do wykonania kopii zapasowej bazy danych, nie naraża danych osobowych w niej zawartych na naruszenie ich poufności.

Komentarz eksperta

Przemysław Zegarek, Prezes Lex Artist sp. z o.o., ekspert ds. ochrony danych osobowych

Kara nałożona została w maksymalnym możliwym wymiarze dla podmiotu publicznego, tj. 100 tys. złotych. Z pewnością, przesłanką mającą wpływ na wysoki wymiar kary, była skala naruszenia. Naruszenie dotyczyło ok. 50 tys. osób i wydarzyło się w organizacji, zajmującej się szkoleniem sędziów i prokuratorów. Zakres informacji, które zostały ujawnione, jest szeroki: imię i nazwisko, adres e-mail, nazwę użytkownika, numer telefonu, jednostkę, wydział, adres jednostki, miejscowość, numer ewidencyjny PESEL.

Przy większości naruszeń RODO, kończących się nałożeniem wysokich kar, przyczyn jest co najmniej kilka. W tym przypadku jest oczywiście podobnie. Popełnione błędy to nieuwzględnienie zasady privacy by design, błędna współpraca z procesorem, nieodpowiednie zabezpieczenia techniczne i nieuwzględnienie ryzyka.

Szczególną uwagę zwracam na dwa obszary. Pierwszy z nich to zasada *privacy by design*. Gdyby odpowiednio zabezpieczono dane osobowe już w fazie projektowania procesu, cała sytuacja zakończona naruszeniem, nie miałaby prawa zaistnieć. Więcej ciekawych przykładów o zasadzie privacy by design znajdziesz na naszym blogu.

Jednak nawet brak odpowiedniego zastosowania zasady privacy by design nie musiał zakończyć się naruszeniem RODO i nałożeniem kary. Gdyby ADO odpowiednio kontrolował swojego procesora, to sytuacja wyglądałaby zupełnie inaczej.

Proponuję zapoznanie się z naszym blogowym poradnikiem w zakresie audytu procesora.

Na każde naruszenie warto spojrzeć z perspektywy łańcucha błędów, które w efekcie prowadzą do nałożenia kary. W większości przypadków, pojedynczy błąd wcale nie musi prowadzić do najgorszego. Dopiero suma braków daje efekt w postaci nałożenia kary. Pamiętajmy o tym, że każdy system RODO ma słabe punkty. Jeśli jednak system jako całość funkcjonuje sprawnie, to awaria pojedynczego fragmentu, nie doprowadzi do najgorszego.

Decyzja	Decyzja Prezesa UODO z dnia 5 stycznia 2021 r. DKN.561.16.2020
Ukarany podmiot	Anwara Sp. z o.o.
Kwota kary pieniężnej	21 397,00 PLN
Naruszone przepisy RODO	• art. 31 RODO – obowiązek współpracy z organem nadzorczym w ramach wykonywania przez niego swoich zadań • art. 58 ust. 1 lit. a RODO – uprawnienie organu nadzorczego do nakazania dostarczenia wszelkich informacji potrzebnych do realizacji swoich zadań
Kontekst	Prezes UODO nałożył karę w wysokości ponad 21 tys. złotych na spółkę Anwara Sp. z o.o. z siedzibą w Warszawie, która, będąc administratorem danych osobowych, nie wywiązała się z obowiązku współpracy z organem nadzorczym i nie dostarczyła mu wszelkich informacji potrzebnych do realizacji jego zadań w toku postępowania. Ukarana spółka w związku z postępowaniem administracyjnym, prowadzonym w celu rozpoznania skargi osoby fizycznej, dwukrotnie zignorowała wystosowane do niej pisemne wezwania do złożenia wyjaśnień. Pomimo prawidłowego doręczenia pism spółka nie przedstawiła żadnych przyczyn uzasadniających zaniechanie po jej stronie. W związku z nieudzieleniem przez spółkę informacji, organ nadzorczy wszczął z urzędu postępowanie administracyjne w przedmiocie nałożenia na nią administracyjnej kary pieniężnej. Ukarany podmiot także w tej sprawie nie ustosunkował się w żaden sposób do ww. korespondencji i nie złożył wyjaśnień.

Komentarz eksperta

Krystian Dobosz, starszy specjalista ds. ochrony danych osobowych

Kara dla Spółki Anwara to kolejny przykład braku współpracy administratora danych z Prezesem UODO. Jednym z obowiązku administratora jest udzielanie odpowiedzi na wszelkie pytania przesłane przez regulatora. Brak współpracy co do zasady jest negatywnie odbierany przez kontrolerów UODO. Tak było w tej sytuacji.

Spółka zignorowała pisma skierowane do niej i w mojej ocenie zadziałała na swoją niekorzyść. Organ chce widzieć kooperację, chce rzetelnie wyjaśnić stan faktyczny. Brak kontaktu ze strony Spółki był odebrany jako brak chęci współpracy, co przełożyło się finalnie na wysokość nałożonej kary.

Milczenie z naszej strony – jako administratora danych - nie spowoduje, że Prezes UODO o nas zapomni. Dlatego też róbmy wszystko by wyjaśniać wątpliwości organu nadzorczego.

Co zrobić kiedy napisze do nas Prezes UODO? Tego dowiecie się z naszego artykułu poświęconego zasadom korespondencji z organem.

Decyzja	Decyzja Prezesa UODO z dnia 11 stycznia 2021 r. DKN.5131.7.2020
Ukarany podmiot	ENEA S.A.
Kwota kary pieniężnej	136 437,00 PLN
Naruszone przepisy RODO	• art. 33 ust. 1 RODO – zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu
Kontekst	Prezes Urzędu Ochrony Danych Osobowych nałożył na spółkę ENEA S.A. administracyjną karę pieniężną w wysokości ponad 136 tys. zł za brak zgłoszenia naruszenia ochrony danych osobowych. Do UODO wpłynęła informacja o naruszeniu ochrony danych osobowych pochodząca od osoby, która stała się nieuprawnionym adresatem danych osobowych. Naruszenie to polegało na wysłaniu e-maila z niezaszyfrowanym, nie zabezpieczonym hasłem załącznikiem zawierającym dane osobowe kilkuset osób. Nadawcą maila był współpracownik ukaranego przedsiębiorstwa. UODO zwróciło się do spółki o wyjaśnienie okoliczności zdarzenia. Ukarany podmiot wskazał, że została dokonana ocena pod kątem ryzyka naruszenia praw i wolności osób fizycznych, na podstawie której spółka uznała, iż nie doszło do naruszenia skutkującego koniecznością zawiadomienia UODO. ENEA S.A. uznała, że ze względu na szybko podjęte działania, jak oświadczenie nieuprawnionego adresata, że w sposób trwały zniszczył załącznik, do którego otrzymania nie był upoważniony, wyeliminowano możliwość zaistnienia w przyszłości negatywnych skutków tego zdarzenia dla osób, których dane dotyczą. Z uwagi na brak zgłoszenia naruszenia ochrony danych osobowych, organ wszczął wobec spółki postępowanie administracyjne. UODO wskazał, że w przedmiotowej sprawie doszło do wysłania do nieuprawnionego odbiorcy wiadomości e-mail wraz z załącznikiem w postaci niezaszyfrowanego pliku zawierającego dane osobowe adresata wiadomości i innych osób. Oznacza to, że doszło do naruszenia bezpieczeństwa prowadzącego do przypadkowego ujawnienia danych osobowych osobie nieuprawnionej do otrzymania tych danych, a więc do naruszenia poufności danych tych osób, co przesądza, że wystąpiło naruszenie ochrony danych osobowych. Do dnia wydania niniejszej decyzji, spółka nie wykonała obowiązku wynikającego z art. 33 RODO. Ustalając wysokość administracyjnej kary pieniężnej, organ uwzględnił również okoliczności łagodzące, mające wpływ na ostateczny wymiar kary, tj. działania podjęte przez administratora w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą.

Komentarz eksperta

Małgorzata Zdunek, ekspert ds. ochrony danych osobowych

To już kolejna kara finansowa Prezesa UODO związana z naruszeniem ochrony danych osobowych. Tym razem mamy do czynienia z sytuacją, kiedy administrator danych w sposób odmienny niż organ, zinterpretował zdarzenie związane z wysyłką niezaszyfrowanego pliku z danymi do nieuprawnionego adresata. ENEA S.A. nie doszukała się w tym zakresie znamion incydentu, powołując się m.in. na odebrane od nieuprawnionego adresata oświadczenie.

Mając w pamięci decyzję Prezesa UODO nakładającą karę na TUiR WARTA S.A. trudno zrozumieć takie postępowanie ukaranej spółki. W powoływanej decyzji, organ wskazał, że odebrane od nieuprawnionego adresata oświadczenie o zniszczeniu otrzymanej korespondencji, nie ma wpływu na kwalifikację danego zdarzenia jako naruszenie. Nie ma bowiem pewności, że wcześniej osoba ta nie wykonała np. kserokopii danych osobowych. Administrator nie ma też możliwości faktycznej weryfikacji złożonego oświadczenia.

Jak zatem poprawie dokonać kwalifikacji zdarzenia, które może być naruszeniem ochrony danych osobowych? Zapraszam do zapoznania się z praktycznymi przykładami naruszeń, z którymi na co dzień mierzą się nasi eksperci.

Decyzja	Decyzja Prezesa UODO z dnia 22 kwietnia 2021 r. DKN.5130.3114.2020
Ukarany podmiot	Cyfrowy Polsat S.A.
Kwota kary pieniężnej	1 136 975,00 PLN
Naruszone przepisy RODO	• art. 24 ust. 1 RODO – wdrożenie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z rozporządzeniem • art. 32 ust. 1 RODO – wdrożenie odpowiednich środków technicznych i organizacyjnych w celu zapewnienia stopnia bezpieczeństwa odpowiadającego ryzyku naruszenia praw lub wolności osób fizycznych • art. 32 ust. 2 RODO – ocena stopnia bezpieczeństwa przy uwzględnieniu ryzyka wiążącego się z przetwarzaniem
Kontekst	Cyfrowy Polsat S.A. nie wdrożył odpowiednich środków technicznych i organizacyjnych przy współpracy z firmą kurierską. Efektem tego były liczne naruszenia identyfikowane z dużym opóźnieniem. Z powodu tych zaniedbań Prezes UODO nałożył na spółkę karę pieniężną w wysokości ponad 1,1 mln zł. Zgubiona korespondencja z danymi osobowymi lub dostarczenie takiej przesyłki do niewłaściwego odbiorcy – to naruszenia, które spółka często zgłaszała do Urzędu Ochrony Danych Osobowych. W dodatku przeprowadzona przez UODO analiza tych naruszeń wykazała, że administrator zgłaszał naruszenia organowi nadzorczemu, jak i powiadamiał o incydentach osoby, których one dotyczyły, po upływie dwóch, a nawet trzech miesięcy od ich wystąpienia. W toku postępowania okazało się, że administrator zgłaszał naruszenia, gdy tylko informację o nich otrzymał od firmy kurierskiej, z którą miał podpisaną umowę. Zdaniem UODO, to administrator powinien podjąć skuteczne działania, które po pierwsze zminimalizują skalę naruszeń, a po drugie pozwolą na szybsze identyfikowanie takich incydentów i tym samym powiadamianie o nich osób, których dotyczy dane zdarzenie oraz organu nadzorczego. Brak wdrożonych odpowiednich środków organizacyjnych i technicznych pozwalających szybko identyfikować naruszenia powodował, że osoby, których dane dotyczą, przez długi czas nie wiedziały o ryzyku wykorzystania ich danych przez osoby nieuprawnione, np. do tzw. kradzieży ich tożsamości. Pomimo że naruszenia związanie były z nieprawidłowościami po stronie firmy kurierskiej, to właśnie ukarany administrator danych nieprawidłowo realizował nadzór nad egzekwowaniem postanowień umownych, przez co dochodziło do późnej identyfikacji naruszeń. Prezes UODO zdecydował się nałożyć na spółkę karę za naruszenia przepisów RODO, gdyż zastosowanie innych środków naprawczych nie byłoby proporcjonalne

	do stwierdzonych nieprawidłowości. Nie gwarantowałoby również tego, że administrator ten w przyszłości nie dopuści się podobnych zaniedbań.

Komentarz eksperta

Przemysław Zegarek, Prezes Lex Artist sp. z o.o., ekspert ds. ochrony danych osobowych

Kara nałożona na Cyfrowy Polsat jest jedną z wyższych kar w krótkiej historii funkcjonowania UODO. Organ nadzorczy wskazuje na kluczowe elementy, które zaważyły na wysokości kary.

1) Po pierwsze, wyjątkowo długi okres, który upływał między faktycznym wystąpieniem incydentu, a jego zgłoszeniem do UODO. W części przypadków było to nawet 120 dni (!). Dużo mówi w tej materii poniższy fragment Decyzji: „*Nawiasem mówiąc, przypadki zgłaszanych naruszeń ochrony danych osobowych związanych z nieprawidłowościami po stronie operatorów pocztowych nie należą do wyjątkowych w praktyce UODO, do wyjątków należą jednak sytuacje, w których administrator nie podejmuje natychmiastowych działań związanych z zaginięciem bądź nieprawidłowym doręczeniem nadanych przez siebie przesyłek zawierających dane osobowe klientów.*"

2) Z treści decyzji wynika, że również liczba zgłoszonych do UODO naruszeń musiała być wysoka. Niestety nie podano konkretnych liczb.

3) Dodatkowo organ ma także wątpliwości co do stosowanej metodyki kalkulowania ryzyka przez Cyfrowy Polsat. Nie jest również usatysfakcjonowany przesyłanymi odpowiedziami, które nie zawsze stanowią bezpośrednią odpowiedź na pytania UODO. Brakuje też konkretnych dowodów o które prosili urzędnicy.

4) Warto dodać, że bezpośrednim sprawcą naruszeń nie był ukarany Cyfrowy Polsat. To kolejny argument za stosowaniem dobrych umów powierzenia, należycie zabezpieczających administratora danych. Jeśli proces oparty jest na udostępnieniu danych, to również warto przewidzieć sytuacje związane z ryzykiem naruszeń po stronie dostawcy, który nie jest procesorem.

Żeby ustrzec się przed podobnymi sytuacjami, zapraszam do lektury specjalistycznych artykułów na naszym blogu:

1) jak radzić sobie z naruszeniami ochrony danych osobowych,

2) korespondowanie z UODO, które pomoże rozwiązać sprawę, a nie ją zaognić,

3) umowy powierzenia, które dobrze zabezpieczą interesy administratora danych.

Decyzja	Decyzja Prezesa UODO z dnia 27 kwietnia 2021 r. DKE.561.230.2020
Ukarany podmiot	PNP S.A.
Kwota kary pieniężnej	22 739,00 PLN
Naruszone przepisy RODO	• art. 31 RODO – obowiązek współpracy z organem nadzorczym w ramach wykonywania przez niego swoich zadań • art. 58 ust. 1 lit. e RODO – uprawnienia organu nadzorczego w zakresie uzyskiwania od administratora dostępu do wszelkich danych osobowych i informacji
Kontekst	Powodem nałożenia przez Prezesa UODO kary pieniężnej w kwocie ponad 22 tys. złotych był brak współpracy z organem nadzorczym oraz niezapewnienie dostępu do wszelkich informacji niezbędnych do realizacji przez UODO zadań. UODO w celu ustalenia stanu faktycznego sprawy zainicjowanej skargą, trzykrotnie zwrócił się do PNP S.A. z wezwaniem do ustosunkowania się do treści tej skargi oraz do złożenia wyjaśnień. Żadne ze skierowanych wezwań nie zostało przez Spółkę odebrane, pomimo dwukrotnego ich awizowania. W związku z tym wysłane Spółce wezwania zostały uznane za doręczone. W konsekwencji niepodejmowania przez PNP S.A. kierowanej do niej korespondencji, UODO nie uzyskało informacji niezbędnych do rozpatrzenia sprawy. Stanu tego nie zmieniło również wszczęcie postępowania w przedmiocie nałożenia administracyjnej kary pieniężnej. Pismo informujące o wszczęciu takiego postępowania również nie zostało przez Spółkę odebrane. W decyzji podkreślone zostało, że odpowiedzialność za nieudzielenie UODO żądanych przez niego informacji spoczywa na Spółce. Nie zmienia tego okoliczność, że wezwania kierowane przez UODO do Spółki nie zostały ostatecznie przez nią odebrane. Przytaczając orzecznictwo sądów administracyjnych wskazano, że powinnością każdej jednostki organizacyjnej jest zapewnienie takiej organizacji odbioru pism, aby przebieg korespondencji odbywał się w sposób ciągły i niezakłócony oraz wyłącznie przez osoby uprawnione. Zaniedbania w tym zakresie obciążają tę właśnie jednostkę organizacyjną. Spółka nie odpowiadając na wezwania UODO, naruszyła obowiązek zapewnienia organowi nadzorczemu dostępu do informacji niezbędnych do realizacji jego zadań – w tym przypadku do merytorycznego rozstrzygnięcia sprawy.

Komentarz eksperta

Małgorzata Zdunek, ekspert ds. ochrony danych osobowych

To już kolejna kara pieniężna nałożona przez Prezesa UODO za brak współpracy z organem. Tym razem mamy jednak do czynienia z sytuacją, kiedy pisma przesyłane przez regulatora w ogóle nie były odbierane. Pamiętajmy, że nieodebranie kierowanego do nas pisma nie oznacza, że unikniemy postępowania w sprawie, której ono dotyczy. Takim działaniem odbieramy sobie jedynie możliwość przedstawienia naszego stanowiska i narażamy się na poważne (nawet finansowe) konsekwencje.

Nałożona przez Prezesa UODO kara pieniężna, niewątpliwie zdyscyplinuje Spółkę do podjęcia współpracy z organem.

Nie powinniśmy obawiać się prowadzenia korespondencji z UODO. Niejednokrotnie, może ona iść gładko i zakończyć się na jednym piśmie. Warto dołożyć najwyższej staranności i nie popełniać przy tym prostych błędów. O korespondencyjnych błędach oraz o tym jak ich unikać, pisaliśmy na naszym blogu w artykule: Korespondencja z UODO – 7 najczęstszych błędów.

Decyzja	Decyzja Prezesa UODO z dnia 19 marca 2021 r. DKE.561.25.2020
Ukarany podmiot	Funeda Sp. z o.o.
Kwota kary pieniężnej	22 739,50 PLN
Naruszone przepisy RODO	• art. 31 RODO – obowiązek współpracy z organem nadzorczym w ramach wykonywania przez niego swoich zadań • art. 58 ust. 1 lit. a RODO – uprawnienie organu nadzorczego do nakazania dostarczenia wszelkich informacji potrzebnych do realizacji swoich zadań • art. 58 ust. 1 lit. e RODO – uprawnienia organu nadzorczego w zakresie uzyskiwania od administratora dostępu do wszelkich danych osobowych i informacji
Kontekst	Na Funeda Sp. z o.o. została nałożona administracyjna kara pieniężna w wysokości ponad 22 tysięcy złotych za brak współpracy z Urzędem Ochrony Danych Osobowych. Brak współpracy polegał na tym, że ukarana spółka nie zapewniła dostępu do wszelkich danych osobowych i informacji niezbędnych UODO do rozpatrzenia skargi na nieprawidłowości w procesie przetwarzania danych osobowych. Urząd w ramach wszczętego postępowania administracyjnego prowadzonego w celu rozpatrzenia wniesionej skargi, zwrócił się do spółki o ustosunkowanie się do treści skargi oraz o udzielenie odpowiedzi na szczegółowe pytania dotyczące sprawy. UODO dwukrotnie wezwał spółkę do udzielenia wyjaśnień niezbędnych do rozpatrzenia sprawy. Spółka pomimo odbioru korespondencji nie udzieliła żadnej odpowiedzi na skierowane pisma. W związku z nieudzielaniem informacji w sprawie, UODO wszczęło postępowanie w przedmiocie nałożenia administracyjnej kary pieniężnej. Urząd wielokrotnie podejmował próby kontaktu telefonicznego i mailowego ze spółką w oparciu o dane zawarte na stronie internetowej. Do dnia wydania decyzji spółka nie skontaktowała się z Urzędem.

Komentarz eksperta

Krystian Dobosz, starszy specjalista ds. ochrony danych osobowych

Chciałoby się rzec, że nie ma miesiąca, w którym Prezes UODO nie nakłada kary na administratorów danych za brak współpracy. Kolejny raz Spółka, poprzez własne zaniechanie, powoduje, że wszczęte jest postępowanie i nałożona kara administracyjna przez organ nadzorczy.

Wystarczyło złożyć wyjaśnienia, być może dokonać jakichś działań, które były wymagane i sprawa mogłaby zakończyć w sposób mniej dotkliwy dla administratora danych. W tej sytuacji Spółka nie reagowała jednak na pisma otrzymane od Prezesa UODO. Co więcej, organ robił co w jego mocy, żeby nawiązać kontakt ze Spółką – dzwonił, pisał maile, na adresy dostępne na stronie Spółki, lecz niestety nie udało się uzyskać jakichkolwiek wyjaśnień ze strony administratora danych.

Nie wiemy czy Spółka wyszła z założenia, że skoro nie ma kontaktu, nie będzie konsekwencji? Jeśli czytacie nasz rejestr kar, wiecie, że „chowanie głowy w piasek" nie spowoduje, że Prezes UODO odstąpi od dalszych działań. Niestety nasz brak współpracy działa na naszą szkodę i powoduje, że postępowanie może zakończyć się nałożeniem kary finansowej, tak jak było właśnie w tym przypadku.

Daje się natomiast zauważyć pewną prawidłowość – za brak współpracy z regulatorem, nakładana jest stała kwota – ok. 5000 €, co jest równowartością ok. 20000-22000 zł.

Kwota ta ma być przestrogą dla innych administratorów i być odczuwalna w budżecie firmy, tak by w przyszłości nie unikać kooperacji z organem nadzorczym. Po raz kolejny rekomendujemy pełną współpracę z Prezesem UODO, co pozwoli uniknąć przykrych konsekwencji.

Jeśli korespondencja z organem powoduje u Ciebie stres – zajrzyj do naszego artykułu i dyskutuj z UODO po partnersku.

Decyzja	Decyzja Prezesa UODO z dnia 8 czerwca 2021 r. DKN.5131.10.2020
Ukarany podmiot	P4 Sp. z o.o.
Kwota kary pieniężnej	100 000,00 PLN
Naruszone przepisy	• art. 174a ust. 1 Ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne w zw. z art. 2 ust. 2 rozporządzenia Komisji (UE) Nr 611/2013 z dnia 24 czerwca 2013 r. w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej
Kontekst	Prezes Urzędu Ochrony Danych Osobowych nałożył na P4 Sp. z o.o. administracyjną karę pieniężną w wysokości 100 tys. złotych za niezawiadomienie organu nadzorczego w terminie 24 godzin o wykryciu naruszenia danych osobowych. Powodem nałożenia administracyjnej kary było naruszenie przepisów Prawa telekomunikacyjnego oraz rozporządzenia Komisji (UE) nr 611/2013 w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej. Przedsiębiorca telekomunikacyjny w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych zobowiązany jest w szczególności powiadomić o tym organ ds. ochrony danych osobowych, a także abonenta lub użytkownika końcowego, którego dane zostały naruszone. Ponadto na mocy tych przepisów administrator danych jest zobowiązany do zawiadomienia organu nadzorczego o naruszeniu danych osobowych w terminie 24 godzin. Postępowaniem objęto łącznie pięć naruszeń danych osobowych, zgłoszonych po upływie 24 godzin od ich wykrycia. Spółka w postępowaniu wyjaśniła, że dokonanie zawiadomień o naruszeniu danych osobowych po upływie 24 godzin związane było z nieumyślnym błędem pracowników kancelarii odpowiedzialnych za wysyłkę korespondencji. Błąd ten polegał m.in. na niewpisaniu korespondencji do książki nadawczej, czego efektem był jej zwrot przez operatora pocztowego. UODO kilkukrotnie informował spółkę, że zgłoszenia naruszenia danych osobowych można dokonać na dwa sposoby: elektronicznie oraz pocztą tradycyjną, a także wskazywał, że najszybszą drogą jest wysłanie zgłoszenia za pośrednictwem platformy biznes.gov.pl lub platformy ePUAP, co zapewnia dotrzymanie określonego przepisami prawa terminu. Nałożona kara, w opinii UODO, jest adekwatna do stwierdzonego naruszenia przepisów.

Komentarz eksperta

Krystian Dobosz, starszy specjalista ds. ochrony danych osobowych

RODO nakłada na administratora obowiązek zgłoszenia naruszenia w terminie 72h od momentu stwierdzenia. Operatorzy telekomunikacyjni podlegają jednak bardziej restrykcyjnym wymogom, wskazanym w Rozporządzeniu Komisji (UE) w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej. Regulacja ta przewiduje 24h na zgłoszenie naruszenia. Jest to zatem istotna modyfikacja, w stosunku do terminu ogólnego.

W przypadku kary nałożonej na operatora sieci Play naruszenie zgłoszono po terminie, co mogło narazić osoby, które dane wyciekły na negatywne konsekwencje.

Jak się okazało, próby zrzucenia odpowiedzialności na pracowników kancelarii operatora sieci Play nie zostały uznane przez Prezesa Urzędu Ochrony Danych Osobowych, co tylko potwierdza, że to administrator jest odpowiedzialny za takie zorganizowane systemu ochrony danych osobowych, by realizować obowiązki prawidłowego identyfikowania i zgłaszania incydentów.

Co więcej, w dobie coraz bardziej postępującej cyfryzacji, wydaje się, że zgłaszanie naruszeń drogą tradycyjnej wysyłki pocztowej powinno coraz bardziej odchodzić do lamusa, zwłaszcza wtedy, kiedy regulacja szczegółowa nakazuje jak najpilniejsze działanie.

Być może Prezes UODO podszedłby do sprawy bardziej liberalnie, gdyby była to sytuacja jednorazowa. Takich naruszeń dochowania terminu było jednak kilka. Jak się okazało, regulator wskazywał na możliwość elektronicznego zgłaszania naruszeń jako jedną z dróg działania. Operator realizował jednak wysyłkę „tradycyjnie", poprzez wysyłanie listu przez operatora pocztowego.

Jak się okazało, Play wyciągnął wnioski i późniejsze zgłoszenia naruszeń były już realizowane za pośrednictwem platformy ePuap, co jest na pewno pewniejszym i bardziej skutecznym rozwiązaniem.

Podsumowując, operatorzy telekomunikacyjni nie mogą zatem zapominać, że termin 24h jest istotny i jak widać, Prezes UODO będzie respektował jego przestrzeganie z całą stanowczością.

Decyzja	Decyzja Prezesa UODO z dnia 21 czerwca 2021 r. DKN.5131.3.2021
Ukarany podmiot	Sopockie Towarzystwo Ubezpieczeń ERGO Hestia S.A.
Kwota kary pieniężnej	159 176,00 PLN
Naruszone przepisy RODO	• art. 33 ust. 1 RODO – zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu • art. 34 ust. 1 RODO – zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych
Kontekst	Urząd Ochrony Danych Osobowych nałożył administracyjną karę pieniężną na Sopockie Towarzystwo Ubezpieczeń ERGO Hestia S.A. w wysokości prawie 160 tys. zł za niezgłoszenie naruszenia ochrony danych osobowych. Ponadto Spółkę ukarano za niezawiadomienie osoby, której dane dotyczą o naruszeniu, do czego zobowiązał ją także organ nadzorczy. Naruszenie polegało na wysłaniu pocztą elektroniczną przez pracownika pośrednictwa finansami do niewłaściwego odbiorcy analizy potrzeb ubezpieczeniowych oraz oferty ubezpieczenia, zawierającą dane jak imię, nazwisko, numer PESEL, miejscowość, kod pocztowy czy informację o przedmiocie ubezpieczenia. Podmiot ten, będąc administratorem danych w postaci imienia i nazwiska, zdecydował się dokonać zgłoszenia naruszenia ochrony danych osobowych do UODO. Podmiot, który dokonał naruszenia, występował jednocześnie w roli podmiotu przetwarzającego towarzystw ubezpieczeniowych, dlatego też zawiadomił je o naruszeniu. Przeprowadzona przez UODO weryfikacja wykazała, że w związku z tym incydentem kilka towarzystw ubezpieczeniowych jako administratorzy danych, dokonało zgłoszenia naruszenia ochrony danych. Zgłoszenia takiego nie odnotowano od Sopockiego Towarzystwa Ubezpieczeń ERGO Hestia S.A. UODO zwrócił się do spółki o wyjaśnienia. Spółka wskazała, że na podstawie wykonanej oceny pod kątem ryzyka naruszenia praw i wolności osób fizycznych uznano, iż nie doszło do naruszenia skutkującego koniecznością zgłoszenia naruszenia Prezesowi UODO oraz zawiadomienia osoby, której danych osobowych dotyczy naruszenie. Ponadto spółka przedstawiła oświadczenie złożone przez nieuprawnionego odbiorcę wiadomości, z którego wynika, że nie jest w posiadaniu wysłanych dokumentów, oraz że nie jest mu znana treść załączonych do wiadomości dokumentów, gdyż nie zapoznawał się z ich treścią przed usunięciem wiadomości.

	UODO uznał, że oświadczenie takie nie wyklucza przyjęcia, że wystąpiło wysokie ryzyko naruszenia praw lub wolności osoby, której dane dotyczą, jak i nie wyklucza możliwości wystąpienia negatywnych konsekwencji w przyszłości. Zdaniem UODO w tej sprawie doszło do naruszenia bezpieczeństwa, ponieważ dane osobowe zostały udostępnione nieuprawnionemu odbiorcy, którego nie można uznać za „odbiorcę zaufanego", a zakres tych danych przesądza o tym, że wystąpiło wysokie ryzyko naruszenia praw lub wolności osób fizycznych. To skutkuje powstaniem po stronie spółki obowiązku zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu.

Komentarz eksperta

Krystian Dobosz, starszy specjalista ds. ochrony danych osobowych

Tym razem Prezes UODO ukarał Sopockie Towarzystwo Ubezpieczeniowe ERGO Hestia. Naruszenie polegało na przesłaniu danych osobowych niewłaściwemu odbiorcy. Zakres danych był dość istotny – było to m.in. imię, nazwisko, PESEL, adres zamieszkania, a także informacje o przedmiocie ubezpieczenia. Taki zakres danych, już na pierwszy rzut oka wskazuje, że występuje wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą. Dysponując takim kompletem ujawnionych danych, powinniśmy nie dość, że zawiadomić Prezesa Urzędu Ochrony Danych Osobowych, to także osobę, której dane dotyczą. Wynika to z wytycznych oraz praktyki orzeczniczej organu nadzorczego.

Posiadanie danych identyfikujących w postaci PESELu, może m.in. powodować stratę finansową, możliwość zawierania umów cywilnoprawnych przy wykorzystaniu dowodu kolekcjonerskiego, czy próbę wejścia w posiadanie danych medycznych tej osoby. ERGO Hestia jako jedyna odstąpiła od powiadomienia regulatora (zrobiły to inne towarzystwa). Ponadto ERGO Hestia nie powiadomiła osoby, której dane dotyczą, mimo nakazu ze strony Prezesa UODO.

Dodatkowo, w toku postępowania organu nadzorczego okazało się, że analiza naruszenia została przeprowadzona w sposób nierzetelny. Analiza ta zaniżała wiele istotnych czynników czy wręcz pomijała je, co miało usprawiedliwiać brak zgłoszenia naruszenia do organu nadzorczego. Co istotne, ERGO Hestia otrzymała od osoby, która weszła w posiadanie tych danych w sposób nieuprawnionych, oświadczenie wskazujące, że osoba ta nie zapoznała się z treścią dokumentów, a także dokumenty te zostały trwale usunięte. Miał to być kolejny argument wskazujący na brak konieczności powiadamiania organu nadzorczego.

Organ uznał, że takie oświadczenie nie powoduje, że nie występuje wysokie ryzyko naruszenia praw lub wolności osoby, której dane dotyczą, a także nie wyklucza wystąpienia negatywnych konsekwencji w przyszłości. Mimo takiego oświadczenia, nie można uznać takiej osoby, za „odbiorcę zaufanego" i przewidzieć czy na pewno nie będzie chciała wykorzystać takiego zakresu danych, w sposób sprzeczny z przepisami.

Jest to kolejne tego typu stanowisko Prezesa UODO. Wedle organu, oświadczenia takie nie powodują, że dane nie mogą zostać wykorzystane w przyszłości przez osobę, która ich adresatem

nie była. Podobna argumentacja co w sprawie ERGO Hestia, znalazła się w decyzji nakładającą karę na Towarzystwo Ubezpieczeń i Reasekuracji WARTA S.A.

Wszelkie czynniki spowodowały, że Prezes UODO nałożył karę w wysokości prawie 160 tys. zł, co ma wpłynąć na wszystkich administratorów, którzy celowo zaniżają poziom ryzyka w swoich analizach, byleby unikać zgłaszania naruszenia czy powiadamiania osób. Jeśli nie masz pewności, czy masz do czynienia z naruszeniem, zapoznaj się z naszym artykułem.

Decyzja	Decyzja Prezesa UODO z dnia 30 czerwca 2021 r. DKN.5131.11.2020
Ukarany podmiot	Fundacja Promocji Mediacji i Edukacji Prawnej Lex Nostra
Kwota kary pieniężnej	13 644,00 PLN
Naruszone przepisy RODO	• art. 33 ust. 1 RODO – zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu • art. 34 ust. 1 RODO – zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych
Kontekst	Fundacja Promocji Mediacji i Edukacji Prawnej Lex Nostra została ukarana administracyjną karą pieniężną w wysokości ponad 13 tys. zł za niezgłoszenie organowi nadzorczemu naruszenia ochrony danych osobowych oraz niezawiadomienie o incydencie osób, których dane dotyczą. Dodatkowo UODO nakazało Fundacji zawiadomienie osób, których dane dotyczą o zaistniałym naruszeniu w terminie 3 dni od doręczenia decyzji. Jesienią 2020 r. do Urzędu Ochrony Danych Osobowych wpłynęło zawiadomienie o podejrzeniu naruszenia zasad przestrzegania przepisów o ochronie danych osobowych przez Fundację Promocji Mediacji i Edukacji Prawnej LEX NOSTRA polegające na utracie danych osobowych wielu osób, jaka miała miejsce na początku 2020 r., na skutek kradzieży teczek zawierających dane osobowe beneficjentów. Fundacja tego incydentu nie zgłosiła, gdyż dokonana przez nią analiza naruszenia dała ocenę jego wagi na poziomie niskim. Na jej podstawie Fundacja uznała, iż nie doszło do naruszenia skutkującego koniecznością zawiadomienia organu nadzorczego. W toku dalszych czynności ustalono, że naruszenie dotyczyło 96 osób, a utracona dokumentacja zawierała następujące kategorie danych jak m.in. imię, nazwisko, adres do korespondencji, numer telefonu. W przypadku 3-4 osób prawdopodobnie utracono także numer PESEL. UODO podkreślił, że z ryzykiem naruszenia praw lub wolności osób fizycznych mamy do czynienia wówczas, kiedy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych. Możliwe konsekwencje nie muszą się zmaterializować, samo potencjalne wystąpienie ryzyka dla praw lub wolności powinno skłonić administratora danych osobowych, do zgłoszenia naruszenia oraz powiadomienia o incydencie zainteresowanych osób.

	Fundacja podejmując decyzję o niezawiadomieniu o naruszeniu organu nadzorczego, jak i osób, których dane dotyczą, w praktyce pozbawiła te osoby możliwości przeciwdziałania potencjalnym szkodom.

Komentarz eksperta

Małgorzata Zdunek, ekspert ds. ochrony danych osobowych

To kolejna kara Prezesa UODO nałożona za naruszenie przepisów art. 33 i 34 RODO, czyli w związku z naruszeniem ochrony danych osobowych. Kolejny administrator doszedł do wniosku, że informowanie organu oraz osób, których dane zostały naruszone jest zbędne. Warto zauważyć, że ukarany podmiot wskazał, że dokonana kalkulacja naruszenia wskazywała, że występuje ryzyko naruszenia praw i wolności osób, których dane dotyczą. Nie było ono jednak wysokie.

Zgodnie z postanowieniami RODO, organ nadzoru powinien być informowany o naruszeniach, w przypadku których występuje ryzyko naruszenia praw i wolności podmiotów danych. Nie ma przy tym znaczenia czy ryzyko to jest niskie, średnie czy wysokie. W każdym z tych przypadków należy powiadomić o zdarzeniu Prezesa UODO. Wysokość ryzyka ma natomiast wpływ na zawiadomienie o naruszeniu podmiotów danych. Administrator ma obowiązek go dokonać przy ryzyku wysokim.

Prezes UODO wyraźnie daje do zrozumienia, że naruszenia ochrony danych należy traktować poważnie i nie można zapominać o ich negatywnych konsekwencjach dla osób, których dane dotyczą. Przypominamy, że na naszym blogu dostępne jest kompendium wiedzy o radzeniu sobie z naruszeniami ochrony danych osobowych.

Decyzja	Decyzja Prezesa UODO z dnia 13 lipca 2021 r. DKN.5131.22.2021
Ukarany podmiot	Prezes Sądu Rejonowego w Zgierzu
Kwota kary pieniężnej	10 000,00 PLN
Naruszone przepisy RODO	• art. 5 ust. 1 lit. f RODO – zasada integralności i poufności • art. 25 ust. 1 RODO – zasada *privacy by design* • art. 32 ust. 1 lit. b RODO – zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania • art. 32 ust. 1 lit. d RODO – regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania • art. 32 ust. 2 RODO – ocena stopnia bezpieczeństwa przy uwzględnieniu ryzyka wiążącego się z przetwarzaniem
Kontekst	Decyzja o nałożeniu kary związana była ze zgłoszeniem przez Prezesa Sądu Rejonowego w Zgierzu naruszenia ochrony danych osobowych polegającego na zagubieniu nieszyfrowanej przenośnej pamięci typu pendrive przez kuratora sądowego. Na nośniku przechowywano dane 400 osób, podlegających nadzorowi kuratorskiemu i objętych wywiadem środowiskowym. Zaginiony i zarazem niezabezpieczony nośnik pamięci nie został odnaleziony. W toku postępowania UODO, administrator wskazał, że wdrożył system ochrony danych osobowych w postaci zasad przetwarzania danych osobowych. Dokumentacja jest na bieżąco aktualizowana i audytowana przez powołanego do tego celu IOD. Ponadto administrator zapewnił, że podejmował działania w postaci szkoleń stacjonarnych oraz e-learningowych dotyczące ochrony danych osobowych oraz zapisów wdrożonej dokumentacji, dyżurów pełnionych przez IOD, dyżurów on-line oraz doraźnych kontroli prowadzonych przez IOD podczas dyżurów. Zgodnie z obowiązującymi u administratora dokumentami, obowiązek zabezpieczenia nośników spoczywa na użytkownikach. Zdaniem UODO takie podejście jest niewłaściwe. Postępowanie wykazało, że administrator naruszył m.in. zasadę poufności i integralności danych osobowych poprzez wydanie do użytku służbowego kuratorom sądowym niezabezpieczonego przenośnego nośnika pamięci oraz zobowiązanie ich do wdrożenia zabezpieczeń tej pamięci we własnym zakresie. Następstwem braku wprowadzenia odpowiednich środków organizacyjnych i technicznych, w przypadku zagubienia takiego nośnika przez kuratora sądowego, jest umożliwienie osobom nieuprawnionym dostępu do danych osobowych znajdujących się na nim.

	Organ wskazał, że to administrator danych, nie zaś pracownik lub osoba wykonująca zadania służbowe, jest zobowiązany do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z wymaganiami RODO. Ustalając wysokość administracyjnej kary pieniężnej, UODO uwzględnił jako okoliczność łagodzącą dobrą współpracę Prezesa Sądu z organem nadzorczym podjętą i prowadzoną w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków.

Komentarz eksperta

Małgorzata Guðfinnsson, ekspert ds. ochrony danych osobowych

To co zwraca uwagę w przedmiotowej decyzji Prezesa UODO to przede wszystkim zakres środków organizacyjnych wdrożonych przez ukaranego administratora. Prezes Sądu Rejonowego w Zgierzu zadbał o odpowiednią dokumentację ochrony danych osobowych, przeszkolił pracowników, zapewnił im stały kontakt z IOD, a dodatkowo poddawał się regularnym audytom. Gdzie zatem tkwił błąd, którego konsekwencją było naruszenie? Faktyczne zabezpieczenie nośników administrator pozostawił jego użytkownikom. Nie wskazał im żadnych przykładowych oraz adekwatnych zabezpieczeń, które pracownik może zastosować. Administrator założył, że posiadają oni stosowną wiedzę, jak, w sposób adekwatny, należy zabezpieczać nośniki z danymi osobowymi. Problem w tym, że taka wiedza powinna płynąć od niego. Wdrożenie odpowiednich środków technicznych i organizacyjnych nie jest obowiązkiem pracowników lecz administratora. Odpowiednich, czyli jakich? Na to pytanie odpowiadamy w jednym z artykułów na naszym blogu.

Decyzja	Decyzja Prezesa UODO z dnia 14 października 2021 r. DKN.5131.16.2021
Ukarany podmiot	Bank Millennium S.A.
Kwota kary pieniężnej	363 832,00 PLN
Naruszone przepisy RODO	• art. 33 ust. 1 RODO – zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu • art. 34 ust. 1 RODO – zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych
Kontekst	UODO o naruszeniu ochrony danych dowiedział się ze skargi, jaka wpłynęła na Bank Millennium S.A. Wynikało z niej, że doszło do zgubienia przez firmę kurierską korespondencji z danymi osobowymi, takimi jak: imię, nazwisko, PESEL, adres zameldowania, numery rachunków bankowych, numer identyfikacyjny nadawany klientom banku. Skarżący zostali o tym fakcie powiadomieni przez Bank, ale informacje na ten temat nie były wystarczające – nie spełniały wymagań określonych w RODO. W toku sprawy okazało się, że administrator danych nie wypełnił obowiązków, jakie na nim ciążą w związku z naruszeniem ochrony danych osobowych. Bank uznał, że ryzyko negatywnych konsekwencji dla osób dotkniętych naruszeniem jest średnie, dlatego nie zgłosił tego naruszenia organowi nadzorczemu oraz nie zrealizował w pełni obowiązku związanego z powiadomieniem osób, których dane dotyczą. UODO zwrócił uwagę, że gdyby w omawianej sprawie administrator powiadomił organ nadzorczy, to dostałby wówczas informację, że należy także powiadomić o naruszeniu osoby. Co ważne UODO wskazał, że z punktu widzenia przepisów o ochronie danych osobowych, biorąc pod uwagę możliwość szkodliwego wpływu na prawa lub wolności osób, nie jest istotne czy nieuprawniony odbiorca w istocie wszedł w posiadanie danych i się z nimi zapoznał, ale sam fakt, że wystąpiło takie ryzyko. Nie bez znaczenia jest także kwestia zakresu danych osobowych objętych naruszeniem, a więc nie tylko imienia i nazwiska, ale także numeru PESEL, który powinien podlegać ochronie. W omawianej decyzji organ nadzorczy nie tylko nałożył karę na administratora, ale nakazał również zawiadomienie osób poszkodowanych naruszeniem w sposób określony w art. 34 ust. 2 RODO. UODO decydując o nałożeniu kary wziął pod uwagę m.in. to, że w toku postępowania Bank w dalszym ciągu nie zrealizował obowiązków związanych z

	naruszeniem, jak i niezadowalający stopień współpracy z organem nadzoru, umyślność działania oraz charakter i wagę naruszenia.

Komentarz eksperta

Krystian Dobosz, starszy specjalista ds. ochrony danych osobowych

Mamy do czynienia z kolejną karą dotyczącą zgłaszania naruszeń, a właściwie braku aktywności administratora na tym polu. Sprawa dotyczy banku, który nie zgłosił naruszenia do Prezesa UODO i nie powiadomił osób, których dane dotyczą.

Każdy administrator jest zobligowany do zgłaszania incydentów, gdy tylko istnieje prawdopodobieństwo wystąpienia naruszenia praw i wolności (wyższe niż małe) osób, których dane dotyczą. Szeroki zakres danych (tj. imię, nazwisko, nr PESEL, adres zameldowania, numery rachunków bankowych, numer identyfikacyjny nadawany klientom banku (CIF)) spowodował wystąpienie wysokiego ryzyka, co wiąże się z obowiązkami notyfikacyjnymi wobec regulatora i tych osób.

Każdy administrator musi pamiętać, że argumenty mówiące o tym, że osoby nieuprawnione nie zapoznały się z danymi osobowymi, bądź też nie wykorzystały ich niezgodnie z przeznaczeniem, nie powoduje, że do naruszenia nie dochodzi (i nie trzeba go zgłaszać do organu nadzorczego) czy też powoduje, że nie występuje obowiązek powiadomienia osoby, której dane dotyczą.

Jeśli w toku czynności kontrolnych jesteśmy pytani o jakieś działania, których nie wykonaliśmy (np. powiadomienie osób, których dane dotyczą), należy wykonać je niezwłocznie, bo brak takiej aktywności, będzie wzięty pod uwagę przy wymiarze kary.

Kara ta ma mieć charakter przypominający każdemu administratorowi o obowiązku zgłaszania naruszeń, gdy tylko wystąpi ryzyko. Ponadto administratorzy muszą mieć na względzie traktowanie identyfikatora PESEL, jako szczególnie istotnego, który razem z innymi danymi (np. imieniem i nazwiskiem) spowoduje wystąpienie wysokiego ryzyka i będzie wymagał powiadomienia osób, których dane dotyczą, zgodnie z treścią art. 34 RODO. Pamiętajmy o tym, gdy przyjdzie analizować nam naruszenia w naszej organizacji.

O tym, jak radzić sobie z naruszeniami, w tym m.in. jak prawidłowo dokonywać ich analizy, kiedy i jak zgłaszać je organowi lub osobom fizycznym, pisaliśmy na naszym blogu w cyklu poświęconym incydentom ochrony danych osobowych

Decyzja	Decyzja Prezesa UODO z dnia 9 grudnia 2021 r. DKN.5130.2559.2020
Ukarany podmiot	Politechnika Warszawska
Kwota kary pieniężnej	45 000,00 PLN
Naruszone przepisy RODO	• art. 5 ust. 1 lit. f RODO – zasada integralności i poufności • art. 5 ust. 2 RODO – zasada rozliczalności • art. 24 ust. 1 RODO – obowiązek wdrażania odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO i wykazania podjętych działań w tym zakresie oraz w razie potrzeby poddawania tych środków przeglądom i uaktualnianiu • art. 25 ust. 1 RODO – zasada *privacy by design* • art. 32 ust. 1 RODO – wdrożenie odpowiednich środków technicznych i organizacyjnych • art. 32 ust. 2 RODO – ocena stopnia bezpieczeństwa przy uwzględnieniu ryzyka wiążącego się z przetwarzaniem
Kontekst	Postępowanie wobec Politechniki Warszawskiej wszczęto po tym jak do Urzędu Ochrony Danych Osobowych wpłynęło zgłoszenie naruszenia ochrony danych. Jak wskazano, nieuprawniona osoba dokonała pobrania z zasobów sieci informatycznej uczelni bazy danych, zawierającej dane osobowe studentów i wykładowców (ponad 5 tys. osób). Jednostka organizacyjna Politechniki wykorzystywała aplikację, która służyła do zapisywania się na przedmioty oraz pozwalała mieć wgląd w historię nauczania, ocen czy rozliczania opłat. Aplikacja ta była modyfikowana w zależności od potrzeb administratora. Na początku stycznia 2020 roku nieuprawniona osoba wykorzystała funkcjonalność umieszczania plików w aplikacji, dysponując danymi uwierzytelniającymi. Z kolei z początkiem maja 2020 roku dokonano nieautoryzowanego pobrania danych osobowych. W ocenie UODO, administrator nie przedstawił dowodów na spełnienie obowiązków wdrożenia odpowiednich środków technicznych i organizacyjnych, które zapewnią bezpieczeństwo przetwarzanych danych osobowych. Nie dokonywano formalnej oceny ryzyka, a zagrożenia identyfikowano poprzez zbieranie informacji od jednostek uczelni. Ponadto nie uzasadniono adekwatności stosowanych zabezpieczeń do ryzyka. Biorąc pod uwagę niedopełnienie obowiązków przez administratora oraz wysokie ryzyko wystąpienia negatywnych skutków w przyszłości dla osób objętych

	incydentem, organ nadzorczy uznał za zasadne i konieczne nałożenie administracyjnej kary pieniężnej w wysokości 45 tys. zł.

Komentarz eksperta

Małgorzata Guðfinnsson, ekspert ds. ochrony danych osobowych

W swojej decyzji nakładającej karę na Politechnikę Warszawską organ akcentuje przede wszystkim kwestię ryzyka. Zdaniem Prezesa UODO, administrator nie uwzględnił ryzyka związanego z przetwarzaniem danych osobowych co skutkowało brakiem odpowiednich środków technicznych i organizacyjnych mających zapewnić poufność informacji. To kolejna decyzja, w której organ zwraca uwagę na skuteczność wdrożonych środków ochrony danych osobowych. Pokazuje to, jak ważne jest właściwie zrozumienie oceny ryzyka, o której mowa w RODO.

O różnicach pomiędzy oceną ryzyka, a oceną skutków, DPIA, a PIA oraz o tym jak zabrać się za ich przeprowadzenie, tak aby zrobić to zgodnie z RODO i efektywnie, pisaliśmy w naszym mini poradniku poświęconym ocenie ryzyka przetwarzania danych osobowych.

Decyzja	Decyzja Prezesa UODO z dnia 1 grudnia 2021 r. DKE.561.16.2021
Ukarany podmiot	Pactum Poland Sp. z o.o.
Kwota kary pieniężnej	18 000,00 PLN
Naruszone przepisy RODO	• art. 31 RODO – obowiązek współpracy z organem nadzorczym w ramach wykonywania przez niego swoich zadań • art. 58 ust. 1 lit. e) RODO – uprawnienia organu nadzorczego w zakresie uzyskiwania od administratora dostępu do wszelkich danych osobowych i informacji
Kontekst	Urząd Ochrony Danych Osobowych, aby ustalić stan faktyczny sprawy zainicjowanej skargą, zwrócił się do Pactum Poland Sp. z o.o. o ustosunkowanie się do treści skargi oraz o udzielenie odpowiedzi na szczegółowe pytania dotyczące sprawy. Z czterech wysłanych Spółce wezwań, ta odebrała tylko jedno, na które jednak nie odpowiedziała. Odpowiedzialność za nieudzielenie na żądanie UODO informacji spoczywa na administratorze, czyli w tym przypadku Spółce. Zdaniem UODO nieudzielenie odpowiedzi na zawarte w odebranym przez Spółkę piśmie pytania, a także nieodbieranie pozostałych wezwań, wskazują na brak woli do współpracy w ustaleniu stanu faktycznego sprawy i prawidłowym jej rozstrzygnięciu. Zachowanie stanowi naruszenie obowiązku zapewnienia organowi nadzorczemu dostępu do informacji. Lekceważenie obowiązków związanych ze współpracą z UODO stanowi naruszenie o dużej wadze i jako takie podlega sankcjom finansowym. Dlatego też w tym przypadku, organ nadzorczy nałożył administracyjną karę pieniężną.

Komentarz eksperta

Krystian Dobosz, starszy specjalista ds. ochrony danych osobowych

Prezes Urzędu Ochrony Danych Osobowych nałożył karę na podmiot, który nie współpracował z organem w trakcie trwającego postępowania. Obowiązkiem Spółki jest zapewnienie takiej organizacji odbioru pism, aby obieg korespondencji odbywał się w sposób ciągły i niezakłócony, przez osoby uprawnione. Spółka unikała jednak odbioru pism i kontaktu z regulatorem.

Jest to kolejny dowód na to, że nie warto prezentować takiej postawy, ponieważ brak ustosunkowania się do kierowanych do Spółki pism, powoduje zarzut określony w art. 58 ust. 1 RODO – nie wypełnienie obowiązku zapewnienia organowi nadzorczemu dostępu do informacji, niezbędnych do realizacji jego zadań.

To już kolejna kara za brak współpracy. Można także zauważyć, że Prezes Urzędu Ochrony Danych Osobowych w takich przypadkach nakłada kary, które wynoszą 18000-20000 zł. Świadczy to o wytworzeniu się pewnej „praktyki" w tym zakresie.

Pamiętajmy jednak, że dużo lepszym rozwiązaniem jest współpraca z organem, pozwoli to rozwiać wątpliwości organu w danej sprawie, a przede wszystkim być może uniknąć kary finansowej.

Gdybyście chcieli dowiedzieć jak przygotować się do kontroli UODO – zapoznajcie się z tym artykułem.

Decyzja	Decyzja Prezesa UODO z dnia 19 stycznia 2022 r. DKN.5131.33.2021
Ukarany podmiot	Santander Bank Polska S.A.
Kwota kary pieniężnej	545 748,00 PLN
Naruszone przepisy RODO	• art. 34 ust. 1 RODO – zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych
Kontekst	Santander Bank Polska S. A. zgłosił do UODO naruszenie ochrony danych osobowych po tym, gdy stwierdził, że były pracownik Banku mimo zakończenia pracy, posiada nieuprawniony dostęp do profilu płatnika na Platformie Usług Elektronicznych ZUS (PUE ZUS). W wyniku tego mógł on przeglądać znajdujące się na profilu płatnika dane pracowników. W toku postępowania ustalono, że pracownik po zakończeniu pracy korzystał z przysługujących mu uprawień i pięciokrotnie logował się do platformy. Po dokonaniu analizy zgłoszenia naruszenia, UODO uznało, że doszło do naruszenia poufności danych, które wiąże się jednocześnie z zaistnieniem wysokiego ryzyka dla naruszenia praw lub wolności osób, których dane dotyczą. Z tego też względu zdaniem organu nadzorczego konieczne jest zawiadomienie osób, których dane dotyczą, o zaistniałym incydencie. W ocenie Banku nie zidentyfikowano nielegalnego przetwarzania danych i uznano, że nie doszło do naruszenia ochrony danych osobowych w rozumieniu RODO. Jak wyjaśnił administrator pierwotnie zgłoszenia naruszenia ochrony danych osobowych dokonał jedynie ze względów ostrożności. Po analizie sprawy uznał on, że incydent nie wiąże się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych. Bank umieścił jednak na platformie komunikacji wewnętrznej komunikat przypominający zasady przetwarzania danych osobowych. W ocenie UODO tego typu komunikat był zbyt ogólny, nie odnosił się do konkretnego przypadku, a jedynie zaprezentowano w nim przykładowe rodzaje naruszeń. UODO wyraził także swoje zastrzeżenia co do wyboru adresatów komunikatu, do których został on skierowany, czyli jedynie do obecnych pracowników Banku, korzystających z platformy komunikacji wewnętrznej. W ocenie UODO w prezentowanej sprawie zaszły wszelkie okoliczności, które potwierdzały konieczność zawiadomienia o naruszeniu osób, których dane dotyczą. Dostęp do danych o tak szerokim zakresie stwarza ryzyko dla praw lub wolności osób, których dane dotyczą. Dane przetwarzane na platformie PUE ZUS mogą zostać wykorzystane przez nieuprawnione osoby m.in.: do uzyskania dostępu do korzystania ze świadczeń opieki zdrowotnej i wglądu do danych o stanie zdrowia,

	czy uzyskania przez osoby trzecie danych umożliwiających zaciągnięcie pożyczek w instytucjach pozabankowych. Prezes UODO podjął decyzję nie tylko o nałożeniu administracyjnej kary pieniężnej w wysokości ponad 545 tys. zł, ale także nakazał spełnienie obowiązku wynikającego z RODO jakim jest zawiadomienie osób o zaistniałym incydencie.

Komentarz eksperta

Tomasz Wasilczyk, starszy specjalista ds. ochrony danych osobowych

To kolejna decyzja Prezesa UODO nakładająca administracyjną karę pieniężną za niewłaściwe postępowanie administratora w przypadku wystąpienia naruszenia ochrony danych osobowych. W tym przypadku chodziło o naruszenie przepisu art. 34 ust. 1 RODO polegającego na niezawiadomieniu o naruszeniu ochrony danych osobowych, bez zbędnej zwłoki osób, których dane dotyczą. Raz jeszcze należy zatem podkreślić, jak ważna jest rzetelna ocena ryzyka zaistniałego naruszenia, która powinna uwzględniać wszelkie okoliczności. Bank uznał bowiem, że nieuprawniony dostęp do konta PUE ZUS przez byłego pracownika nie wiąże się z wysokim ryzykiem naruszenia praw i wolności osób, których dane dotyczą. W tym przypadku możliwy dostęp do danych osobowych dotyczył ok. 10 500 pracowników Banku, a swoim zakresem obejmował w szczególności takie dane jak numer PESEL oraz zwolnienia lekarskie tj. dane dotyczące zdrowia. Już sam zakres danych objęty naruszeniem może wskazywać na wysokie ryzyko naruszenia praw lub wolności osób fizycznych, co potwierdza stanowisko Prezesa UODO prezentowane w uzasadnieniu do wcześniejszych decyzji nakładających administracyjne kary pieniężne czy też w publikowanych materiałach.

W kontekście tej sprawy warto zwrócić uwagę na stanowisko organu nadzorczego do kwestii zaufania do nieuprawnionego odbiorcy – byłego pracownika. W ocenie Prezesa UODO byłego pracownika nie należało utożsamiać z odbiorcą zaufanym. W związku z powyższym Bank powinien zachować się w sposób bardziej ostrożny, ponieważ nie można uznać ponad wszelką wątpliwość, iż były pracownik zachowa się w odpowiedni sposób.

Prezes UODO w swojej decyzji powtórzył również wcześniej wyrażane stanowisko, iż dla powstania obowiązku zawiadomienia o naruszeniu ochrony danych osobowych osób, których dane dotyczą, nie jest konieczne zmaterializowanie się negatywnych konsekwencji naruszenia, wystarczająca jest w tym zakresie sama możliwość (ryzyko) wystąpienia takich konsekwencji, które według organu nadzorczego było wysokie.

Istotny jest jeszcze jeden aspekt tej sprawy. Bank powinien zastosować takie środki, które zapewniają monitorowanie zakresu nadanych uprawnień do systemów informatycznych, w szczególności w przypadku zakończenia stosunku pracy z danym pracownikiem. Z treści uzasadnienia do decyzji wynika, że były pracownik miał dostęp do platformy PUE ZUS przez 8 miesięcy, w tym czasie kilkukrotnie logował się do tej platformy, zyskując dostęp do danych osobowych pracowników Banku, a następnie sam zgłosił byłemu pracodawcy, iż posiada nieuprawniony dostęp do wspomnianej platformy. Co więcej, Bank nie odebrał uprawnień dostępu

do platformy PUE ZUS również dwóm innym byłym pracownikom Banku, co zdaniem organu nadzorczego potwierdza nieskuteczność zastosowanych środków.

Decyzja	Decyzja Prezesa UODO z dnia 19 stycznia 2022 r. DKN.5130.2215.2020
Ukarany podmiot	Fortum Marketing and Sales Polska S.A. oraz PIKA Sp. z o.o.
Kwota kary pieniężnej	Fortum Marketing and Sales Polska S.A. – 4 911 732,00 PLN PIKA Sp. z o.o. – 250 135,00 PLN
Naruszone przepisy RODO	Fortum Marketing and Sales Polska S.A. • art. 5 ust. 1 lit. f RODO – zasada integralności i poufności • art. 24 ust. 1 – obowiązek wdrażania odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO i wykazania podjętych działań w tym zakresie oraz w razie potrzeby poddawania tych środków przeglądom i uaktualnianiu • art. 25 ust. 1 – – zasada *privacy by design* • art. 28 ust. 1 – korzystanie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych • art. 32 ust. 1 RODO – wdrożenie odpowiednich środków technicznych i organizacyjnych • art. 32 ust. 2 RODO – ocena stopnia bezpieczeństwa przy uwzględnieniu ryzyka wiążącego się z przetwarzaniem PIKA S.A. • art. 32 ust. 1 RODO – wdrożenie odpowiednich środków technicznych i organizacyjnych • art. 32 ust. 2 RODO – ocena stopnia bezpieczeństwa przy uwzględnieniu ryzyka wiążącego się z przetwarzaniem • art. 28 ust. 3 lit. c) i f) – umowa stanowi w szczególności, że podmiot przetwarzający podejmuje wszelkie środki wymagane na mocy art. 32 RODO oraz uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO
Kontekst	Po przeanalizowaniu zgłoszenia naruszenia danych osobowych od Fortum Marketing and Sales Polska S.A., organ nadzorczy wszczął z urzędu postępowanie administracyjne w sprawie naruszenia przepisów o ochronie danych osobowych przez Spółkę.

	Naruszenie ochrony danych polegało na skopiowaniu danych klientów administratora przez nieuprawnione osoby. Doszło do tego w momencie wprowadzania zmiany w środowisku teleinformatycznym. Zmiany tej dokonał podmiot przetwarzający, z którym administrator współpracuje na podstawie zawartych umów, w tym umowy powierzenia przetwarzania danych osobowych. W trakcie dokonywanych zmian utworzona została dodatkowa baza danych klientów Fortum. Baza ta została jednak skopiowana przez nieuprawnione osoby, gdyż serwer, na którym została ona wdrożona, nie miał odpowiednio skonfigurowanych zabezpieczeń. Administrator dowiedział się o incydencie nie od podmiotu przetwarzającego, a od dwóch niezależnych internautów, którzy powiadomili go, że mają nieuprawniony dostęp do bazy. W toku przeprowadzonego postępowania Urząd ustalił, że spółka w postanowieniach umownych z podmiotem przetwarzającym określiła wymogi w zakresie bezpieczeństwa danych osobowych, które należy zastosować, m.in. pseudonimizację i szyfrowanie danych osobowych. W trakcie procesu dokonywania zmian w systemie zostały użyte rzeczywiste dane osobowe klientów administratora, a skuteczność zastosowanych zabezpieczeń nie została zweryfikowana przed przekazaniem do Fortum nowego rozwiązania. Ponadto funkcje bezpieczeństwa nie były testowane w trakcie prowadzonych w tym celu prac. Podmiot przetwarzający działał niezgodnie z powszechnie znanymi normami ISO, a jednocześnie wbrew postanowieniom własnej „Polityki bezpieczeństwa”, która do tych norm się odwołuje. Nie stosował się również do postanowień umowy powierzenia przetwarzania danych osobowych. Zaistniałe naruszenie wynikało z niezastosowania przez podmiot przetwarzający podstawowych zasad bezpieczeństwa polegających na niezabezpieczeniu danych osobowych przed dostępem osób nieuprawnionych. Zatem ponosi on bezpośrednią odpowiedzialność za naruszenie ochrony danych osobowych klientów administratora, a tak rażące zaniedbanie w procesie przetwarzania danych osobowych. Administrator pomimo wdrożonych procedur oraz posiadanej wiedzy, jak zgodnie z powszechnie stosowanymi praktykami powinno przebiegać wprowadzanie zmian w systemach informatycznych, na żadnym etapie wdrożenia nie prowadził nadzoru nad tym, czy wdrożenie faktycznie przebiega zgodnie z powszechnie obowiązującymi standardami. Na administratorze spoczywa także obowiązek regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. Gdyby administrator dokonał weryfikacji sposobu realizacji przez podmiot przetwarzający zmian mających na celu usprawnienie działania systemu przetwarzającego dane osobowe, gdyby wymagał przedstawienia

	planu prac i dalsze ich wdrożenie zgodnie z przyjętą przez Fortum procedurą, znacząco obniżyłby ryzyko uzyskania dostępu przez osoby nieuprawnione do danych przetwarzanych w tym systemie.

Komentarz eksperta

Małgorzata Guðfinnsson, ekspert ds. ochrony danych osobowych

Jedna decyzja, dwa ukarane podmioty, z czego jednemu z nich przyszło zmierzyć się z rekordową karą za naruszenie przepisów RODO. Wszystko rozpoczęło się od naruszenia ochrony danych osobowych, do którego doszło podczas wdrażania nowego narzędzia informatycznego. Bez wątpienia zawinił tu podmiot przetwarzający, niewłaściwie zabezpieczając serwer, na którym znalazły się dane osobowe. W związku z działaniem niezgodnie z powszechnie znanymi normami ISO ukarany został przez Prezesa UODO karą finansową.

Dużo wyższa sankcja nałożona została jednak na administratora, jako podmiot, który powinien dokonywać weryfikacji sposobu realizacji dokonywanych przez procesora zmian w systemie. Gdyby tylko administrator rzeczywiście kontrolował działania podmiotu przetwarzającego, gdyby wymagał od niego przedstawienia planu prac i dalszego ich wdrażania zgodnie z przyjętą procedurą, ryzyko uzyskania dostępu do danych przez osoby nieuprawnione zostałoby znacznie zminimalizowane.

Decyzja ta pokazuje, jak ważne jest kontrolowanie procesorów, nawet jeżeli są to podmioty będące specjalistami w swojej branży. RODO audyt procesora – jak to zrobić z głową?