GRUPA ROBOCZA DS. OCHRONY DANYCH ART. 29

17/PL

WP 253

Wytyczne w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia nr 2016/679

Przyjęte w dniu 3 października 2017 r.

GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE

PRZETWARZANIA DANYCH OSOBOWYCH

powołana na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.,

uwzględniając art. 29 i 30 tej dyrektywy,

uwzględniając swój regulamin wewnętrzny,

PRZYJMUJE NINIEJSZE WYTYCZNE:

Spis treści:

I. Wprowadzenie

UE zakończyła kompleksową reformę rozporządzenia o ochronie danych w Europie. Reforma opiera się na kilku filarach (kluczowych elementach): spójnych zasadach, uproszczonych procedurach, skoordynowanych działaniach, zaangażowaniu użytkowników, skuteczniejszym informowaniu i silniejszych uprawnieniach wykonawczych.

Administratorzy danych i podmioty przetwarzające dane mają większe obowiązki w zakresie zapewnienia skutecznej ochrony danych osobowych osób fizycznych. Organy nadzorcze są uprawnione do zapewnienia przestrzegania zasad ogólnego rozporządzenia o ochronie danych (zwanego dalej „rozporządzeniem"), a także praw osób fizycznych, których dane osobowe są lub mogą być przetwarzane, zgodnie z jego literą i duchem.

Konsekwentne egzekwowanie zasad ochrony danych ma kluczowe znaczenie dla zharmonizowanego systemu ochrony danych. Administracyjne kary pieniężne są zasadniczym elementem nowego systemu egzekwowania wprowadzonego na mocy rozporządzenia, stanowiąc tym samym wraz z innymi środkami przewidzianymi w art. 58 istotną część zestawu narzędzi umożliwiających egzekwowanie prawa przez organy nadzorcze.

Niniejszy dokument jest przeznaczony do użytku organów nadzorczych w celu zapewnienia lepszego stosowania i egzekwowania rozporządzenia oraz wyraża wspólne rozumienie przepisów art. 83 rozporządzenia, a także ich współzależność z art. 58 i 70 oraz odpowiednimi motywami.

W szczególności, zgodnie z art. 70 ust. 1 lit. e), Europejska Rada Ochrony Danych jest uprawniona do wydawania wytycznych i zaleceń oraz określania najlepszych praktyk, by zachęcić do spójnego stosowania tego rozporządzenia, a art. 70 ust. 1 lit. k) stanowi podstawę do wydawania wytycznych dotyczących ustalania wysokości administracyjnych kar pieniężnych.

Wytyczne te nie są ani wyczerpujące, ani nie zawierają wyjaśnień co do różnic występujących między systemami prawa administracyjnego, cywilnego i karnego, jeżeli chodzi o nakładanie kar administracyjnych w ogólności.

W celu osiągnięcia spójnego podejścia do kwestii nakładania administracyjnych kar pieniężnych, które to podejście w odpowiedni sposób uwzględnia wszystkie zasady zawarte w niniejszych wytycznych, Europejska Rada Ochrony Danych uzgodniła wspólne rozumienie kryteriów oceny ujętych w art. 83 ust. 2 rozporządzenia. Europejska Rada Ochrony Danych i poszczególne organy nadzorcze zobowiązują się do stosowania niniejszych wytycznych jako wspólnego podejścia.

II. Zasady

W przypadku gdy w oparciu o ocenę okoliczności faktycznych sprawy zostanie stwierdzone naruszenie rozporządzenia, właściwy organ nadzorczy obowiązany jest wskazać najodpowiedniejszy środek naprawczy (najodpowiedniejsze środki naprawcze) w celu zaradzenia takiemu naruszeniu. Przepisy art. 58 ust. 2 lit. b)–j)[1] określają działania, które organy nadzorcze mogą podejmować w przypadku nieprzestrzegania odpowiednich przepisów przez administratora lub podmiot przetwarzający. Korzystając ze wskazanych uprawnień, organy nadzorcze mają obowiązek przestrzegać następujących zasad:

1. Naruszenie rozporządzenia powinno prowadzić do nałożenia „równoważnych kar".

Pojęcie „równoważności" ma zasadnicze znaczenie dla określenia zakresu obowiązków organów nadzorczych w celu zapewnienia spójności w korzystaniu z uprawnień naprawczych zgodnie z art. 58 ust. 2 w ogóle, a w szczególności w odniesieniu do stosowania administracyjnych kar pieniężnych[2].

Aby zapewnić wysoki i spójny stopień ochrony osób fizycznych oraz usunąć przeszkody w przepływie danych osobowych w Unii, ***należy zapewnić równorzędny stopień ochrony*** *we wszystkich państwach członkowskich* (motyw 10). Motyw 11 wyjaśnia, że równorzędny stopień ochrony danych osobowych w Unii wymaga m.in. „*równorzędnych uprawnień w zakresie monitorowania i egzekwowania przepisów o ochronie danych osobowych oraz równorzędnych kar za naruszenia tych przepisów w państwach członkowskich*". Ponadto równorzędne kary w państwach członkowskich oraz skuteczna współpraca organów nadzorczych różnych państw członkowskich są postrzegane jako środki „*zapobiegania rozbieżnościom hamującym swobodny przepływ danych osobowych na rynku wewnętrznym*", zgodnie z motywem 13 rozporządzenia.

Rozporządzenie ustanawia solidniejszą podstawę zapewnienia większej spójności niż dyrektywa 95/46/WE, gdyż jest ono bezpośrednio stosowane w państwach członkowskich. Podczas gdy organy nadzorcze działają „w sposób w pełni niezależny" (art. 52) w odniesieniu do rządów krajowych, administratorów lub podmiotów przetwarzających, mają one obowiązek współpracować „*w celu zapewnienia spójnego stosowania i egzekwowania niniejszego rozporządzenia*" (art. 57 ust. 1 lit. g)).

W rozporządzeniu wymaga się większej spójności w zakresie nakładania kar niż w dyrektywie 95/46. W sprawach transgranicznych spójność osiąga się przede wszystkim poprzez zastosowanie mechanizmu kompleksowej współpracy oraz w pewnym stopniu mechanizmu spójności określonego w nowym rozporządzeniu.

W przypadkach krajowych objętych rozporządzeniem organy nadzorcze będą stosować niniejsze wytyczne w duchu współpracy zgodnie z art. 57 ust. 1 lit. g) i art. 63 w celu zapewnienia spójnego stosowania i egzekwowania rozporządzenia. Chociaż organy nadzorcze zachowują niezależność w wyborze środków naprawczych wymienionych w art. 58 ust. 2, należy unikać sytuacji, w których organy nadzorcze w podobnych sprawach stosują różne środki naprawcze.

[1] Artykuł 58 ust. 2 lit. a) stanowi, że ostrzeżenia mogą być wydawane w odniesieniu do „możliwości naruszenia przepisów niniejszego rozporządzenia poprzez planowane operacje przetwarzania". Innymi słowy, w sprawie objętej przepisem nie doszło jeszcze do naruszenia rozporządzenia.

[2] Nawet jeżeli systemy prawne w niektórych krajach UE nie przewidują nakładania administracyjnych kar pieniężnych określonych w rozporządzeniu, takie stosowanie zasad we wspomnianych państwach członkowskich musi mieć skutek równoważny administracyjnym karom pieniężnym nakładanym przez organy nadzorcze (motyw 151). Sądy są związane rozporządzeniem, lecz nie są związane wytycznymi Europejskiej Rady Ochrony Danych.

Ta sama zasada obowiązuje, gdy owymi środkami naprawczymi są nakładane kary.

2. Podobnie jak wszystkie środki naprawcze wybierane przez organy nadzorcze, administracyjne kary pieniężne winny być „skuteczne, proporcjonalne i odstraszające”.

Podobnie jak wszelkie środki naprawcze w ogólności, administracyjne kary pieniężne powinny w stosowny sposób odpowiadać charakterowi, wadze i konsekwencjom naruszenia, a organy nadzorcze muszą dokonywać oceny okoliczności faktycznych danej sprawy w sposób spójny i obiektywnie uzasadniony. Ocena tego, co jest skuteczne, proporcjonalne i odstraszające, w każdym przypadku będzie musiała również odzwierciedlać cel wybranego środka naprawczego, którym jest przywrócenie zgodności z przepisami lub ukaranie za bezprawne zachowanie (lub oba te cele).

Organy nadzorcze powinny określić środek naprawczy, który jest „*skuteczny, proporcjonalny i odstraszający*” (art. 83 ust. 1) zarówno w sprawach krajowych (art. 55), jak i w sprawach związanych z transgranicznym przetwarzaniem danych osobowych (jak określono w art. 4 ust. 23).

W niniejszych wytycznych uznano, że prawodawstwo krajowe może wprowadzić dodatkowe wymogi w zakresie prowadzenia przez organy nadzorcze postępowania przymuszającego. Mogą one przykładowo obejmować powiadomienia adresowe, formę, terminy składania oświadczeń, środki odwoławcze, egzekucję, uiszczanie płatności[3].

Takie wymogi nie powinny jednak w praktyce utrudniać osiągnięcia skuteczności, proporcjonalności lub odstraszającego charakteru stosowanych środków naprawczych.

Bardziej precyzyjne określenie skuteczności, proporcjonalności lub odstraszającego charakteru przyniesie rozwijająca się praktyka samych organów nadzorczych (w zakresie ochrony danych oraz doświadczenia organów w innych sektorach regulacyjnych), a także orzecznictwo zawierające wykładnię tych zasad.

W celu nałożenia skutecznych, proporcjonalnych i odstraszających kar pieniężnych organ nadzorczy stosuje definicję pojęcia przedsiębiorstwa przyjętą przez TSUE do celów stosowania art. 101 i 102 TFUE, a mianowicie, że poprzez pojęcie przedsiębiorstwa **należy rozumieć** jednostkę gospodarczą, którą może utworzyć spółka dominująca i wszystkie zaangażowane podmioty zależne. Zgodnie z prawem i orzecznictwem[4] UE przedsiębiorstwo jest tu rozumiane jako jednostka gospodarcza, która prowadzi działalność handlową/gospodarczą, bez względu na osobę prawną (motyw 150).

3. Właściwy organ nadzorczy dokonuje oceny „w każdym indywidualnym przypadku”.

[3] Przykładowo ramy konstytucyjne i projektowane regulacje prawne w zakresie ochrony danych w Irlandii stanowią, że w sprawie samego naruszenia podjęta zostaje formalna decyzja, a o decyzji tej informuje się odpowiednie strony przed dokonaniem oceny skali kary (kar). Decyzji w sprawie samego naruszenia nie można zmienić podczas oceny skali kary (kar).

[4] Definicja sformułowana w orzecznictwie TSUE brzmi następująco: „pojęcie przedsiębiorstwa obejmuje każdy podmiot prowadzący działalność gospodarczą niezależnie od statusu prawnego podmiotu i sposobu, w jaki jest on finansowany” (sprawa Höfner i Elsner, pkt 21, ECLI:UE:C:1991:161). Pojęcie przedsiębiorstwa „winno być rozumiane jako odnoszące się do jednostki gospodarczej, nawet jeśli z prawnego punktu widzenia owa jednostka gospodarcza składa się z wielu osób fizycznych lub prawnych” (sprawa Confederación Española de Empresarios de Estaciones de Servicio, pkt 40, ECLI:EU:C:2006:784).

Administracyjne kary pieniężne mogą być nakładane w odpowiedzi na cały szereg naruszeń. Artykuł 83 rozporządzenia przewiduje zharmonizowane podejście do przypadków naruszenia obowiązków enumeratywnie wyliczonych w ust. 4–6. Prawo państw członkowskich może rozszerzyć stosowanie art. 83 na organy i podmioty publiczne ustanowione w konkretnym państwie członkowskim. Ponadto prawo państwa członkowskiego może dopuszczać — a nawet wydać upoważnienie — w zakresie nałożenia kary pieniężnej za naruszenie innych przepisów prawa niż art. 83 ust. 4–6.

Rozporządzenie wymaga dokonania oceny każdego przypadku z osobna[5]. Artykuł 83 ust. 2 stanowi punkt wyjścia dla przeprowadzenia takiej indywidualnej oceny. Ustęp ten stanowi, że „*decydując, czy nałożyć administracyjną karę pieniężną, oraz ustalając jej wysokość, zwraca się w każdym indywidualnym przypadku należytą uwagę na...*". Stosownie do powyższego oraz w świetle motywu 148[6] organ nadzorczy jest odpowiedzialny za wybór najodpowiedniejszego środka (najodpowiedniejszych środków). W przypadkach, o których mowa w art. 83 ust. 4–6, wybór ten **musi** uwzględniać wszystkie środki naprawcze, w tym nałożenie odpowiedniej administracyjnej kary pieniężnej, czy to towarzyszącej środkowi naprawczemu na mocy art. 58 ust. 2, czy też występującej samodzielnie.

Kary pieniężne są ważnym narzędziem, które organy nadzorcze powinny stosować w odpowiednich okolicznościach. Zachęca się organy nadzorcze do stosowania rozważnego i wyważonego podejścia w zakresie stosowania środków naprawczych, tak aby reakcja na dane naruszenie była zarówno skuteczna i odstraszająca, jak również proporcjonalna. Celem nie jest tu traktowanie kar pieniężnych jako ostateczności, czy też powstrzymywanie się od ich stosowania, lecz nakładanie ich w sposób uniemożliwiający podważanie ich skuteczności jako narzędzia.

Europejska Rada Ochrony Danych, w sytuacjach gdy jest do tego upoważniona na mocy art. 65 rozporządzenia, wyda wiążącą decyzję w sprawie sporów między organami w kwestiach dotyczących przede wszystkim stwierdzenia istnienia naruszenia. W przypadku gdy istotny i uzasadniony sprzeciw wiąże się z kwestią zgodności środka naprawczego z wytycznymi ogólnego rozporządzenia o ochronie danych, w decyzji Europejskiej Rady Ochrony Danych określi się również sposób, w jaki

[5] W związku ze stosowaniem kryteriów określonych w art. 83 istnieją inne przepisy, które wzmacniają fundamenty takiego podejścia, a mianowicie:

- Motyw 141: „*Postępowanie wyjaśniające na podstawie skargi powinno być prowadzone – z zastrzeżeniem kontroli sądowej – w zakresie odpowiadającym konkretnej sprawie*".
- Motyw 129: „*Swoje uprawnienia organy nadzorcze powinny wykonywać zgodnie z odpowiednimi zabezpieczeniami proceduralnymi przewidzianymi w prawie Unii i prawie państwa członkowskiego, bezstronnie, sprawiedliwie i w rozsądnym terminie. W szczególności każdy środek powinien być odpowiedni, niezbędny i proporcjonalny, aby zapewnić przestrzeganie niniejszego rozporządzenia – z uwzględnieniem okoliczności danej sprawy...".*
- Artykuł 57 ust. 1 lit f): „*rozpatruje skargi wniesione przez osobę, której dane dotyczą, lub przez podmiot, organizację lub zrzeszenie zgodnie z art. 80, w odpowiednim zakresie prowadzi postępowania w przedmiocie tych spraw*".

[6] „*Aby egzekwowanie przepisów niniejszego rozporządzenia było skuteczniejsze, należy za jego naruszenie nakładać sankcje, w tym administracyjne kary pieniężne – oprócz lub zamiast odpowiednich środków nakładanych na mocy niniejszego rozporządzenia przez organ nadzorczy. Jeżeli naruszenie jest niewielkie lub jeżeli grożąca kara pieniężna stanowiłaby dla osoby fizycznej nieproporcjonalne obciążenie, można zamiast tego udzielić upomnienia. Powinno się jednak zwrócić należytą uwagę na charakter, wagę oraz czas trwania naruszenia, na to, czy naruszenie nie było umyślne, na działania podjęte dla zminimalizowania szkody, na stopień odpowiedzialności lub wszelkie mające znaczenie wcześniejsze naruszenia, na sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, na przestrzeganie środków nałożonych na administratora lub podmiot przetwarzający, na stosowanie kodeksów postępowania oraz wszelkie inne czynniki obciążające lub łagodzące. Nakładanie sankcji, w tym administracyjnych kar pieniężnych, powinno podlegać odpowiednim zabezpieczeniom proceduralnym zgodnym z ogólnymi zasadami prawa Unii i z Kartą praw podstawowych, w tym skutecznej ochronie prawnej i prawu do rzetelnego procesu*".

zaproponowana przez właściwy organ nadzorczy w projekcie decyzji administracyjna kara pieniężna spełnia zasady skuteczności, proporcjonalności i odstraszania. Wytyczne Europejskiej Rady Ochrony Danych dotyczące stosowania art. 65 rozporządzenia w kontekście decyzji, którą ma podjąć Europejska Rada Ochrony Danych, będą przedmiotem osobnego szczegółowego omówienia.

---

4. Zharmonizowane podejście do administracyjnych kar pieniężnych w zakresie ochrony danych wymaga aktywnego udziału i wymiany informacji między organami nadzorczymi.

W niniejszych wytycznych uznaje się, że uprawnienia w zakresie nakładania kar pieniężnych są dla niektórych krajów nowością w dziedzinie ochrony danych, co z kolei wiąże się z wieloma kwestiami związanymi z zasobami, organizacją i ukształtowaniem postępowania. W szczególności od decyzji dotyczących wykonywania przez organy nadzorcze przyznanych im uprawnień w zakresie nakładania kar pieniężnych będzie można się odwołać do sądów krajowych.

Organy nadzorcze współpracują ze sobą oraz — w stosownych przypadkach — z Komisją Europejską przy wykorzystaniu mechanizmów współpracy określonych w rozporządzeniu w celu usprawnienia formalnej i nieformalnej wymiany informacji np. poprzez regularne warsztaty. Współpraca ta powinna opierać się na wymianie doświadczeń i praktyk w zakresie nakładania kar pieniężnych, tak aby ostatecznie wypracować większą spójność.

Ta proaktywna wymiana informacji, oprócz rozwijającego się orzecznictwa dotyczącego korzystania z takich uprawnień, może prowadzić do rewizji zasad lub poszczególnych szczegółów niniejszych wytycznych.

III. Kryteria oceny określone w art. 83 ust. 2

Artykuł 83 ust. 2 zawiera wykaz kryteriów, którymi organy nadzorcze powinny się posługiwać, przeprowadzając ocenę zarówno tego, czy należy nałożyć karę pieniężną, jak i określając jej wysokość. Regulacja ta nie zaleca dokonywania ponownej oceny tych samych kryteriów, lecz przeprowadzenie oceny uwzględniającej wszystkie okoliczności każdego indywidualnego przypadku zgodnie z art. 83[7].

Wnioski wyciągnięte na pierwszym etapie oceny mogą zostać wykorzystane w drugiej części dotyczącej wysokości kary, tym samym pozwalając uniknąć powtórnej oceny przy użyciu tych samych kryteriów.

Niniejsza sekcja zawiera wskazówki dla organów nadzorczych dotyczące sposobu interpretacji poszczególnych okoliczności faktycznych sprawy w świetle kryteriów określonych w art. 83 ust. 2.

a) Charakter, waga i czas trwania naruszenia

Zgodnie z rozporządzeniem prawie wszystkie obowiązki administratorów i podmiotów przetwarzających są podzielone na kategorie zgodnie z ich **charakterem** określonym w przepisach art. 83 ust. 4–6. Poprzez ustanowienie dwóch różnych maksymalnych wysokości administracyjnej kary pieniężnej (10/20 mln EUR) w rozporządzeniu wskazuje się, że naruszenie niektórych przepisów rozporządzenia może być poważniejsze niż naruszenie innych przepisów. Niemniej oceniając okoliczności faktyczne sprawy w świetle ogólnych kryteriów określonych w art. 83 ust. 2, właściwy organ nadzorczy może zdecydować, że w danym przypadku istnieje większa lub mniejsza potrzeba reagowania za pomocą środka naprawczego w formie kary pieniężnej. W przypadku gdy wybrano karę pieniężną jako jeden z wielu właściwych środków naprawczych, należy zastosować system klasyfikacji rozporządzenia (art. 83 ust. 4–6) w celu wskazania maksymalnej kary pieniężnej, którą można nałożyć zgodnie z charakterem omawianego naruszenia.

W motywie 148 wprowadza się pojęcie „niewielkich naruszeń". Takie naruszenia mogą odnosić się do pogwałcenia jednego lub kilku przepisów rozporządzenia wymienionych w art. 83 ust. 4 lub 5. Ocena kryteriów określonych w art. 83 ust. 2 może jednak skłonić organ nadzorczy do uznania, że w konkretnych okolicznościach danego przypadku dane naruszenie na przykład nie stanowi poważnego zagrożenia dla praw osób, których dane dotyczą, oraz nie wpływa na istotę danego obowiązku. W takich przypadkach karę pieniężną można (choć nie zawsze) zastąpić upomnieniem.

W motywie 148 nie przewiduje się obowiązku zastępowania przez organ nadzorczy kary pieniężnej każdorazowo upomnieniem w przypadku niewielkiego naruszenia („*można zamiast tego udzielić upomnienia*"), a raczej wskazuje się na możliwość, z której można skorzystać po dokonaniu konkretnej oceny wszystkich okoliczności sprawy.

Motyw 148 stwarza taką samą możliwość zastąpienia kary pieniężnej upomnieniem w przypadku gdy administratorem danych jest osoba fizyczna, a grożąca kara pieniężna stanowiłaby dla osoby fizycznej nieproporcjonalne obciążenie. Punktem wyjścia jest tu ocena organu nadzorczego, czy — w świetle istniejących okoliczności sprawy — nałożenie kary jest konieczne. Jeżeli organ tak uzna, obowiązany jest również ocenić, czy grożąca kara pieniężna stanowiłaby dla osoby fizycznej nieproporcjonalne obciążenie.

W rozporządzeniu poszczególnym naruszeniom nie są przypisane konkretne kwoty, a jedynie określone są pułapy (kwoty maksymalne). Może to wskazywać na względnie niższą wagę naruszenia

[7] Ocena kary, jaka zostanie nałożona, może nadejść oddzielnie po dokonaniu oceny, czy doszło do naruszenia z powodu krajowych przepisów proceduralnych wynikających z wymogów konstytucyjnych w niektórych krajach. To z kolei może ograniczyć treść i ilość szczegółów w projekcie decyzji wydanym przez główny organ nadzorczy w takich krajach.

zobowiązań wymienionych w art. 83 ust. 4 w porównaniu z zobowiązaniami określonymi w art. 83 ust. 5. Skuteczna, proporcjonalna i odstraszająca reakcja na naruszenie art. 83 ust. 5 będzie jednak zależeć od okoliczności danej sprawy.

Niemniej należy zauważyć, że naruszenia przepisów rozporządzenia, które ze swej natury należą do kategorii „w wysokości do 10 mln EUR lub w wysokości do 2% jego całkowitego rocznego światowego obrotu", jak określono w art. 83 ust. 4, mogą w pewnych okolicznościach kwalifikować się do wyższej kategorii (20 mln EUR). Taka sytuacja może mieć miejsce, kiedy owe naruszenia były już wcześniej przedmiotem nakazu[8] orzeczonego przez organ nadzorczy, do którego to nakazu administrator lub podmiot przetwarzający się nie zastosowali[9] (art. 83 ust. 6). Przepisy prawa krajowego mogą w praktyce mieć wpływ na tę ocenę[10]. Charakter naruszenia, jak również „*zakres, cel danego przetwarzania, liczba poszkodowanych osób, których dane dotyczą, oraz rozmiar poniesionej przez nie szkody*" będą wskazywać na **wagę** naruszenia. Występowanie kilku różnych naruszeń popełnionych łącznie w konkretnym pojedynczym przypadku oznacza, że organ nadzorczy może nakładać administracyjne kary pieniężne w sposób, który jest zarazem skuteczny, proporcjonalny i odstraszający na poziomie najpoważniejszego naruszenia. Dlatego też w przypadku wykrycia naruszenia art. 8 i art. 12 organ nadzorczy może zastosować środki naprawcze określone w art. 83 ust. 5, które odpowiadają kategorii najpoważniejszego naruszenia, a mianowicie art. 12. Przedstawienie dalszych szczegółów na tym etapie wykracza poza zakres niniejszych wytycznych (szczegółowe wyliczenia mogłyby być przedmiotem kolejnego etapu opracowywania wytycznych).

Poniższe czynniki należy oceniać łącznie, np. liczbę osób, których dane dotyczą, wraz z potencjalnym wpływem na te osoby.

Należy ocenić **liczbę** osób, których dane dotyczą, w celu ustalenia, czy jest to pojedyncze zdarzenie, czy też mamy do czynienia z bardziej systematycznym naruszeniem lub brakiem odpowiednich sposobów postępowania. Nie oznacza to, że pojedyncze zdarzenie nie powinno być egzekwowane, gdyż nawet pojedyncze zdarzenie może mieć wpływ na dużą liczbę osób, których dane dotyczą. W zależności od okoliczności sprawy będzie to dotyczyć, odpowiednio, np. całkowitej liczby osób

[8] Nakazy wymienione w art. 58 ust. 2 to:

- nakazanie administratorowi lub podmiotowi przetwarzającemu spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy niniejszego rozporządzenia;
- nakazanie administratorowi lub podmiotowi przetwarzającemu dostosowania operacji przetwarzania do przepisów niniejszego rozporządzenia, a w stosownych przypadkach wskazanie sposobu i terminu;
- nakazanie administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych;
- wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania;
- nakazanie na mocy art. 16, 17 i 18 sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazanie na mocy art. 17 ust. 2 i art. 19 powiadomienia o tych czynnościach odbiorców, którym dane osobowe ujawniono;
- nakazanie podmiotowi certyfikującemu cofnięcia certyfikacji udzielonej na mocy art. 42 lub 43, lub nakazanie podmiotowi certyfikującemu nieudzielania certyfikacji, jeżeli jej wymogi nie są spełnione lub przestały być spełniane;
- nakazanie zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej.

[9] Stosowanie art. 83 ust. 6 w sposób bezwzględny wymaga uwzględnienia krajowych przepisów postępowania. Prawo krajowe określa, w jaki sposób wydawany jest nakaz, jak jest on doręczany, od którego momentu zaczyna obowiązywać, czy istnieje okres karencji na jego przestrzeganie. W szczególności należy uwzględnić wpływ wniesienia środka odwoławczego na wykonalność nakazu.

[10] Przepisy ustawowe dotyczące przedawnienia mogą skutkować tym, że poprzedni nakaz organu nadzorczego może nie zostać uwzględniony z uwagi na czas, jaki upłynął od orzeczenia poprzedniego nakazu. W niektórych systemach prawnych przepisy wymagają, aby po upływie terminu przedawnienia nakazu nie można było nałożyć kary pieniężnej za nieprzestrzeganie tego nakazu zgodnie z art. 83 ust. 6. Od organu nadzorczego w systemie prawnym danego kraju zależeć będzie, w jaki sposób regulacje takie będą miały na niego wpływ.

rejestrujących się w danej bazie danych, liczby użytkowników usługi, liczby klientów lub populacji danego kraju.

Należy również ocenić **cel** przetwarzania. W opinii Grupy Roboczej Art. 29 w sprawie „ograniczenia celu”[11] przeanalizowano wcześniej dwa podstawowe elementy tej zasady w przepisach o ochronie danych: określenie celu i zgodne zastosowanie. Oceniając cel przetwarzania w kontekście art. 83 ust. 2, organy nadzorcze powinny określić, w jakim stopniu przetwarzanie spełnia dwa kluczowe elementy tej zasady[12]. W niektórych sytuacjach organ nadzorczy może uznać za konieczne, aby w analizie art. 83 ust. 2 uwzględnić głębszą analizę celu samego przetwarzania.

W przypadku gdy osoba, której dane dotyczą, poniosła **szkodę**, należy uwzględnić rozmiar poniesionej szkody. Przetwarzanie danych osobowych może generować ryzyko naruszenia praw i wolności danej osoby, co ilustruje motyw 75:

> „*Ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności: jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną; jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi; jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa; jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się— w celu tworzenia lub wykorzystywania profili osobistych; jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci; lub jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą*”.

Jeżeli szkoda została lub może zostać poniesiona z powodu naruszenia rozporządzenia, organ nadzorczy winien to uwzględnić przy wyborze środka naprawczego, chociaż sam organ nadzorczy nie jest właściwy do przyznania szczególnego odszkodowania za poniesioną szkodę.

Nałożenie kary pieniężnej nie zależy od zdolności organu nadzorczego do ustalenia związku przyczynowo-skutkowego pomiędzy naruszeniem a stratą materialną (zob. np. art. 83 ust. 6).

Czas trwania naruszenia może przykładowo świadczyć o:

a) celowym działaniu administratora danych;

b) braku podjęcia odpowiednich środków zapobiegawczych;

c) niemożności wprowadzenia wymaganych środków technicznych i organizacyjnych.

[11] Opinia nr 03/2013 WP 203 w sprawie ograniczenia celu dostępna jest na stronie internetowej: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[12] Zob. także dokument grupy roboczej WP 217 dot. opinii nr 6/2014 w sprawie pojęcia prawnie uzasadnionych interesów administratora danych na mocy art. 7, a dokładnie odpowiedź na pytanie na str. 24: „Co sprawia, że interes jest »uzasadniony« lub »nieuzasadniony«?”

b) Umyślny lub nieumyślny charakter naruszenia

Zasadniczo „umyślność" obejmuje zarówno wiedzę, jak i celowe działanie, w związku z cechami charakterystycznymi czynu zabronionego, podczas gdy „nieumyślność" oznacza brak zamiaru spowodowania naruszenia, pomimo niedopełnienia przez administratora/podmiot przetwarzający obowiązku staranności wymaganego prawem.

Ogólnie uznaje się, że wykazujące pogardę wobec przepisów prawa umyślne naruszenia są poważniejsze niż te nieumyślne, a w konsekwencji częściej wiążą się z nałożeniem administracyjnej kary pieniężnej. Odpowiednie wnioski dotyczące umyślnego lub nieumyślnego charakteru naruszenia zostaną wyciągnięte na podstawie identyfikacji obiektywnych elementów działania zebranych w oparciu o okoliczności faktyczne sprawy. Ponadto rozwijające się orzecznictwo i praktyka w zakresie ochrony danych, do których zastosowanie ma rozporządzenie, wyeksponują okoliczności, które pozwolą wyodrębnić bardziej czytelne progi służące ocenie, czy dane naruszenie miało charakter umyślny.

Okolicznościami wskazującymi na umyślne naruszenia mogą być niezgodne z prawem przetwarzanie wyraźnie zatwierdzone przez ścisłe kierownictwo administratora lub – wbrew opinii inspektora ochrony danych lub wbrew istniejącym zasadom – na przykład uzyskiwanie i przetwarzanie danych o pracownikach u konkurenta z zamiarem zdyskredytowania tego konkurenta na rynku.

Innymi przykładami mogą być:

- zmiana danych osobowych w celu wywołania mylącego (pozytywnego) wrażenia dotyczącego rzekomego osiągnięcia celów — tak stało się w przypadku celów dotyczących okresów oczekiwania w szpitalach;
- handel danymi osobowymi w celach marketingowych, tj. sprzedaż danych jako „wybranych" bez sprawdzenia poglądów / ignorując poglądy osób, których dane dotyczą, w odniesieniu do sposobu użycia tych danych.

Innymi okolicznościami wskazującymi na zaniedbanie mogą być nieprzeczytanie i nieprzestrzeganie istniejących zasad, błąd ludzki, niesprawdzenie danych osobowych w opublikowanych źródłach, niedokonanie aktualizacji technicznych w odpowiednim czasie, nieprzyjęcie zasad (w przeciwieństwie do ich niestosowania).

Przedsiębiorstwa powinny być odpowiedzialne za przyjmowanie struktur i zasobów adekwatnych do charakteru i złożoności swej działalności. W związku z tym administratorzy i podmioty przetwarzające nie mogą uzasadniać naruszania przepisów o ochronie danych powołując się na niedobór zasobów. Podstawą procedur i dokumentacji działań związanych z przetwarzaniem jest podejście oparte na analizie ryzyka zgodnie z rozporządzeniem.

Istnieją szare obszary, które wpłyną na decyzję co do zastosowania/niezastosowania środka naprawczego. Wówczas organ być może uznać za niezbędne przeprowadzenie obszerniejszego dochodzenia w celu ustalenia okoliczności faktycznych sprawy i zapewnienia, że wszystkie szczególne okoliczności w każdym indywidualnym przypadku zostały należycie uwzględnione.

c) Działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą

Administratorzy danych i podmioty przetwarzające dane mają obowiązek wdrażania środków technicznych i organizacyjnych w celu zapewnienia poziomu bezpieczeństwa odpowiedniego do stopnia ryzyka, dokonywania oceny skutków dla ochrony danych oraz minimalizowania ryzyka naruszenia praw i wolności osób fizycznych wynikającego z przetwarzania danych osobowych. Jeżeli jednak dojdzie do naruszenia i osoba, której dane dotyczą, poniesie szkodę, strona odpowiedzialna powinna podjąć wszelkie możliwe starania celem ograniczenia skutków naruszenia dla danej osoby

(danych osób). Organ nadzorczy uwzględni taką odpowiedzialną postawę (lub brak takiej postawy) podczas dokonywania wyboru środka naprawczego (środków naprawczych) oraz przy ustalaniu wysokości kary pieniężnej mającej zastosowanie w konkretnym przypadku.

Pomimo szczególnej roli, jaką odgrywają czynniki obciążające i łagodzące w dostosowaniu wysokości kary pieniężnej do konkretnych okoliczności sprawy, nie należy umniejszać roli tych czynników w wyborze właściwego środka naprawczego. W przypadkach, w których ocena oparta na innych kryteriach pozostawia wątpliwości co do stosowności administracyjnej kary pieniężnej zarówno jako samodzielnego środka naprawczego, lub też w połączeniu z innymi środkami na mocy art. 58, owe obciążające lub łagodzące okoliczności mogą pomóc organowi nadzorczemu w dokonaniu wyboru odpowiednich środków, przechylając szalę na korzyść tego, co w danym przypadku okazuje się bardziej skuteczne, proporcjonalne i odstraszające.

Przepis ten ma na celu oszacowanie stopnia odpowiedzialności administratora po wystąpieniu naruszenia. Może on obejmować przypadki, w których administrator / podmiot przetwarzający wyraźnie nie wykazali się lekkomyślną/lekceważącą postawą, ale po stwierdzeniu naruszenia dołożyli wszelkich starań, by naprawić skutki swoich działań.

Wcześniejsze doświadczenia regulacyjne organów nadzorczych ze stosowania dyrektywy 95/46/WE dowiodły, że właściwe może być wykazanie się pewną elastycznością wobec administratorów danych / podmiotów przetwarzających, którzy przyznali się do naruszenia i podjęli działania zmierzające do naprawy lub ograniczenia skutku swoich działań. Działania takie mogą obejmować (choć nie muszą prowadzić do większej elastyczności w każdym przypadku):

- kontaktowanie się z innymi administratorami / podmiotami przetwarzającymi, którzy mogli uczestniczyć w rozszerzeniu zakresu przetwarzania, np. w przypadku gdy doszło do omyłkowego udostępnienia danych stronom trzecim.
- działania podjęte we właściwym czasie przez administratora / podmiot przetwarzający w celu powstrzymania naruszenia lub jego dalszego rozwoju do poziomu lub etapu, na którym owo naruszenie stałoby się znacznie poważniejsze niż pierwotnie.

d) Stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32

Rozporządzenie wprowadziło znacznie wyższy poziom rozliczalności administratora danych w porównaniu z dyrektywą o ochronie danych 95/46/WE.

Stopień odpowiedzialności administratora lub podmiotu przetwarzającego oceniany w kontekście stosowania odpowiedniego środka naprawczego może obejmować następujące kwestie:

- Czy administrator wdrożył środki techniczne zgodne z zasadą uwzględniania ochrony danych w fazie projektowania lub z zasadą domyślnej ochrony danych (art. 25)?
- Czy administrator wdrożył środki organizacyjne, które zapewniają skuteczność zasady uwzględniania ochrony danych w fazie projektowania i zasady domyślnej ochrony danych (art. 25) na wszystkich poziomach organizacji?
- Czy administrator / podmiot przetwarzający zapewnił odpowiedni poziom bezpieczeństwa (art. 32)?
- Czy na odpowiednim poziomie zarządzania w organizacji są znane i stosowane właściwe procedury/polityki ochrony danych (art. 24)?

Przepisy art. 25 i 32 rozporządzenia wymagają, by administratorzy „*uwzględnili stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania*”. Zamiast ustanowienia obowiązku celu, przepisy te

wprowadzają raczej obowiązek zapewnienia środków, tzn. administrator musi dokonać niezbędnych ocen i wyciągnąć odpowiednie wnioski. Następnie organ nadzorczy musi odpowiedzieć na pytanie, w jakim stopniu administrator „zrobił wszystko, czego można by było oczekiwać", zważywszy na charakter, cele lub zakres przetwarzania oraz w świetle obowiązków nałożonych na niego przez rozporządzenie.

W ocenie tej należy odpowiednio uwzględnić wszelkie sposoby postępowania lub metody opierające się na „najlepszych praktykach", jeżeli takie istnieją i mają zastosowanie. Należy wziąć pod uwagę normy branżowe, a także kodeksy postępowania w danej dziedzinie lub zawodzie. Kodeksy postępowania mogą wskazywać na to, co jest powszechną praktyką w danej dziedzinie, oraz jaki jest poziom wiedzy na temat różnych środków rozwiązywania typowych problemów bezpieczeństwa związanych z przetwarzaniem.

Chociaż zwykle idealnym działaniem jest naśladowanie najlepszych praktyk, to przy dokonywaniu oceny stopnia odpowiedzialności należy brać pod uwagę szczególne okoliczności danej sprawy.

e) Wszelkie istotne wcześniejsze naruszenia, których dopuścił się administrator lub podmiot przetwarzający

To kryterium ma na celu ocenę dotychczasowego przebiegu działalności podmiotu dopuszczającego się naruszenia. Organy nadzorcze powinny wziąć pod uwagę fakt, że zakres takiej oceny może być dość szeroki, gdyż każdy rodzaj naruszenia rozporządzenia, nawet jeśli jest inny niż ten, który jest obecnie badany przez organ nadzorczy, może być „istotny" dla oceny, ponieważ mógłby wskazywać na ogólny poziom niewystarczającej wiedzy lub lekceważenie zasad ochrony danych.

Organ nadzorczy powinien ocenić:

- Czy administrator / podmiot przetwarzający dopuścił się wcześniej tego samego naruszenia?
- Czy administrator / podmiot przetwarzający dopuścił się naruszenia rozporządzenia w ten sam sposób? (np. w wyniku niewystarczającej znajomości istniejących procedur w organizacji lub w wyniku niewłaściwej oceny ryzyka, braku reakcji na wnioski osób, których dane dotyczą, w odpowiednim czasie, nieuzasadnionego opóźnienia w udzielaniu odpowiedzi na wnioski itp.).

f) Stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków

Artykuł 83 ust. 2 stanowi, że należy zwrócić „należytą uwagę" na stopień współpracy podczas podejmowania decyzji na temat ewentualnego nałożenia administracyjnej kary pieniężnej oraz ustalenia jej wysokości. Rozporządzenie nie zawiera precyzyjnej odpowiedzi na pytanie, w jaki sposób uwzględnić starania administratorów lub podmiotów przetwarzających na rzecz usunięcia naruszenia wykrytego przez organ nadzorczy. Ponadto oczywiste jest, że kryteria te stosuje się zwykle przy ustalaniu wysokości kary pieniężnej, jaka zostanie nałożona.

Jednakże w przypadku gdy interwencja administratora spowodowała brak negatywnych konsekwencji dla praw danych osób lub bardziej ograniczony wpływ tych konsekwencji niż mogłoby to mieć miejsce, można to również uwzględnić przy wyborze środka naprawczego, który będzie proporcjonalny w konkretnej sprawie.

Jednym z przykładów sprawy, w którym warto rozważyć współpracę z organem nadzorczym, może być następująca sytuacja:

- Czy podmiot zareagował w określony sposób na wnioski organu nadzorczego w fazie dochodzenia w tej konkretnej sprawie, co w rezultacie znacznie ograniczyło wpływ na prawa danych osób?

Należy równocześnie zaznaczyć, że niestosowne byłoby dodatkowe podnoszenie kwestii współpracy, która jest już wymagana przepisami prawa, np. podmiot jest zobowiązany w każdym przypadku do zapewnienia organowi nadzorczemu dostępu do pomieszczeń w celu przeprowadzenia audytów/inspekcji.

g) Kategorie danych osobowych, których dotyczyło naruszenie

Oto kilka przykładów kluczowych pytań, na które organ nadzorczy — w stosownych przypadkach — może uznać za konieczne udzielić odpowiedzi:

- Czy naruszenie dotyczy przetwarzania szczególnych kategorii danych określonych w art. 9 lub 10 rozporządzenia?
- Czy dane są bezpośrednio/pośrednio możliwe do zidentyfikowania?
- Czy przetwarzanie obejmuje dane, których rozpowszechnienie natychmiast spowodowałoby szkodę/dyskomfort danej osoby (leżące poza zakresem kategorii określonych w art. 9 lub 10)?

- Czy dane są dostępne bezpośrednio bez zabezpieczeń technicznych, czy też są zaszyfrowane[13]?

h) Sposób, w jaki organ nadzorczy dowiedział się o naruszeniu — w szczególności czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosił naruszenie

Organ nadzorczy może dowiedzieć się o naruszeniu w wyniku postępowania, skarg, artykułów w prasie, anonimowych wskazówek lub powiadomienia przez administratora danych. Zgodnie z rozporządzeniem administrator ma obowiązek zawiadomić organ nadzorczy o naruszeniu ochrony danych osobowych. Zwykłe dopełnienie tego obowiązku przez administratora nie może być interpretowane jako czynnik osłabiający/łagodzący. Podobnie administrator / podmiot przetwarzający, który wykazał się niedbałością, gdyż nie dopełnił obowiązku powiadomienia lub co najmniej nie powiadomił o wszystkich szczegółach naruszenia wskutek niepoprawnej oceny rozmiaru naruszenia, może według organu nadzorczego zasłużyć na poważniejszą sankcję — innymi słowy jest mało prawdopodobne, by takie naruszenie zostało uznane za niewielkie.

i) Jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie środki, o których mowa w art. 58 ust. 2 — przestrzeganie tych środków

Po wykryciu wcześniejszego naruszenia administrator lub podmiot przetwarzający mogli być monitorowani przez organ nadzorczy pod kątem przestrzegania tych środków, natomiast do kontaktów z inspektorem ochrony danych, jeśli takowe istniały, prawdopodobnie dochodziło wielokrotnie. Z tego powodu organ nadzorczy uwzględni wcześniejsze kontakty.

W przeciwieństwie do kryteriów określonych w lit. e) niniejsze kryteria oceny mają jedynie na celu przypomnienie organom nadzorczym, by stosowały środki, które same uprzednio wydały wobec tego samego administratora lub podmiotu przetwarzającego „*w tej samej sprawie*".

j) Stosowanie zatwierdzonych kodeksów postępowania na mocy art. 40 lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42

Organy nadzorcze mają obowiązek „*monitorować i egzekwować stosowanie niniejszego rozporządzenia*" (art. 57 ust. 1 lit. a)). Administrator lub podmiot przetwarzający mogą wykazać wywiązywanie się z ciążących na nich obowiązków poprzez stosowanie zatwierdzonych kodeksów postępowania zgodnie z art. 24 ust. 3, art. 28 ust. 5 lub art. 32 ust. 3.

W przypadku naruszenia jednego z przepisów rozporządzenia stosowanie zatwierdzonego kodeksu postępowania może wskazywać na kompleksowość potrzeby interweniowania za pomocą skutecznej, proporcjonalnej i odstraszającej administracyjnej kary pieniężnej lub innego środka naprawczego wyznaczonego przez organ nadzorczy. Zgodnie z art. 40 ust. 4 zatwierdzone kodeksy postępowania przewidują „*mechanizmy pozwalające (monitorującemu) podmiotowi prowadzić obowiązkowe monitorowanie przestrzegania przepisów kodeksu*".

W przypadku gdy administrator lub podmiot przetwarzający zastosował się do zatwierdzonego kodeksu postępowania, organ nadzorczy może być przekonany, że społeczność stosująca kodeks odpowiedzialna za zarządzanie kodeksem sama podejmie odpowiednie działania przeciwko swojemu członkowi, np. za pomocą systemów monitorowania i egzekwowania kodeksu postępowania. Zatem organ nadzorczy może uznać, że takie środki są wystarczająco skuteczne, proporcjonalne lub odstraszające w danym przypadku, bez konieczności nakładania dodatkowych środków przez sam

[13] Nie zawsze należy uważać za „bonusowy" czynnik łagodzący to, że naruszenie dotyczy wyłącznie pośrednio możliwych do zidentyfikowania lub nawet spseudonimizowanych/zaszyfrowanych danych. W przypadku takich naruszeń ogólna ocena pozostałych kryteriów może w sposób umiarkowany lub zdecydowany zasugerować nałożenie kary pieniężnej.

organ nadzorczy. Pewne formy karania niezgodnego z przepisami zachowania można wprowadzić za pomocą schematu monitorowania, zgodnie z art. 41 ust. 2 lit. c) i art. 41 ust. 4, np. poprzez zawieszenie lub wykluczenie administratora lub podmiot przetwarzający spośród stosujących kodeks. Niemniej jednak uprawnienia organu monitorującego pozostają „*bez uszczerbku dla zadań i uprawnień właściwego organu nadzorczego*", innymi słowy organ nadzorczy nie ma obowiązku uwzględnienia wcześniej nałożonych kar dotyczących systemu samoregulacyjnego.

Niestosowanie środków samoregulacyjnych może również ujawniać zaniedbanie administratora / podmiotu przetwarzającego lub umyślne niestosowanie tych środków.

k) Wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty

Sam przepis zawiera przykłady innych elementów, które można uwzględniać przy podejmowaniu decyzji co do stosowności administracyjnej kary pieniężnej nałożonej za naruszenie przepisów, o których mowa w art. 83 ust. 4–6.

Informacje na temat korzyści finansowych uzyskanych w wyniku naruszenia mogą być szczególnie istotne dla organów nadzorczych, gdyż takie korzyści nie mogą być rekompensowane za pomocą środków, które nie mają charakteru pieniężnego. W związku z tym fakt, że administrator osiągnął korzyści z tytułu naruszenia rozporządzenia może stanowić wyraźną przesłankę do zastosowania kary pieniężnej.

IV. Wniosek

Rozważania dotyczące kwestii takich jak te, o których mowa była w poprzedniej sekcji, umożliwią organom nadzorczym zidentyfikowanie — na podstawie odpowiednich okoliczności faktycznych sprawy — kryteriów, które są najbardziej przydatne przy podejmowaniu decyzji dotyczącej ewentualnego nałożenia, oprócz lub zamiast innych środków na mocy art. 58, odpowiedniej administracyjnej kary pieniężnej. Biorąc pod uwagę kontekst takiej oceny, organ nadzorczy określi najbardziej skuteczny, proporcjonalny i odstraszający środek naprawczy w celu zaradzenia naruszeniu.

Artykuł 58 zawiera wytyczne dotyczące rodzaju środków, które organ nadzorczy może zastosować, gdyż same środki naprawcze mają różny charakter i są dostosowane przede wszystkim do osiągnięcia różnych celów. Niektóre ze środków opisanych w art. 58 można nawet łączyć, osiągając tym samym działanie regulacyjne obejmujące więcej niż jeden środek naprawczy.

Nie zawsze jest konieczne uzupełnienie środka innym środkiem naprawczym. Na przykład: Skuteczność i odstraszający charakter interwencji organu nadzorczego przy należytym uwzględnieniu tego, co jest proporcjonalne do tego konkretnego przypadku, można osiągnąć wyłącznie za pomocą kary pieniężnej.

Krótko mówiąc, organy muszą przywrócić zgodność za pomocą wszystkich dostępnych im środków naprawczych. Organy nadzorcze będą miały również obowiązek dokonać wyboru najwłaściwszego sposobu wdrożenia działań regulacyjnych. Przykładowo takim sposobem może być nałożenie sankcji karnych (jeżeli są one dostępne na poziomie krajowym).

Konsekwentne stosowanie administracyjnych kar pieniężnych w całej Unii Europejskiej to rozwijająca się praktyka. Współpracujące ze sobą organy nadzorcze winny podejmować działania zmierzające do ciągłego zapewniania większej spójności w stosowaniu tych kar. Można to osiągnąć dzięki regularnej wymianie doświadczeń w ramach warsztatów szkoleniowych poświęconych rozpatrywaniu spraw lub innym wydarzeniom, które umożliwią porównanie spraw ze szczebla niższego niż krajowy, krajowego i transgranicznego. Zaleca się utworzenie stałej podgrupy powiązanej z odpowiednią częścią Europejskiej Rady Ochrony Danych w celu wspierania tej bieżącej działalności.