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: 16.04.2020

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 PLN
Naruszone przepisy RODO	• 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	• 5 ust. 1 lit. f RODO – zasada integralności i poufności • 32 ust. 1 lit. b RODO – zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług 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	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 PLN
Naruszone przepisy RODO	• 5 ust. 1 lit. a RODO – zasada zgodności z prawem, rzetelności i przejrzystości • 5 ust. 1 lit. f RODO – zasada integralności i poufności • 5 ust. 2 RODO – zasada rozliczalności • 6 ust. 1 RODO – podstawy prawne przetwarzania danych osobowych • 7 ust. 1 RODO – obowiązek wykazania, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych • 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 • 25 ust. 1 RODO – zasada *privacy by design* • 32 ust. 1 lit. b RODO – zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania • 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	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 PLN
Naruszone przepisy RODO	• 5 ust. 1 lit. a RODO – zasada zgodności z prawem, rzetelności i przejrzystości • 5 ust. 1 lit. f RODO – zasada integralności i poufności • 5 ust. 1 lit. e RODO – zasada ograniczenia przechowywania danych • 5 ust. 2 RODO – zasada rozliczalności • 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 • 28 ust. 3 RODO – obowiązek zawarcia umowy powierzenia danych osobowych w przypadku udostępnia danych podmiotom przetwarzającym • 30 ust. 1 lit. d oraz f - obowiązek wskazania w rejestrze czynności przetwarzania odbiorców danych oraz terminów usunięcia danych • 32 ust. 1 lit. b RODO – zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania • 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. 1 – 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 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 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?