NAKŁADANIE ADMINISTRACYJNYCH KAR PIENIĘŻNYCH W ROZPORZĄDZENIU O OCHRONIE DANYCH OSOBOWYCH

Aspekty praktyczne

Magdalena Abu Gholeh
Dominika Kuźnicka-Błaszkowska

Wolters Kluwer

NAKŁADANIE ADMINISTRACYJNYCH KAR PIENIĘŻNYCH W ROZPORZĄDZENIU O OCHRONIE DANYCH OSOBOWYCH

Aspekty praktyczne

Magdalena Abu Gholeh
Dominika Kuźnicka-Błaszkowska

Wolters Kluwer

WARSZAWA 2020

SERIA **MONOGRAFIE**

Stan prawny na 16 grudnia 2020 r.

Wydanie publikacji zostało dofinansowane przez
Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego

Recenzent
Dr hab. Agnieszka Grzelak, prof. ALK

Wydawca
Dagna Kordyasz

Redaktor prowadzący
Paulina Ambroży

Opracowanie redakcyjne
Katarzyna Świerk-Bożek

Projekt okładek serii
Wojtek Kwiecień-Janikowski, Przemek Dębowski

ISBN 978-83-8223-352-0 *ISBN PDF-a: 978-83-8223-817-4*
ISSN 1897-4392

Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 22 535 82 19
e-mail: ksiazki@wolterskluwer.pl

księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

WYKAZ SKRÓTÓW

Akty prawne

dyrektywa 95/46/WE	–	dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. UE L 281, s. 31, ze zm.) – uchylona
k.p.	–	ustawa z 26.06.1974 r. – Kodeks pracy (Dz.U. z 2020 r. poz. 1320 ze zm.)
KPP	–	Karta praw podstawowych Unii Europejskiej (Dz. Urz. UE C 202 z 2016 r., s. 389)
RODO	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1, ze sprost.)
TFUE	–	Traktat o funkcjonowaniu Unii Europejskiej (Dz. Urz. UE C 202 z 2016 r., s. 47)
u.o.d.o.	–	ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781)

Inne

NSA	–	Naczelny Sąd Administracyjny
TSUE/TS	–	Trybunał Sprawiedliwości Unii Europejskiej (do 1.12.2009 r. jako Trybunał Sprawiedliwości)
UODO	–	Urząd Ochrony Danych Osobowych
WSA	–	wojewódzki sąd administracyjny

WSTĘP

Efektywność każdej regulacji, niezależnie od zakresu jej stosowania, zależy w wielu aspektach od skuteczności działania organów stojących na straży przestrzegania jej przepisów. W przypadku rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) zapewnienie efektywności stosowania regulacji jest szczególnie utrudnione z uwagi na rozproszony system organów nadzorczych oraz fakt, że każde z państw członkowskich charakteryzuje się swoistymi odmiennościami w interpretacji przepisów unijnych. Dość krótki okres obowiązywania RODO oraz niejednolitość rozstrzygnięć wydawanych przez organy nadzorcze sprzyja powstawaniu wielu wątpliwości interpretacyjnych oraz niepewności administratorów danych w odniesieniu do treści obowiązków nałożonych na nich przez prawodawcę.

Autorki niniejszej monografii podjęły próbę zbadania, w jaki sposób naruszenie poszczególnych obowiązków wynikających z RODO przekłada się na charakter i zakres nałożonej administracyjnej kary pieniężnej. Zanim jednak do tego dojdzie, konieczne jest przeanalizowanie modelu odpowiedzialności przyjętego przez RODO, jak również genezy i celu przyjętych w rozporządzeniu administracyjnych kar pieniężnych. Trudno bowiem podjąć próbę wydawania praktycznych rekomendacji co do realizacji poszczególnych obowiązków wynikających z omawianego aktu prawnego bez dokładnego wskazania, kto, kiedy i w jakim zakresie podlega odpowiedzialności, narażając się na kary finansowe. Koniecz-

ne jest również określenie zakresu obowiązków, jakie spoczywają na organie nadzorczym, jego pozycji względem innych organów państw członkowskich oraz gwarancji jego niezależności.

Biorąc pod uwagę katalog przedmiotowy możliwych naruszeń oraz najczęstsze błędy popełnianie przez administratorów, autorki zdecydowały się poddać analizie następujące obowiązki nałożone przez RODO: przestrzeganie zasad ogólnych przetwarzania danych; przetwarzanie danych osobowych w oparciu o co najmniej jedną z przesłanek wynikających z RODO; realizacja praw osób, których dane dotyczą; realizacja obowiązku informacyjnego; przetwarzanie danych osobowych z zapewnieniem odpowiednich zabezpieczeń technicznych i organizacyjnych; współpraca z organem nadzorczym oraz obowiązki wynikające z konieczności powołania inspektora ochrony danych. Każdy z rozdziałów rozpoczyna się częścią teoretyczną, gdzie w sposób zwięzły i praktyczny opisane są poszczególne elementy obowiązków nałożonych na administratorów danych i/lub podmioty przetwarzające. Następnie analizie poddano wymierzone przez poszczególne organy nadzorcze kary administracyjne, które autorki uznały za szczególnie istotne dla dalszej praktyki interpretacyjnej. Zwieńczeniem rozważań poczynionych w każdym z rozdziałów jest próba zbudowania wniosków i rekomendacji co do dalszej interpretacji poszczególnych obowiązków wynikających z RODO, biorąc pod uwagę dotychczas nałożone administracyjne kary pieniężne.

Prezentowana monografia przez analizę dotychczas nałożonych administracyjnych kar pieniężnych przez organy nadzorcze ma za zadanie znalezienie rozwiązania na najczęściej pojawiające się problemy praktyczne. Analizując poszczególne rozstrzygnięcia, przede wszystkim pod kątem przedmiotowym, autorki w sposób szczegółowy wskażą, kiedy i w jakim zakresie może dojść do naruszenia poszczególnych obowiązków nałożonych na administratorów danych osobowych oraz podmioty przetwarzające, a co bardziej istotne – jakie potencjalne ryzyko finansowe niesie ze sobą niedopełnienie poszczególnych obowiązków. Wnioski prezentowane po zakończeniu każdego z rozdziałów pozwolą na oszacowanie ryzyka i podjęcie świadomej decyzji co do zakresu i charakteru czynności przetwarzania.

Autorki mają nadzieję, że przedstawione przykłady rozwieją wątpliwości związane ze stosowaniem postanowień RODO oraz będą stanowić przydatne źródło wiedzy dla praktyków i teoretyków prawa. Celem opracowania jest zapełnienie luki w literaturze dotyczącej ochrony danych osobowych oraz przedstawienie szerszemu gronu czytelników najważniejszych decyzji wydanych przez organy nadzorcze poszczególnych państw członkowskich w zakresie stosowania przepisów RODO.

Powstanie publikacji nie byłoby możliwe bez wsparcia Profesora dr. hab. Mariusza Jabłońskiego, który był inicjatorem i jej pomysłodawcą, a także w toku prac oferował pomoc zarówno merytoryczną, jak i organizacyjną. Ostateczny kształt, jaki niniejsza książka przybrała, jest efektem wielu żywiołowych dyskusji, których istotną postacią był Profesor Jabłoński, za co autorki w tym miejscu chcą mu podziękować.

Magdalena Abu Gholeh
Dominika Kuźnicka-Błaszkowska

Rozdział I

ODPOWIEDZIALNOŚĆ PODMIOTÓW PRZETWARZAJĄCYCH DANE OSOBOWE NA GRUNCIE RODO

1. Model odpowiedzialności przyjęty w RODO

Ogólne rozporządzenie o ochronie danych nałożyło na administratorów danych oraz podmioty przetwarzające dane wiele obowiązków. Część z nich występowała już na gruncie wcześniej obowiązującej dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych oraz ustaw krajowych. Nie ulega jednak wątpliwości, że wiele z nich stanowi istotne *novum* dla podmiotów zaangażowanych w procesy przetwarzania danych. Co niezwykle istotne, RODO wprowadziło również zmiany w zakresie odpowiedzialności za naruszenie obowiązków ochrony danych osobowych. Unijne rozporządzenie przewiduje możliwość poniesienia przez administratorów i podmioty przetwarzające odpowiedzialności administracyjnej oraz cywilnoprawnej. Dodatkowo przyznaje ono państwom członkowskim możliwość wprowadzenia innych sankcji. W praktyce przekłada się to na wprowadzenie odpowiedzialności karnej przez krajowych ustawodawców.

Prawodawca unijny wprowadził definicję legalną naruszenia ochrony danych osobowych. Zgodnie z art. 4 pkt 12 RODO należy przez nie

rozumieć naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Rozporządzenie nakłada na administratora obowiązek zgłoszenia naruszenia krajowemu organowi nadzorczemu. Przepisy przewidują jednak wyjątek od tego obowiązku w sytuacji, gdy jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. W przypadku naruszenia powstałego po stronie podmiotu przetwarzającego ma on obowiązek zgłoszenia go administratorowi (art. 33 RODO).

Zgodnie z zasadą rozliczalności, wprowadzoną w art. 5 ust. 2 RODO, administrator jest odpowiedzialny za przestrzeganie zasad ogólnych przetwarzania danych osobowych. Musi on być również w stanie wykazać ich przestrzeganie. Przepis ten stanowi pierwszy przejaw tzw. podejścia opartego na ryzyku, który bardziej szczegółowo omówiony jest w dalszych rozdziałach. Należy jednak wskazać, że praktyczny aspekt zasady rozliczalności wyraża się przede wszystkim w art. 24 RODO, który nakłada na administratora obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia zgodnego z prawem przetwarzania danych[1]. Warto jednak pamiętać, iż w przypadku powierzenia przetwarzania danych innemu podmiotowych reguła ta ulegnie zmianie, a część obowiązków będzie spoczywać na podmiocie przetwarzającym.

Przepisy RODO wprowadzają również koncepcję współadministrowania. Zgodnie z art. 26 RODO ze współadministrowaniem mamy do czynienia w sytuacji, gdy co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania danych. W przypadku zaistnienia takiej sytuacji współadministratorzy zobligowani są do dokonania uzgodnień w zakresie odpowiedzialności dotyczącej wypełnienia obowiązków wynikających z RODO. Warto jednak podkreślić, że prawodawca nie wprowadza żadnych szczegółowych wymogów w zakresie tych ustaleń.

[1] A. Nerka [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Legalis 2018, art. 5.

Należy więc przyjąć, iż administratorom przysługuje w tym zakresie pewna swoboda. Uzgodnienia powinny jednak w jasny sposób konkretyzować, na którym z administratorów ciąży obowiązek realizacji poszczególnych obowiązków, a tym samym odpowiedzialność za ich spełnienie[2].

Jak zasygnalizowano wyżej, administratorzy nie zawsze dokonują samodzielnie wszystkich operacji przetwarzania. Większość z nich zakłada udział podmiotu przetwarzającego, który dokonuje przetwarzania danych w imieniu administratora. Zgodnie z treścią art. 28 RODO administrator ma obowiązek korzystania wyłącznie z usług podmiotów, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych w celu spełnienia wymogów ogólnego rozporządzenia. Powierzenie przetwarzania danych innemu podmiotowi nie wpływa na zakres praw i obowiązków administratora. Wciąż decyduje on o celach i sposobach przetwarzania danych. Co istotne, administrator w dalszym ciągu ponosi odpowiedzialność za realizację ciążących na nim obowiązków, które wynikają z przepisów RODO[3]. Możliwa jest jednak sytuacja, w której podmiot przetwarzający zacznie podejmować decyzje o celach i sposobach przetwarzania danych. Jak wiadomo, czynności te zastrzeżone są wyłącznie dla administratora, tym samym podjęcie ich przez podmiot przetwarzający nakazuje uznać go za administratora w odniesieniu do danej operacji przetwarzania[4]. Wpłynie to w sposób oczywisty na zakres jego odpowiedzialności[5].

---

[2] P. Fajgielski [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, red. P. Fajgielski, LEX 2018, art. 26.

[3] Szerzej na temat powierzenia danych A. Pyka, *Powierzenie przetwarzania danych osobowych w świetle ogólnego rozporządzenia o ochronie danych*, „Prawo Mediów Elektronicznych" 2020/1, s. 10 oraz K. Cieniak, *Powierzanie przetwarzania danych osobowych*, „Monitor Prawniczy" 2019/9, s. 505.

[4] P. Fajgielski [w:] *Ogólne...*, red. P. Fajgielski, LEX 2018, art. 26.

[5] Wkroczenie przez podmiot przetwarzający w zakres uprawnień przysługujących administratorowi (tj. określanie celów i sposobów przetwarzania danych) nakazuje uznać go za administratora danych. Dotyczy to jednak wyłącznie tej operacji przetwarzania, wobec której podmiot podjął takie działania. Uznanie podmiotu przetwarzającego za administratora oznacza, że będzie on ponosił pełną odpowiedzialność, jaką ogólne rozporządzenie przewiduje dla administratora. Rozwiązanie to pozostaje bez uszczerbku dla art. 82, 83 i 84 RODO. Tym samym przetwarzający będzie odpowiadał niezależnie

W odniesieniu do czynności podejmowanych przez podmioty przetwarzające należy pamiętać również o możliwości korzystania przez nie z usług innych podmiotów przetwarzających. Mamy wtedy do czynienia z tzw. podpowierzeniem. Skorzystanie z takiego rozwiązania wymaga uzyskania przez podmiot przetwarzający uprzedniej pisemnej zgody administratora. Administrator ma możliwość udzielenia zgody ogólnej (która wymaga informowania administratora o wszelkich zamierzonych zmianach dotyczących kolejnych podmiotów przetwarzających) lub szczegółowej. W kontekście odpowiedzialności trzeba podkreślić, że w przypadku niewywiązania się podprocesora z obowiązku ochrony danych, pełną odpowiedzialność wobec administratora poniesie pierwotny podmiot przetwarzający. Wprowadzenie takiego rozwiązania ma skłaniać podmioty przetwarzające do rozsądnego i przemyślanego doboru kontrahentów.

Jak wspomniano we wstępie, RODO przewiduje modele odpowiedzialności administracyjnej i cywilnej za naruszenie przepisów ochrony danych. W ramach pierwszego z nich prawodawca wprowadził możliwość nałożenia administracyjnej kary pieniężnej. Zgodnie z treścią art. 83 RODO może być ona nałożona zarówno na administratora, jak i podmiot przetwarzający. W wyjątkowych sytuacjach istnieje możliwość nałożenia administracyjnej kary pieniężnej również na podmioty monitorujące oraz certyfikujące. Szczegółowego omówienia tej sankcji dokonano w pkt 2.

Artykuł 82 RODO wprowadza zasady odpowiedzialności odszkodowawczej administratora oraz podmiotów przetwarzających wobec osoby, która poniosła szkodę w wyniku naruszenia ochrony danych osobowych. Jak wskazuje się w literaturze przedmiotu, przepis ten sanowi samodzielną postawę roszczeń odszkodowawczych[6]. Motyw 146 preambuły RODO nakazuje interpretować pojęcie szkody szeroko,

od odpowiedzialności administratora w zakresie wskazanym w tych przepisach. Za: M. Sakowska-Baryła [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Legalis 2018, art. 28.

[6] N. Zawadzka [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, art. 82, s. 1049.

zgodnie z orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej. Interpretacja ta powinna w pełni odzwierciedlać cele RODO. W treści wspomnianego przepisu prawodawca doprecyzowuje, że odszkodowanie przysługuje jednostce w wyniku poniesienia zarówno szkody majątkowej, jak i niemajątkowej. Prawodawca w sposób jasny określa zakres odpowiedzialności administratorów oraz podmiotów przetwarzających. Ci pierwsi odpowiadają za szkody spowodowane przetwarzaniem, które narusza przepisy RODO. Natomiast podmiot przetwarzający odpowiada za szkody wyłącznie wtedy, gdy nie dopełnił obowiązków bezpośrednio nałożonych przez rozporządzenie lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom. Należy jednak pamiętać, że zgodnie z motywem 146 preambuły RODO za przetwarzanie dokonywane w sposób naruszający ogólne rozporządzenie rozumie się również przetwarzanie, które narusza akty delegowane i wykonawcze przyjęte na mocy RODO oraz prawo państwa członkowskiego doprecyzowujące ogólne rozporządzenie.

Przesłanki odpowiedzialności odszkodowawczej z art. 82 RODO obejmują poniesienie szkody przez podmiot danych, naruszenie przez administratora lub podmiot przetwarzający przepisów ogólnego rozporządzenia, zaistnienie związku przyczynowego między szkodą a naruszeniem oraz wystąpienie winy w naruszeniu RODO. Warto zaznaczyć, że w sytuacji gdy w przetwarzaniu danych uczestniczy więcej podmiotów, odpowiadają one solidarnie za wyrządzoną krzywdę. Sytuacja ta może dotyczyć między innymi współadministrowania oraz powierzenia czynności przetwarzania podmiotowi lub podmiotom przetwarzającym[7].

W sytuacji gdy administrator lub podmiot przetwarzający udowodni, że w żadnym stopniu nie ponosi winy za sytuację, która doprowadziła do powstania szkody, zostaje on zwolniony z odpowiedzialności.

Zgodnie z treścią art. 82 ust. 6 RODO jurysdykcję sądową ustala się na podstawie art. 79 ust. 2 RODO. Tym samym postępowanie przeciwko

[7] P. Litwiński, P. Barta, M. Kawecki [w:] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, Warszawa 2017, art. 82, s. 823–824.

administratorowi lub podmiotowi przetwarzającemu wszczyna się przed sądem państwa członkowskiego, w którym administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną. Ewentualne postępowanie można wszcząć również przed sądem państwa członkowskiego, w którym podmiot danych ma miejsce zwykłego pobytu (chyba że administrator lub podmiot przetwarzający są organami publicznymi wykonującymi swoje uprawnienia publiczne). W przypadku Polski sądem właściwym w sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych jest sąd okręgowy (art. 93 u.o.d.o.). Warto wspomnieć, że na gruncie ustawy z 10.05.2018 r. o ochronie danych osobowych sąd w postępowaniu o naprawienie szkody wyrządzonej przez naruszenie przepisów o ochronie danych osobowych związany jest decyzją organu nadzorczego (art. 97). Ustawodawca zadecydował o zastosowaniu takiego rozwiązania przyjmując, że to Prezes UODO posiada specjalistyczną wiedzę z zakresu ochrony danych osobowych. Tym samym nie ma konieczności samodzielnego badania naruszenia przepisów przez sąd. Możliwe jest jednak zaistnienie okoliczności, w których to sąd będzie zobligowany do przeprowadzenia oceny naruszenia ochrony danych osobowych. Dotyczy to między innymi sytuacji, w których sprawa zostaje wniesiona do sądu przy braku wcześniejszej decyzji organu nadzorczego[8].

Zadania te mogą być podejmowane we współpracy z organami nadzorczymi innych państw członkowskich, szczególnie w przypadku transgranicznego przetwarzania danych osobowych. W takich sytuacjach, jeśli zostaną spełnione odpowiednie warunki, tylko jeden z organów będzie prowadził postępowanie. Wskazuje się jednak, że każdy z nich powinien posiadać odpowiednie kompetencje i narzędzia do jego przejęcia[9]. Jest to *novum*, biorąc pod uwagę przepisy dyrektywy 95/46/WE, gdzie co do zasady w przypadku transgranicznego przetwarzania danych osobowych administrator danych i podmiot przetwarzający musieli zapewnić zgodność przetwarzania z wewnętrznymi przepisami każdego

[8] M. Abu Gholeh, *Pozycja ustrojowa organu nadzorczego ochrony danych osobowych na przykładzie Polski*, „Przegląd Prawa Konstytucyjnego" 2019/4, s. 179.

[9] E. Szabo, *About Specific Issues of the GDPR of the European Union*, „Hungarian Yearbook of International Law and European Law" 2017, s. 366.

z państw, na terytorium którego dochodziło do przetwarzania, a każdy z organów nadzorczych mógł prowadzić własne postępowanie. Zasada *one-stop-shop*, ustanowiona na gruncie RODO, ma zapewnić jednolitość w stosowaniu przepisów unijnych[10], przyspieszyć postępowanie, a przede wszystkim nakłonić przedsiębiorców do przetwarzania transgranicznego wewnątrz Unii Europejskiej w celu wzmocnienia jednolitego rynku wewnętrznego. Zasada ta nie będzie miała zastosowania w przypadku transgranicznego przetwarzania danych osobowych przez organ publiczny bądź podmiot prywatny podejmujący przetwarzanie w celu wypełnienia obowiązku prawnego nałożonego na administratora przez przepisy wewnętrzne państwa członkowskiego bądź gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Organ nadzorczy pozostaje właściwy również do rozpatrzenia skargi, którą do niego wniesiono lub zajęcia się ewentualnym naruszeniem RODO, jeżeli sprawa dotyczy wyłącznie jednostki organizacyjnej w jego państwie członkowskim lub znacznie wpływa na osoby, których dane dotyczą wyłącznie w jego państwie członkowskim. W pozostałych przypadkach właściwy dla postępowań prowadzonych w przypadku transgranicznego przetwarzania danych będzie organ nadzorczy głównej lub pojedynczej jednostki organizacyjnej administratora danych osobowych. Zasada *one-stop-shop* nie będzie miała jednak zastosowania w przypadku, gdy podmioty z grupy administratora danych osobowych przetwarzają samodzielnie dane osobowe w poszczególnych krajach członkowskich, ale nie dochodzi do wymiany danych między nimi (brak elementu transgranicznego). W takim przypadku każdorazowo właściwy będzie organ nadzorczy państwa, w którym dochodzi do przetwarzania. Jednak wydaje się, że w przypadku prowadzenia odrębnych postępowań, pożądana w tym zakresie będzie wymiana informacji między organami nadzorczymi (tak jak jest w opisywanym w dalszej części przypadku spółki Bisnode, wobec której niezależne postępowania prowadzone były (są) w Pol-

[10] Zob. EU General Data Protection Regulation, General Information Document, Article 29 Data Protection Working Party Documents, s. 6; S. Schmitz, *The Article 29 Working Party's Guidelines for Identifying the Lead Supervisory Authority in Cross-Border Data Processing*, „European Data Protection Law Review" 2017/1, s. 90–92.

sce, Czechach i Słowacji, a organy ze sobą wzajemnie współpracują). W kontekście niniejszej publikacji zasada ta ma szczególne znaczenie. Analizując poszczególne kary administracyjne, poszukiwana jest odpowiedź na pytanie, czy RODO stosowane jest jednolicie we wszystkich krajach członkowskich, a do tego niezbędna jest współpraca i dialog między organami nadzorczymi.

Jak wskazano wcześniej, ogólne rozporządzenie nie przewiduje wprost odpowiedzialności karnej za naruszenie ochrony danych osobowych. Prawodawca unijny przyznał jednak państwom członkowskim możliwość realizacji zadań związanych z ochroną danych. Motyw 149 preambuły RODO wskazuje, że państwa członkowskie powinny mieć możliwość ustanawiania przepisów wprowadzających odpowiedzialność karną za naruszenie ogólnego rozporządzenia oraz krajowych przepisów przyjętych na jego mocy. Artykuł 84 RODO stanowi, że państwa członkowskie przyjmują przepisy określające „inne sankcje" za naruszenie przepisów rozporządzenia. Rozporządzenie nie wskazuje na rodzaj ani typ sankcji, wymaga jednak, by były one skuteczne, proporcjonalne i odstraszające.

Polski ustawodawca skorzystał z przyznanego mu prawa do zdefiniowania dodatkowych sankcji. Ustawa o ochronie danych osobowych wprowadza katalog czynów zabronionych związanych z naruszeniem ochrony danych osobowych. Pierwszy z nich polega na przetwarzaniu danych osobowych w sytuacji, gdy przetwarzanie to jest niedopuszczalne lub podejmowane przez osobę do tego nieuprawnioną. Czyn ten podlega karze grzywny, ograniczenia wolności lub pozbawienia wolności do lat dwóch. Należy przyjąć, że przetwarzanie danych jest niedopuszczalne, gdy nie zachodzi żadna z okoliczności określonych w art. 6 lub 10 RODO bądź gdy zachodzą okoliczności dodatkowe uniemożliwiające przetwarzanie danych (np. wyrażenie sprzeciwu przez osobę, której dane dotyczą). Ustawodawca przewidział również kwalifikowaną formę tego przestępstwa, polegająca na nielegalnym przetwarzaniu szczególnych kategorii danych. W tym przypadku osoba przetwarzająca dane podlega karze grzywny, ograniczenia wolności lub pozbawienia wolności do lat trzech (art. 107 u.o.d.o.). Przestępstwa określone w art. 107 u.o.d.o.

stanowią występek, który można popełnić tylko umyślnie. Czyny te ścigane są z urzędu[11].

Drugim przestępstwem uregulowanym przez polskiego ustawodawcę jest udaremnienie lub utrudnienie prowadzenia kontroli przestrzegania przepisów o ochronie danych osobowych. Może ono polegać na każdym działaniu lub zaniechaniu działania, które zakłóca przebieg kontroli lub uniemożliwia jej przeprowadzenie. Co oczywiste, znamion czynu zabronionego nie realizuje korzystanie przez podmiot kontrolowany z przysługujących mu uprawnień[12]. Przestępstwo z art. 108 ust. 1 u.o.d.o. zagrożone jest karą grzywny, ograniczenia wolności lub pozbawienia wolności do lat dwóch. Ustęp 2 tego artykułu penalizuje czyn polegający na niedostarczeniu danych niezbędnych do określenia podstawy wymiaru administracyjnej kary pieniężnej lub dostarczaniu danych, które uniemożliwiają ustalenie podstawy wymiaru administracyjnej kary pieniężnej. Podobnie jak przestępstwa opisane wyżej, ma ono charakter powszechny. W praktyce jednak mogą je popełnić jedynie te osoby, które posiadają dostęp do tych informacji. Można więc przyjąć, że są nimi kierownik podmiotu wobec, którego toczy się postępowanie, inspektor ochrony danych, jeżeli został powołany oraz wybrani pracownicy bądź inne osoby, którym powierzono przetwarzanie danych[13]. Czyn ten również zagrożony jest karą grzywny, ograniczenia wolności lub pozbawienia wolności do lat dwóch.

Jak wskazano wyżej, odpowiedzialność karna za naruszenie ochrony danych osobowych została wprowadzona na gruncie polskiego ustawodawstwa, a nie ogólnego rozporządzenia. Ze względu na powszechny charakter przestępstw należy przyjąć, że odpowiedzialność karna ma znacznie szerszy zakres niż odpowiedzialność administracyjna lub cywilnoprawna, gdyż nie została ograniczona wyłącznie do administratorów danych i podmiotów przetwarzających. Trzeba jednak pamiętać, że

[11] M. Zimna, *Odpowiedzialność karna za naruszenie ochrony danych osobowych*, „Prokuratura i Prawo" 2020/1, s. 57 i n.

[12] J. Łuczak-Tarka [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. D. Lubasz, LEX 2019, art. 108.

[13] J. Łuczak-Tarka [w:] *Ustawa...*, red. D. Lubasz, LEX 2019, art. 108.

reżim odpowiedzialności karnej nie zastępuje odpowiedzialności administracyjnej przewidzianej przez przepisy RODO. Obydwa reżimy obowiązują równolegle jako systemowo różne rodzaje odpowiedzialności[14].

2. Administracyjna kara pieniężna jako narzędzie zapewniające efektywność regulacji

Jednym z najważniejszych elementów reformy europejskiego prawa ochrony danych osobowych było wprowadzenie nowej sankcji za naruszenie ochrony danych osobowych w postaci administracyjnej kary pieniężnej. Unijny prawodawca uznał karę za kluczowy element egzekwowania przepisów rozporządzenia, mający zapewnić jak największą skuteczność nowej regulacji (motyw 148 preambuły RODO). Należy wszak pamiętać, że jednym z celów przeprowadzonej reformy była właśnie poprawa skuteczności egzekwowania przestrzegania przepisów. Prawodawca uznał, że zagrożenie wysoką karą pieniężną zmusi administratorów i podmioty przetwarzające do większej ostrożności w zakresie podejmowanych czynności przetwarzania[15]. Istotnym elementem nowej instytucji prawnej było wprowadzenie jednolitych zasad nakładania administracyjnych kar pieniężnych, co uczyniono na gruncie art. 83 RODO[16]. Rozporządzanie wymienia jedynie rodzaje naruszeń oraz wskazuje górną granicę zagrożenia i kryteria ustalania wysokości kar. Określenie tych reguł było niezbędne dla zharmonizowanego stosowania administracyjnych kar administracyjnych przez organy nadzorcze poszczególnych państw członkowskich. Prawodawca unijny stworzył swoiste ramy odpowiedzialności administracyjnej, dzięki którym niezależnie od państwa, w którym toczyć się będzie postępowanie, penalizowane będą dokładnie te same naruszenia, a wysokość kar będzie oscylować w zbliżonym przedziale. Motyw 150 preambuły

[14] M. Zimna, *Odpowiedzialność*..., s. 57 i n.

[15] P. Fajgielski [w:] *Ogólne*..., red. P. Fajgielski, LEX 2018, art. 83.

[16] Szerzej na temat administracyjnych kar pieniężnych w prawie unijnym A. Weyembergh, N. Joncheray, *Punitive administrative sanctions and procedural safeguards. A blurred picture that needs to be addressed*, „New Journal of European Criminal Law" 2016/7(2), s. 190–209 oraz A. de Moor-van Vugt, *Administrative Sanctions in EU Law*, „Review of European Administrative Law" 2012/5(1), s. 5–41.

RODO wyraźnie wskazuje, że to do organu nadzorczego należy obowiązek określenia wysokości kary indywidualnie dla każdego przypadku z uwzględnieniem wszystkich stosowanych okoliczności danej sytuacji.

Warto wskazać, że w związku z wieloletnimi dyskusjami nad istotą administracyjnej kary pieniężnej, ustawodawca zadecydował o wprowadzeniu jej definicji legalnej w polskim porządku prawnym[17]. Na mocy ustawy z 7.04.2017 r. o zmianie ustawy – Kodeks postępowania administracyjnego oraz niektórych innych ustaw[18] wprowadzono do Kodeksu postępowania administracyjnego art. 189b. Zgodnie z jego treścią przez administracyjną karę pieniężną należy rozumieć sankcję o charakterze pieniężnym, nakładaną przez organ administracji publicznej, w drodze decyzji, w następstwie naruszenia prawa polegającego na niedopełnieniu obowiązku albo naruszeniu zakazu ciążącego na osobie fizycznej, osobie prawnej albo jednostce organizacyjnej nieposiadającej osobowości prawnej.

Zgodnie z RODO administracyjne kary pieniężne powinny być skuteczne, proporcjonalne i odstraszające. W opinii Grupy Roboczej Art. 29 oznacza to, że kary pieniężne (podobnie jaki inne środki naprawcze) powinny odpowiadać charakterowi, wadze i konsekwencjom naruszenia. Ocena skuteczności kary musi uwzględniać cel wybranego środka naprawczego. Może nim być przywrócenie zgodności z obowiązującymi przepisami, ukaranie za bezprawne działanie lub obywa z nich[19]. Już w chwili obecnej można zaobserwować, że krajowe organy nadzorcze uwzględniają cel nakładanej sankcji w procesie jej wymierzania. W ramach przykładu warto przytoczyć fragment decyzji polskiego organu nadzorczego nakładającego administracyjną karę pieniężną na administratora danych: „Wskazać należy, że kara pieniężna nałożona na Spółkę w związku z brakiem współpracy z Prezesem Urzędu Ochrony Danych Osobowych ma charakter represyjny (ma spowodować by Spółka ponio-

[17] J. Łuczak [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, art. 83, s. 1057.

[18] Dz.U. poz. 935.

[19] Grupa Robocza Art. 29, Wytyczne w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia nr 2016/679, przyjęte 3.10.2017 r., WP 253, s. 6 (Wytyczne WP 253).

sła karę finansową za unikanie kontroli) oraz prewencyjny (ma zapobiec naruszaniu prawa w przyszłości przez Spółkę, ale i przez inne podmioty). Ponadto, kara pieniężna nałożona na Spółkę ma również charakter odstraszający i wiąże się z zapobieganiem popełniania naruszeń. Kara ma odstraszać zarówno Spółkę przed ponownym naruszeniem, jak i inne podmioty"[20]. Przytoczona decyzja wyraźnie wskazuje na podwójny wymiar administracyjnej kary pieniężnej – indywidualny oraz *erga omnes*. Nie ulega wątpliwości, że decyzja wywiera skutek represyjny wobec podmiotu, który dokonał naruszenia ochrony danych osobowych. Sankcja ta ma także charakter prewencyjny wobec ukaranego podmiotu[21]. Trzeba jednak pamiętać, że kara nałożona przez organ nadzorczy będzie miała również wpływ na innych administratorów danych (bezpośrednio niezaangażowanych w daną czynność przetwarzania). Decyzja wywrze na nich przede wszystkim skutek prewencyjny, ale i edukacyjny. Organ nadzorczy w uzasadnieniu swojej decyzji dokonuje wszakże interpretacji przepisów, które w przyszłości mogą stanowić istotną wskazówkę zarówno dla ukaranego, jak i innych podmiotów.

Grupa Robocza Art. 29 wskazuje, że lepsze zrozumienie skuteczności, proporcjonalności oraz odstraszającego charakteru kar przyniesie w najbliższej przyszłości praktyka krajowych organów nadzorczych oraz orzecznictwo. Należy jednak zaznaczyć, iż Trybunał Sprawiedliwości Unii Europejskiej wypowiadał się na temat proporcjonalności kar już na gruncie wcześniej obowiązujących przepisów[22]. Wydaje się więc, że rozważania te mogą stanowić cenną wskazówkę dla krajowych organów

[20] Decyzja Prezesa Urzędu Ochrony Danych Osobowych z 9.03.2020 r. w sprawie Vis Consulting Sp. z o.o., ZSPR.421.19.2019, https://uodo.gov.pl/decyzje/ZSPR.421.19.2019 (dostęp: 8.11.2020 r.).

[21] Również na ten temat A. Mednis, *Administracyjne kary pieniężne w ogólnym rozporządzeniu o ochronie danych*, „Informacja w Administracji Publicznej" 2016/3, s. 15–20.

[22] W tym miejscu warto wskazać m.in. na wyrok TS z 23.02.1983 r., C-66/82, Fromançais S.A. v. Fonds d'orientation et de régularisation des marchés agricoles, ECLI:EU:C:1983:42 oraz wyrok TS z 14.01.1987 r., C-281/84, Zuckerfabrik Bedburg AG and others v. Council and Commission of the European Communities, ECLI:EU:C:1986:489. Szerzej na temat proporcjonalności J. Maliszewska-Nienartowicz, *Rozwój zasady proporcjonalności w europejskim prawie wspólnotowym*, „Studia Europejskie" 2006/1, s. 59–80.

nadzorczych oraz sądów (w szczególności w chwili obecnej, gdy linia orzecznicza nie została jeszcze w pełni ugruntowana).

Administracyjna kara pieniężna może zostać nałożona na administratorów danych, podmioty przetwarzające, podmioty certyfikujące oraz podmioty monitorujące[23]. W zależności od okoliczności indywidualnego przypadku, organ nadzorczy może wymierzyć karę zamiast lub obok innych środków naprawczych wymienionych w art. 58 ust. 2 lit. a–h oraz j RODO. Katalog ten przewiduje między innymi wydawanie ostrzeżeń, udzielanie upomnień, nakazanie spełnienia żądania osoby, której dane dotyczą, nakazanie dostosowania operacji przetwarzania do przepisów rozporządzenia oraz wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania.

Organ nadzorczy, decydując czy nałożenie administracyjnej kary pieniężnej jest zasadne, a następnie ustalając jej wysokość, ma obowiązek uwzględnienia okoliczności wskazanych w art. 83 ust. 2 RODO. Należy podkreślić, że katalog ten ma charakter otwarty, a organ nadzorczy powinien uwzględnić wszystkie inne czynniki mające wpływ na okoliczności sprawy (nawet jeżeli nie zostały wymienione we wspomnianym przepisie). Jak sugerują P. Litwiński, P. Barta i M. Kawecki, okoliczności zawarte w katalogu można podzielić na cztery grupy[24]. Pierwsza z nich odnosi się do działań lub zaniechań podmiotu w ramach konkretnie rozpatrywanej sprawy oraz ich skutków dla osób poszkodowanych. Mowa tu między innymi o charakterze, wadze i czasie trwania naruszenia, przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą oraz rozmiaru poniesionej

[23] Zgodnie z art. 83 RODO organ nadzorczy może nałożyć administracyjną karę pieniężną nie tylko na administratorów i podmioty przetwarzające dane, lecz także na podmioty certyfikujące i monitorujące. Podmiotem certyfikującym jest podmiot dokonujący certyfikacji zgodności przetwarzania danych z obowiązującym prawem. Natomiast podmiotem monitorującym jest podmiot monitorujący przestrzeganie kodeksów postępowania przyjętych na podstawie art. 40 RODO. Ogólne rozporządzenie dopuszcza możliwość nałożenia kary na wspomniane wyżej pomioty w przypadku naruszenia obowiązków wyrażonych w art. 41 ust. 4, art. 42 oraz 43. Za: P. Fajgielski [w:] *Ogólne...*, red. P. Fajgielski, LEX 2018, art. 83.

[24] P. Litwiński, P. Barta, M. Kawecki [w:] *Rozporządzenie UE...*, red. P. Litwiński, art. 83, s. 835–836.