

GRUPA ROBOCZA ART. 29 DS. OCHRONY DANYCH

**16/EN
WP 243**

Wytyczne dotyczące inspektorów ochrony danych ('DPO')

Przyjęte w dniu 13 grudnia 2016 r.

Grupa Robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym organem doradczym w zakresie ochrony danych i prywatności. Zadania grupy określone są w art. 30 dyrektywy 95/46/WE oraz art. 15 dyrektywy 2002/58/WE.

Sekretariat zapewnia Dyrekcja C (Prawa Podstawowe i Rządy Prawa) Komisji Europejskiej, Dyrekcja Generalna ds. Sprawiedliwości i Konsumentów, B-1049 Bruksela, Belgia, biuro nr MO59 02/27.

Strona internetowa: http://ec.europa.eu/justice/data-protection/index_en.htm

**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 art. 30 wspomnianej dyrektywy,

uwzględniając swój regulamin wewnętrzny,

PRZYJMUJE NINIEJSZE WYTYCZNE:

Spis treści

1. Wstęp	4
2. Wyznaczenie inspektora ochrony danych	5
2.1 Obowiązkowe wyznaczenie DPO.....	5
2.1.1 „Organ lub podmiot publiczny”	6
2.1.2 „Główna działalność administratora”	6
2.1.3 „Duża skala przetwarzania”	7
2.1.4 „Regularne i systematyczne monitorowanie”	8
2.1.5 Szczególne kategorie danych oraz dane dotyczące wyroków skazujących i naruszeń prawa	9
2.2 DPO dla podmiotu przetwarzającego.....	9
2.3 „Łatwość nawiązania z nim kontaktu z każdej jednostki organizacyjnej”	10
2.4 Poziom wiedzy fachowej i kwalifikacje zawodowe DPO	10
2.5 Publikowanie i zawiadomienie o danych kontaktowych DPO.....	12
3. Pozycja DPO	13
3.1 Udział DPO we wszystkich zagadnieniach związanych z ochroną danych osobowych	13
3.2 Niezbędne zasoby.....	13
3.3 Instrukcje i „wykonywanie zadań w sposób niezależny”	14
3.4 Odwołanie lub kara za wykonywanie zadań DPO	15
3.5 Konflikt interesów	15
4. Zadania DPO	16
4.1 Monitorowanie zgodności z RODO.....	16
4.2 Rola DPO w ocenie skutków dla ochrony danych	16
4.3 Podejście oparte na analizie ryzyka.....	17
4.4 Rola DPO w ewidencjonowaniu	17

1. Wstęp

Ogólne rozporządzenie o ochronie danych („RODO”)¹, które zacznie obowiązywać od 25 maja 2018 r. zapewni zmodernizowane, oparte na rozliczalności ramy ochrony danych osobowych w Europie. Dla wielu organizacji Inspektor ochrony danych („DPO” – Data Protection Officer) będzie ważnym punktem w dostosowaniu do tych ram.

Zgodnie z rozporządzeniem obowiązkiem niektórych administratorów i przetwarzających będzie powołanie DPO.² Taki obowiązek będzie miał miejsce w przypadku wszystkich organów i podmiotów publicznych (niezależnie od zakresu przetwarzanych danych), jak również w stosunku do podmiotów, które w ramach swojej głównej działalności regularnie i na dużą skalę monitorują osoby lub jeżeli działalność podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych.

Nawet jeżeli RODO bezpośrednio nie nakłada obowiązku powołania DPO, niejednokrotnie korzystnym dla podmiotów może być dobrowolne wyznaczenie takiej osoby. GR Art. 29 zachęca do takiego postępowania.

Koncepcja DPO nie jest niczym nowym. Choć dyrektywa 95/46/WE³ nie nakładała na żadnego administratora obowiązku powoływania DPO, to jednak na przestrzeni lat praktyka taka wykształciła się w szeregu państw członkowskich.

Przed przyjęciem RODO, GR Art. 29 stała na stanowisku, że DPO jest warunkiem rozliczalności a powołanie DPO może ułatwić przestrzeganie przepisów jak również przyczynić się do wzrostu konkurencyjności przedsiębiorstwa.⁴ Prócz zapewnienia przestrzegania przepisów poprzez wprowadzenie mechanizmów rozliczania (np. ułatwienie lub przeprowadzania audytów i ocen skutków dla ochrony danych) DPO odgrywają rolę pośredników pomiędzy zainteresowanymi stronami (np. organem ochrony danych osobowych, osobami, których dane dotyczą albo jednostkami w ramach przedsiębiorstwa).

DPO nie ponoszą odpowiedzialności w przypadku niezgodności z RODO. Z rozporządzenia jasno wynika, że to administrator lub podmiot przetwarzający zobowiązany jest do zapewnienia i udowodnienia zgodności przetwarzania danych osobowych z przepisami prawa (artykuł 24(1)). Przetwarzanie danych zgodne z rozporządzeniem jest obowiązkiem administratora lub podmiotu przetwarzającego.

Do obowiązków administratora i podmiotu przetwarzającego należy również umożliwienie efektywnego wykonywania zadań przez DPO. Wyznaczenie DPO jest jedynie pierwszym krokiem,

¹ ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 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)

² Wyznaczenie DPO jest również obowiązkiem właściwych organów na podstawie artykułu 32 Dyrektywy 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłającej decyzję ramową Rady 2008/977/WSiSW (Dz.Urz.UE L 119/89) i krajowych przepisów wykonawczych. Wytyczne tutaj przedstawione mają zastosowanie do RODO, jednak można również je odnieść od przepisów dyrektywy 2016/618.

³ Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. U. UE L 281, 23.11.1995, str. 31).

⁴ http://ec.europa.eu/justice/data-protection/article-29/documentation/otherdocument/files/2015/20150617_appendix_core_issues_plenary_en.pdf

istotne jest również zapewnienie wystarczającej niezależności i środków umożliwiających skuteczne wykonywanie obowiązków.

W świetle RODO DPO ma kluczowe znaczenie w procesie administrowania danymi w związku z czym w rozporządzeniu określono warunki jego powołania, status i opis zadań. Założeniem niniejszych wytycznych jest wyjaśnienie stosownych zapisów RODO celem ułatwienia administratorom i podmiotom przetwarzającym dostosowania się do przepisów prawa, jak również ułatwienia inspektorom ochrony danych wykonywania ich zadań. Wytyczne zawierają również zalecane dobre praktyki, oparte na doświadczeniu niektórych państw członkowskich. GR Art. 29 będzie na bieżąco monitorować implementację wytycznych i w razie zaistnienia potrzeby wzbogacać je o dalsze informacje.

2. Wyznaczenie inspektora ochrony danych

2.1 Obowiązkowe wyznaczenie DPO

Artykuł 37(1) RODO wskazuje na obowiązek wyznaczenia DPO w następujących przypadkach⁵:

1. przetwarzania dokonują organ lub podmiot publiczny⁶;
2. główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę;
3. główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych⁷ albo⁸ danych osobowych dotyczących wyroków skazujących i naruszeń prawa.⁹

W kolejnej części opracowanie GR Art. 29 zawiera wytyczne dotyczące kryteriów i terminów użytych w artykule 37(1).

W sytuacji, gdy z przepisów nie wynika obowiązek wyznaczenia DPO, GR Art. 29 zaleca administratorom i podmiotom przetwarzającym udokumentowanie wewnętrznej procedury przeprowadzonej w celu ustalenia obowiązku bądź braku obowiązku wyznaczenia DPO, celem wykazania, iż stosowne czynniki zostały uwzględnione.¹⁰

W sytuacji, w której podmiot dobrowolnie decyduje się na wyznaczenie DPO, wymagania wskazane w artykule 37 i 39 stosuje się odpowiednio do jego wyznaczenia, statusu i zadań, tak jakby wyznaczenie było obowiązkowe.

Powyższe nie uniemożliwia podmiotom niezainteresowanym dobrowolnym wyznaczeniem DPO i niezobowiązaniem do tego przez prawo wyznaczenia pracownika, albo zatrudnienia zewnętrznego konsultanta do wypełniania zadań związanych z ochroną danych osobowych. W przypadku powołania takiej osoby istotne jest, aby nazwa stanowiska, status pracownika, pozycja i zadania nie

⁵ Zgodnie z art. 37(4) przepisy unijne bądź krajowe mogą wymuszać powołanie DPO w innych okolicznościach.

⁶ Z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości.

⁷ Zgodnie z art. 9 są to dane osobowe ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby.

⁸ Artykuł 37(1)(c) stosuje zwrot i („and”). Wyjaśnienie zastosowania „albo” zamiast „i” w sekcji 2.1.5

⁹ Artykuł 10.

¹⁰ Artykuł 24(1).

wprowadzały w błąd. W związku z tym zaleca się poinformowanie pracowników organizacji, jak również organów ochrony danych, osób, których dane dotyczą, i ogółu społeczeństwa, iż osoba zatrudniona nie jest DPO w świetle przepisów RODO.¹¹

2.1.1 „Organ lub podmiot publiczny”

RODO nie przedstawia definicji pojęcia „organu lub podmiotu publicznego”. GR Art. 29 stoi na stanowisku, że takie pojęcie powinno zostać określone na poziomie przepisów krajowych. Do podmiotów takich najczęściej zalicza się organy władzy krajowej, organy regionalne i lokalne, ale również – na mocy właściwego prawa krajowego - szereg innych podmiotów prawa publicznego.¹² We wszystkich tych przypadkach powołanie DPO będzie obowiązkowe.

Zadanie może być realizowane w interesie publicznym lub może być sprawowana władza publiczna¹³ nie tylko przez organy lub podmioty publiczne, ale również przez inne osoby fizyczne i prawne podlegające prawu publicznemu lub prywatnemu, w sektorach takich jak np. transport publiczny, dostarczanie wody i energii, infrastruktura drogowa, radiofonia i telewizja, budynki użyteczności publicznej albo organy powołane dla zwodów regulowanych.

W tych przypadkach sytuacja osób, których dane dotyczą może być bardzo podobna do sytuacji przetwarzania ich danych przez organy lub podmioty publiczne. W szczególności dane mogą być przetwarzane w podobnych celach, a możliwość wpływu osób, których dane dotyczą, na charakter tego przetwarzania może być ograniczona bądź wyłączona, co może wymagać dodatkowej ochrony, jaką daje powołanie DPO.

Choć w powyższych przypadkach obowiązek powołania DPO nie wynika z RODO, to GR Art. 29 zaleca w ramach dobrych praktyk:

- Powoływanie DPO przez prywatne jednostki realizujące zadania w interesie publicznym lub sprawujące władzę publiczną;
- Działalność DPO powinna obejmować również wszelkie operacje przetwarzania prowadzone przez jednostkę, w tym te niezwiązane z zadaniami realizowanymi w interesie publicznym.

2.1.2 „Główna działalność administratora”

Artykuł 37(1)(b) i (c) RODO zawiera zwrot „główna działalność administratora lub podmiotu przetwarzającego”. Zgodnie z motywem 97 rozporządzenia przetwarzanie danych osobowych jest główną działalnością administratora, jeżeli oznacza jego zasadnicze, a nie poboczne czynności. Tak więc „główną działalnością” będzie działalność kluczowa z punktu widzenia osiągnięcia celów administratora albo podmiotu przetwarzającego dane.

„Głównej działalności” nie należy interpretować w sposób wyłączający działalność w zakresie przetwarzania danych nierozdzielnie związaną z działalnością główną. Dla przykładu działalnością główną szpitali będzie zapewnianie opieki medycznej. Natomiast prowadzenie efektywnej opieki

¹¹ Powyższe ma również zastosowanie do istniejących już administratorów bezpieczeństwa informacji albo innych osób specjalistów z dziedziny ochrony prywatności, którzy nie spełniają wymogów RODO, np. w kontekście niezależnego wykonywania zadań albo niezbędnych zasobów i w związku z tym nie można ich uznać za inspektorów ochrony danych

¹² Zobacz definicje terminów „organ sektora publicznego” i „podmiot prawa publicznego” w artykule 2(1) i (2) w Dyrektywie 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz. U. EU L 345, 31.12.2003, str. 90).

¹³ Artykuł 13(1)(e).

medycznej nie byłoby możliwe bez przetwarzania danych medycznych jak np. historii choroby pacjenta. W związku z tym działalność polegająca na przetwarzaniu historii choroby pacjenta również powinna zostać zaklasyfikowana jako działalność główna. Oznacza to, że szpitale będą miały obowiązek powołania DPO.

Kolejnym przykładem może być spółka świadcząca usługi ochrony mienia, prowadząca monitoring w szeregu prywatnych centrów handlowych i przestrzeni publicznej. Jej działalnością główną jest ochrona, natomiast związane z tym bezpośrednio jest przetwarzanie danych osobowych, co oznacza, że takie spółki również muszą powołać DPO.

Jednocześnie GR Art. 29 jest świadoma, że wszystkie podmioty, spółki i inne organizacje prowadzą określone działania, np. prowadząc listę płac albo korzystając z obsługi IT. Są to niezbędne działania umożliwiające prowadzenie działalności głównej, jednak z racji na ich charakter uznane są za poboczne.

2.1.3 „Duża skala przetwarzania”

Artykuł 37(1) (b) i (c) uzależnia obowiązek powołania DPO od przetwarzania danych osobowych na „dużą skalę”. I choć RODO nie definiuje tego pojęcia, to pewne wskazówki znajdują się w motywie 91 rozporządzenia.¹⁴

Nie jest możliwe wskazanie konkretnej wartości, czy to rozmiaru zbioru danych, czy liczby osób, których dane dotyczą, która determinowałaby „dużą skalę”. Nie wyklucza to sytuacji, w której, wraz z rozwojem praktyki ukształtują się standardy, które umożliwiłyby kwantytatywne określenie „dużej skali” w odniesieniu do określonych rodzajów przetwarzania. GR Art. 29 zamierza wspierać ten proces poprzez rozpowszechnianie przykładów odpowiednich progów dla wyznaczenia DPO.

W każdym razie, GR Art. 29 zaleca uwzględnianie następujących czynników przy określaniu, czy przetwarzanie następuje na „dużą skalę”:

- Liczba osób, których dane dotyczą – konkretna liczba albo procent określonej grupy społeczeństwa;
- Zakres przetwarzanych danych osobowych;
- Okres, przez jaki dane są przetwarzane;
- Zakres geograficzny przetwarzania danych osobowych;

Do przykładów „przetwarzania na dużą skalę” zaliczyć można:

- Przetwarzanie danych pacjentów przez szpital w ramach prowadzonej działalności;
- Przetwarzanie danych osób korzystających ze środków komunikacji miejskiej (np. śledzenie za pośrednictwem ‘kart miejskich’);

¹⁴ Motyw stanowi, że „operacje przetwarzania o dużej skali – które służą przetwarzaniu znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym i które mogą wpłynąć na dużą liczbę osób, których dane dotyczą, oraz które mogą powodować wysokie ryzyko”. Z drugiej strony dalsza treść stanowi, że „Przetwarzanie danych osobowych nie powinno być uznawane za przetwarzanie na dużą skalę, jeżeli dotyczy danych osobowych pacjentów lub klientów i jest dokonywane przez pojedynczego lekarza, innego pracownika służby zdrowia lub prawnika.” I choć motyw przedstawia skrajne przykłady przetwarzania danych (przetwarzanie przez jednego lekarza kontra przetwarzanie danych z całego kraju lub Europy), to istnieje wiele innych sytuacji. Ponadto należy zauważyć, iż ten motyw odnosi się do oceny skutków dla ochrony danych, co może oznaczać, iż niektóre aspekty tego zagadnienia nie będą odnosić się do powoływania DPO w sposób analogiczny.

- Przetwarzanie danych geo-lokalizacyjnych w czasie rzeczywistym przez wyspecjalizowany podmiot na rzecz międzynarodowej sieci fast food do celów statystycznych;
- Przetwarzanie danych klientów przez banki albo ubezpieczycieli w ramach prowadzonej działalności;
- Przetwarzanie danych do celów reklamy behawioralnej przez wyszukiwarki;
- Przetwarzanie danych (dotyczących treści, ruchu, lokalizacji) przez dostawców usług telefonicznych lub internetowych.

Przykłady przetwarzania niemieszczącego się w definicji „dużej skali”:

- Przetwarzanie danych pacjentów – klientów, dokonywane przez pojedynczego lekarza;
- Przetwarzanie danych dotyczących wyroków skazujących lub naruszeń prawa przez adwokata lub radcę prawnego.

2.1.4 „Regularne i systematyczne monitorowanie”

Pojęcie „regularnego i systematycznego monitorowania” osób, których dane dotyczą, nie zostało zdefiniowane w RODO, aczkolwiek o „monitorowaniu zachowania osób, których dane dotyczą, wspomniano w motywie 24¹⁵ i pojęcie to obejmuje wszelkie formy śledzenia i profilowania w sieci, w tym na potrzeby reklam behawioralnych.

Samo pojęcie nie jest jednak ograniczone jedynie do środowiska online i śledzenie w sieci powinno być traktowane jedynie jako jeden z przykładów monitorowania zachowań osób, których dane dotyczą.¹⁶

GR Art. 29 definiuje „regularne” jako jedno lub więcej z następujących pojęć:

- Stałe albo występujące w określonych odstępach czasu przez ustalony okres;
- Cykliczne albo powtarzające się w określonym terminie;
- Odbywające się stale lub okresowo.

GR Art. 29 definiuje „systematyczne” jako jedno lub więcej z następujących pojęć:

- Występujące zgodnie z określonym systemem;
- Zaaranżowane, zorganizowane lub metodyczne;
- Odbywające się w ramach generalnego planu zbierania danych;
- Przeprowadzone w ramach określonej strategii.

Przykłady: obsługa sieci telekomunikacyjnej; świadczenie usług telekomunikacyjnych; przekierowywanie e-mail; profilowanie i ocenianie dla celów oceny ryzyka (na przykład dla celów oceny ryzyka kredytowego, ustanawiania składek ubezpieczeniowych, zapobiegania oszustwom, wykrywania prania pieniędzy); śledzenie lokalizacji, na przykład w aplikacjach telefonicznych; programy lojalnościowe; reklama behawioralna; monitorowanie danych o stanie zdrowia za

¹⁵ „Aby stwierdzić, czy czynność przetwarzania można uznać za „monitorowanie zachowania” osób, których dane dotyczą, należy ustalić, czy osoby fizyczne są obserwowane w Internecie, w tym także czy później potencjalnie stosowane są techniki przetwarzania danych polegające na profilowaniu osoby fizycznej, w szczególności w celu podjęcia decyzji jej dotyczącej lub przeanalizowania lub prognozowania jej osobistych preferencji, zachowań i postaw.”

¹⁶ Warto zaznaczyć, że motyw 24 poświęcony jest eksterytorialnemu zastosowaniu RODO. Dodatkowo należy wskazać, iż istnieje różnica pomiędzy pojęciem „monitorowanie ich zachowania” (artykuł 3(2)(b)) a pojęciem „regularne i systematyczne monitorowanie” z art. 37(1)(b), co może skutkować odmiennym rozumieniem tych dwóch zwrotów.

pośrednictwem urządzeń przenośnych; monitoring wizyjny; urządzenia skomunikowane np. inteligentne liczniki, inteligentne samochody, automatyka domowa, etc.

2.1.5 Szczególne kategorie danych oraz dane dotyczące wyroków skazujących i naruszeń prawa

Artykuł 37(1)(c) dotyczy przetwarzania szczególnych kategorii danych zgodnie z artykułem 9, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa określonych w artykule 10. Chociaż przepis używa słowa "i", nie ma powodu, dla którego obie przesłanki powinny być stosowane jednocześnie. Zastosowanie powinien mieć łącznik „lub”.

2.2 DPO dla podmiotu przetwarzającego

Artykuł 37 w kontekście powołania DPO ma zastosowanie zarówno do administratorów¹⁷, jak i podmiotów przetwarzających dane¹⁸. Zależnie od tego, kto spełnia przesłanki obowiązkowego wyznaczenia DPO, obowiązek wyznaczenia DPO spoczywać może tylko na administratorze albo tylko na podmiocie przetwarzającym bądź na obu jednocześnie. W ostatnim przypadku DPO z obu podmiotów powinni współpracować.

Należy podkreślić, iż nawet jeśli administrator spełnia warunki wyznaczenia DPO, to podmiot przetwarzający na rzecz tego administratora takiego obowiązku mieć nie musi. Wyznaczenie przez niego DPO może jednak być spełnione w ramach dobrej praktyki.

Przykłady:

- Mała rodzinna firma dystrybuująca artykuły gospodarstwa domowego na terenie jednego miasta korzysta z usług podmiotu przetwarzającego, którego podstawowa działalność polega na świadczeniu usług analityki internetowej i pomocy w ukierunkowanej reklamie i marketingu. Działalność firmy rodzinnej oraz jej klienci nie generują przetwarzania danych „na dużą skalę”, biorąc pod uwagę niewielką liczbę klientów i stosunkowo ograniczone działania. Jednakże działania podmiotu przetwarzającego, posiadającego wielu klientów takich jak to małe przedsiębiorstwo, zbiorczo kwalifikują się jako przetwarzanie „na dużą skalę”. W związku z tym podmiot przetwarzający, w przeciwieństwie do lokalnego przedsiębiorstwa, zobowiązany będzie do wyznaczenia DPO.
- Średniej wielkości spółka produkująca glazurę zleca świadczenie opieki zdrowotnej w zakresie medycyny pracy zewnętrznemu podmiotowi przetwarzającemu, który posiada szereg klientów zlecających jej w sposób analogiczny taką usługę. Podmiot przetwarzający jest zobowiązany do wyznaczenia DPO na mocy artykułu 37 (1) (c), jeśli prowadzone przez niego przetwarzanie odbywa się „na dużą skalę”. Natomiast administrator niekoniecznie ma obowiązek wyznaczenia DPO.

¹⁷ Administrator w rozumieniu art. 4(7) oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

¹⁸ Podmiot przetwarzający w rozumieniu art. 4(8) oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

W ramach dobrej praktyki GR Art. 29 zaleca by DPO wyznaczony przez podmiot przetwarzający odpowiedzialny był również za procesy nadzór nad działaniami prowadzonymi przez podmiot przetwarzający, w stosunku do których podmiot posiada status administratora (np. HR, IT, logistyka).

2.3 „Łatwość nawiązania z nim kontaktu z każdej jednostki organizacyjnej”

Artykuł 37(2) stanowi, iż grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych, o ile „można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej”. Pojęcie łatwości kontaktu odnosi się do zadań DPO związanych z komunikacją z osobami, których dane dotyczą¹⁹ i obowiązkami punktu kontaktowego dla organu nadzorczego²⁰, jak również funkcjonowaniem wewnątrz podmiotu, biorąc pod uwagę fakt, iż jednym z zadań DPO jest „informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia”.²¹

W celu zapewnienia możliwości łatwego kontaktu z DPO, czy to wewnętrznym czy zewnętrznym, istotne jest udostępnienie jego danych kontaktowych zgodnie z wymogami rozporządzenia.²²

DPO powinien mieć możliwość sprawnego komunikowania się z osobami, których dane dotyczą²³ i współpracy²⁴ z organem nadzorczym. Oznacza to również, że komunikacja musi odbywać się w języku lub językach używanych przez organy nadzorcze i danych osoby, których dane dotyczą.

Zgodnie z artykułem 37(3) jeden DPO może zostać wyznaczony dla kilku organów lub podmiotów publicznych, po uwzględnieniu ich struktury organizacyjnej i wielkości. Te same ustalenia mają zastosowanie do zasobów i komunikacji. Biorąc pod uwagę fakt, iż DPO posiada wiele zadań, administrator musi mieć pewność, że jeden DPO pozytywnie wypełni swoje obowiązki pomimo wyznaczenia go dla kilku podmiotów i organów publicznych.

Dostępność DPO (fizycznie w miejscu pracy, telefonicznie czy przy wykorzystaniu innych bezpiecznych środków komunikacji) jest kluczowa dla zapewnienia kontaktu z DPO. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań zgodnie z prawem Unii lub państwa członkowskiego (artykuł 38(5)). Obowiązek zachowania tajemnicy/poufności nie uniemożliwia DPO kontaktu z organem nadzorczym i zasięgania jego opinii.

2.4 Poziom wiedzy fachowej i kwalifikacje zawodowe DPO

Zgodnie z art. 37(5) „inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39.” Motyw 97 przewiduje, że

¹⁹ Artykuł 38(4): *Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.*

²⁰ Artykuł 39(1)(e): *Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.*

²¹ Artykuł 39(1)(a).

²² Patrz część 2.5 poniżej.

²³ Artykuł 12(1): *Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka – udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14, oraz prowadzić z nią wszelką komunikację na mocy art. 15–22 i 34 w sprawie przetwarzania.*

²⁴ Artykuł 39(1)(d): *„współpraca z organem nadzorczym”.*

niezbędny poziom wiedzy fachowej należy ustalić w szczególności w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają przetwarzane dane osobowe

- **Poziom wiedzy fachowej**

Wymagany poziom wiedzy fachowej nie jest nigdzie jednoznacznie określony, ale musi być współmierny do charakteru, skomplikowania i ilości danych przetwarzanych w ramach jednostki. Dla przykładu,

w przypadku wyjątkowo skomplikowanych procesów przetwarzania danych osobowych lub w przypadku przetwarzania dużej ilości danych szczególnej kategorii, może być wymagany DPO posiadający wyższy poziom wiedzy. Ponadto inaczej sytuacja przedstawiać się będzie w przypadku podmiotów regularnie przekazujących dane do państw trzecich. W związku z tym wybór DPO powinien być dokonany z zachowaniem należytej staranności i brać pod uwagę charakter przetwarzania danych w ramach jednostki.

- **Kwalifikacje zawodowe**

Choć artykuł 37(5) nie wskazuje konkretnych kwalifikacji zawodowych, jakie należy brać pod uwagę wyznaczając DPO, to jednak istotne jest, by DPO posiadał odpowiednią wiedzę z zakresu krajowych i europejskich przepisów o ochronie danych osobowych i praktyk, jak również dogłębną znajomość RODO. Propagowanie odpowiednich i regularnych szkoleń dla inspektorów ochrony danych przez organy nadzorcze również może być przydatne.

Zalecana jest również wiedza biznesowa i sektorowa dotycząca administratora. DPO powinien również posiadać odpowiednią wiedzę na temat procesów przetwarzania danych, systemów informatycznych oraz zabezpieczeń stosowanych u administratora i jego potrzeb w zakresie ochrony danych.

W przypadku organów i podmiotów publicznych DPO powinien również posiadać wiedzę w zakresie procedur administracyjnych i funkcjonowania jednostki.

- **Możliwość wykonania zadań**

Możliwość wykonywania zadań ciążących na DPO powinna być interpretowana zarówno przez pryzmat cech i kwalifikacji DPO, jak również jego pozycji w strukturach podmiotu. Do cech osobowych zaliczyć można rzetelne podejście i wysoki poziom etyki zawodowej. Priorytetem DPO powinno być zapewnienie przestrzegania rozporządzenia. Wytworzenie polityki ochrony danych osobowych w organizacji zależy w dużej mierze od działalności DPO, do jego obowiązków należeć będzie również wsparcie w implementacji RODO, w tym zasad przetwarzania danych osobowych²⁵, praw osób, których dane dotyczą²⁶, ochrony danych w fazie projektowania oraz domyślnej ochrony danych²⁷, rejestru czynności przetwarzania²⁸, wymogów bezpieczeństwa przetwarzania²⁹ i zgłoszenia naruszeń.³⁰

²⁵ Rozdział II.

²⁶ Rozdział III.

²⁷ Artykuł 25.

²⁸ Artykuł 30.

²⁹ Artykuł 32.

³⁰ Artykuł 33 i 34.

- **Pełnienie funkcji DPO na podstawie umowy o świadczenie usług**

Funkcja DPO może być również pełniona na podstawie umowy o świadczenie usług zawartej z osobą fizyczną lub innym podmiotem spoza organizacji administratora/podmiotu przetwarzającego. W tym ostatnim przypadku konieczne jest, aby każdy członek podmiotu sprawującego funkcję DPO spełniał wszystkie istotne wymogi wskazane w Sekcji 4* RODO (np. konieczne jest, aby każda z osób unikała konfliktu interesów). Równie ważne jest, aby każdą z tych osób objąć ochroną przewidzianą w przepisach RODO (np. aby nie miało miejsca nieuzasadnione rozwiązanie umowy o świadczenie usług w zakresie pełnienia funkcji DPO, ale również aby nie miało miejsca niezgodne z prawem zwolnienie osoby będącej członkiem podmiotu realizującego zadania DPO). Jednocześnie w pracy zespołowej można połączyć indywidualne atuty i umiejętności tak, aby zapewnić wydajniejszą obsługę swoich klientów.

W celu zapewnienia przejrzystości prawnej i dobrej organizacji zalecany jest wyraźny podział zadań w ramach zespołu DPO oraz wyznaczenie jednej osoby jako wiodącej osoby kontaktowej i osoby 'odpowiedzialnej' za każdego klienta. Ponadto generalnie wskazane byłoby określenie tych kwestii w umowie o świadczenie usług.

2.5 Publikowanie i zawiadomienie o danych kontaktowych DPO

Artykuł 37(7) RODO nakłada na administratora lub przetwarzającego obowiązek:

- Opublikowania danych DPO; oraz
- Zawiadomienia właściwego organu nadzorczego o danych kontaktowych DPO.

Celem tego artykułu jest zapewnienie, aby osoby, których dane dotyczą (zarówno wewnątrz jak i spoza organizacji) i organy nadzorcze mogły mieć łatwy, bezpośredni i poufny kontakt z DPO, bez konieczności kontaktowania się z innymi jednostkami podmiotu.

Dane kontaktowe DPO powinny zawierać dane umożliwiające osobom, których dane dotyczą, i organom nadzorczym nawiązanie kontaktu w łatwy sposób (adres korespondencyjny, telefon kontaktowy, dedykowany adres email). Gdy to właściwe, powinny również zostać udostępnione inne środki komunikacji dla ogółu społeczeństwa, np. dedykowania infolinia, formularz kontaktowy z DPO na stronie internetowej organizacji.

I choć artykuł 37(7) nie wymaga publikowania imienia i nazwiska DPO, to taka informacja powinna zostać wskazana w ramach dobrej praktyki. Decyzja o tym, czy w określonych okolicznościach udostępnienie tych danych może być konieczne lub pomocne, zależeć będzie od administratora i DPO.³¹

W ramach dobrej praktyki GR Art. 29 zaleca poinformowanie organu nadzorczego i pracowników organizacji o imieniu, nazwisku i danych kontaktowych DPO. Dane te mogą zostać udostępnione wewnętrznie np. poprzez intranet, w wewnętrznej książce telefonicznej albo w ramach rozpisanej struktury organizacyjnej.

³¹ Warto wskazać, że artykuł 33(3)(b), który wskazuje na zakres informacji, jakie muszą być przekazane organowi nadzorcemu w przypadku stwierdzenia naruszenia ochrony danych osobowych, w przeciwieństwie do artykułu 37(7) wymaga również podania imienia i nazwiska DPO (a nie tylko danych kontaktowych).

* Sekcji 4 Rozdziału IV RODO - przypis tłumacza.

3. Pozycja DPO

3.1 Udział DPO we wszystkich zagadnieniach związanych z ochroną danych osobowych

Artykuł 38 stanowi, iż Administrator oraz podmiot przetwarzający zapewniają, „by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.”

Niezwykle istotne jest, by DPO był zaangażowany od najwcześniejszego etapu we wszystkie kwestie związane z przetwarzaniem danych osobowych. Przy ocenie skutków dla ochrony danych RODO wprost wskazuje na zaangażowanie DPO i stanowi, że administrator powinien konsultować się z DPO przy okazji dokonywania takiej oceny.³² Informowanie DPO w początkowych fazach ułatwi zapewnienie zgodności z RODO i uwzględniania ochrony danych w fazie projektowania. W związku z tym angażowanie DPO powinno być standardową procedurą w organizacji. DPO powinien być postrzegany jako partner w dyskusji i włączany w prace grup roboczych poświęconych procesom związanym z przetwarzaniem danych osobowych w ramach organizacji.

W związku z tym organizacja powinna zapewnić między innymi:

- Udział DPO w spotkaniach przedstawicieli wyższego i średniego szczebla organizacji;
- Uczestnictwo DPO przy podejmowaniu decyzji dotyczących przetwarzania danych osobowych. Niezbędne informacje powinny zostać udostępnione DPO odpowiednio wcześniej, umożliwiając DPO zajęcie stanowiska;
- Stanowisko DPO powinno być zawsze brane pod uwagę. GR Art. 29 zaleca, w ramach dobrych praktyk, dokumentowanie przypadków i powodów postępowania niezgodnego z zaleceniem DPO;
- W przypadku stwierdzenia naruszenia albo innego zdarzenia związanego z danymi osobowymi należy natychmiast skonsultować się z DPO.

W określonych przypadkach administrator lub podmiot przetwarzający powinni stworzyć wytyczne ochrony danych osobowych, które wskazywałyby przypadki wymagające konsultacji z DPO.

3.2 Niezbędne zasoby

Artykuł 38(2) nakłada obowiązek wspierania „inspektora ochrony danych w wypełnianiu przez niego zadań[...], zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.” Następujące aspekty powinny zostać wzięte pod uwagę:

- Wsparcie DPO ze strony kadry kierowniczej (np. na poziomie zarządu);
- Wymiar czasu umożliwiający DPO wykonywanie zadań. Jest to szczególnie istotne w przypadku DPO zatrudnionych w niepełnym wymiarze, albo łączących obowiązki DPO z innymi zadaniami. Wystąpienie sprzecznych priorytetów skutkować mogłoby zaniedbaniem obowiązków DPO. Posiadanie wystarczającej ilości czasu na wypełnianie obowiązków DPO, jest bardzo ważne. Dobrą praktyką byłoby wskazanie czasu, który należy poświęcić na obowiązki DPO, oszacowanie czasu potrzebnego na wypełnienie tych obowiązków, ustalenie priorytetów DPO i stworzenie planu pracy DPO (lub organizacji);

³² Artykuł 5(2).

- Odpowiednie wsparcie finansowe, infrastrukturalne (pomieszczenia, sprzęt, wyposażenie) i kadrowe, gdy to właściwe;
- Oficjalne zakomunikowanie wszystkim pracownikom faktu wyznaczenia DPO, tak aby wiedzieli o jego istnieniu oraz o pełnionych przez niego funkcjach
- Umożliwienie dostępu do innych działów organizacji, np. HR, działu prawnego, IT, ochrony etc., celem stworzenia przepływu informacji między tymi jednostkami a DPO i zapewnienia mu niezbędnego wsparcia;
- Ciągłe szkolenie. DPO powinien mieć możliwość ciągłego aktualizowania wiedzy z zakresu ochrony danych osobowych. Celem powinno być zwiększanie wiedzy DPO i zachęcanie go do udziału w szkoleniach, warsztatach, forach poświęconych ochronie danych etc.;
- W zależności od rozmiaru i struktury organizacji przydatne może być powołanie zespołu inspektora ochrony danych (DPO i jego pracowników). W przypadku powołania takiego zespołu, jego struktura, podział i zakres obowiązków powinny zostać jasno ustalone. Również w przypadku wyznaczenia DPO spoza organizacji, zespół pracowników podmiotu zewnętrznego powołany do wypełniania obowiązków związanych z ochroną danych osobowych może efektywnie wypełniać zadania DPO, gdy wyznaczona zostanie osoba odpowiedzialna za kontakt z klientem.

Co do zasady im bardziej skomplikowane procesy przetwarzania danych, tym więcej środków należy przeznaczyć dla DPO. Ochrona danych musi być skuteczna i wymaga wystarczających zasobów, odpowiednich do zakresu przetwarzanych danych.

3.3 Instrukcje i „wykonywanie zadań w sposób niezależny”

Artykuł 38(3) wyznacza pewien zakres gwarancji, których celem jest umożliwianie DPO wykonywania obowiązków z odpowiednim stopniem niezależności w ramach organizacji. Administrator / podmiot przetwarzający mają w szczególności zapewnić *„by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań.”* Motyw 97 uzupełnia to o stwierdzenie, iż *„inspektorzy ochrony danych – bez względu na to, czy są pracownikami administratora – powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny.”*

Oznacza to, że w ramach wypełniania zadań z art. 39 DPO nie może otrzymywać instrukcji dotyczących sposobu rozpoznania sprawy, środków jakie mają zostać podjęte czy celu jaki powinien zostać osiągnięty, czy też faktu, czy należy skontaktować się z organem nadzorczym. Nie może również zostać zobligowany do przyjęcia określonego stanowiska w sprawie z zakresu prawa ochrony danych, np. określonej wykładni przepisów.

Niezależność DPO nie oznacza jednak, iż DPO posiada uprawnienia decyzyjne wykraczające poza zadania z art. 39.

Administrator i podmiot przetwarzający są odpowiedzialni za przestrzeganie przepisów dotyczących ochrony danych i muszą być w stanie wykazać ich przestrzeganie.³³ W sytuacji podjęcia przez administratora lub podmiot przetwarzający decyzji niezgodnej z przepisami RODO i zaleceniami DPO, DPO powinien mieć możliwość jasnego przedstawienia swojego stanowiska osobom podejmującym decyzję.

³³ Artykuł 5(2).

3.4 Odwołanie lub kara za wykonywanie zadań DPO

Artykuł 38(3) stanowi również, że DPO „*nie jest odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań.*”

Wymóg ten zwiększa niezależność DPO i zapewnia możliwość wykonywania zadań w niezależny i odpowiednio chroniony sposób.

Kary w świetle RODO niedozwolone są tylko w przypadkach, gdy są nałożone w związku z wypełnianiem przez DPO swoich zadań. Dla przykładu, DPO może uznać określone przetwarzanie za wysoce ryzykowne i zalecić administratorowi lub podmiotowi przetwarzającemu, ale administrator lub podmiot przetwarzający nie zgadza się z oceną DPO. W takiej sytuacji DPO nie może zostać odwołany ani karany za udzielenie określonego zalecenia.

Kary mogą przybrać szereg form i mogą być bezpośrednie albo pośrednie. Mogą polegać na braku albo opóźnieniu awansu, utrudnieniu rozwoju zawodowego, ograniczeniu dostępu do korzyści oferowanych pozostałym pracownikom. Nieistotny jest przy tym fakt nałożenia kary, gdyż sama możliwość jej wykonania i obawa z tym związana może być wystarczająca do utrudnienia DPO wykonywania zadań.

Zgodnie z normalnymi regułami, przepisami karnymi i prawa pracy, jak w przypadku każdego innego pracownika, DPO może zostać odwołany w uzasadnionych sytuacjach z przyczyn innych niż wykonywanie obowiązków DPO (np. kradzież, nękanie fizyczne i psychiczne, molestowanie seksualne, ciężkie naruszenie obowiązków).

W tym kontekście RODO nie wyjaśnia jak i kiedy DPO może zostać odwołany i zastąpiony inną osobą. Jednak im stabilniejszy kontrakt i szerszy zakres ochrony przed odwołaniem, tym większa szansa na wykonywanie zadań DPO w sposób niezależny. GR Art. 29 zaleca stosowanie takiej polityki.

3.5 Konflikt interesów

Artykuł 38(6) umożliwia DPO wykonywanie „*innych zadań i obowiązków*”. Dalej w artykule widnieje zapis, iż „*administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.*”

Wymóg niepowodowania konfliktu interesów jest ściśle związany z wymogiem wykonywania zadań w sposób niezależny. I choć DPO mogą posiadać inne zadania i obowiązki to jednak te nie mogą powstania konfliktu interesów. Oznacza to, że DPO nie może zajmować w organizacji stanowiska pociągającego za sobą określanie sposobów i celów przetwarzania danych. Ze względu na indywidualny charakter każdej organizacji ten aspekt powinien być analizowany osobno dla każdego podmiotu.³⁴

Zależnie od rodzaju działalności, rozmiaru i struktury organizacji, dobrą praktyką dla administratorów i podmiotów przetwarzających może być:

- Zidentyfikowanie stanowisk niekompatybilnych z funkcją DPO;
- Opracowanie wewnętrznej polityki uniemożliwiającej godzenie stanowisk będących w konflikcie interesów;
- Opracowanie generalnego dokumentu dotyczącego konfliktu interesów;

³⁴ Jako regułę można uznać, że za powodujące konflikt interesów uważane będą stanowiska kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT), ale również niższe stanowiska, jeśli biorą udział w określaniu celów i sposobów przetwarzania danych.

- Ustalenie, iż nie ma konfliktu interesów w funkcjonowaniu obecnego DPO, celem zwiększenia świadomości na temat tego wymogu;
- Wprowadzenie odpowiednich zabezpieczeń do wewnętrznych zasad organizacji celem zapewnienia, by ogłoszenia o rekrutacji na stanowisko DPO były jasne, precyzyjne i niwelowały ryzyko powstania konfliktu interesów. W tym kontekście należy również pamiętać, że konflikt interesów może przybierać różne formy, w zależności od tego, czy rekrutacja na stanowisko DPO ma charakter wewnętrzny czy zewnętrzny.

4. Zadania DPO

4.1 Monitorowanie zgodności z RODO

Artykuł 39(1)(b) nakłada na DPO między innymi obowiązek monitorowania przestrzegania RODO. Motyw 97 doprecyzowuje, iż „w monitorowaniu wewnętrznego przestrzegania niniejszego rozporządzenia administrator lub podmiot przetwarzający powinni być wspomagani przez osobę dysponującą wiedzą fachową na temat prawa i praktyk w dziedzinie ochrony danych.”

W ramach monitorowania DPO mogą między innymi:

- Zbierać informacje w celu identyfikacji procesów przetwarzania;
- Analizować i sprawdzać zgodność tego przetwarzania;
- Informować, doradzać i rekomendować określone działania administratorowi albo podmiotowi przetwarzającemu.

Monitorowanie nie oznacza odpowiedzialności DPO w przypadkach naruszenia RODO. Z rozporządzenia jasno wynika, iż to administrator, a nie DPO „wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać” (Artykuł 24(1)). Spełnianie wymogów rozporządzenia należy do obowiązków korporacyjnych administratora, a nie DPO.

4.2 Rola DPO w ocenie skutków dla ochrony danych

Zgodnie z artykułem 35(1) do obowiązków administratora, a nie DPO, należy przeprowadzanie w określonych przypadkach oceny skutków dla ochrony danych. Jednak DPO może odgrywać istotną rolę

i wspierać administratora przy przeprowadzaniu takiej oceny. Zgodnie z zasadą ochrony danych w fazie projektowania, artykuł 35(2) nakłada na administratora obowiązek konsultowania się z DPO przy dokonywaniu oceny skutków dla ochrony danych. Natomiast z art. 39(1)(c) wynika obowiązek DPO „udzielania na żądanie zaleceń co do oceny skutków dla ochrony danych”.

GR Art. 29 zaleca administratorowi konsultowanie z DPO m.in. następujących kwestii³⁵:

- faktu, czy należy przeprowadzić ocenę skutków dla ochrony danych;
- metodologii przeprowadzenia oceny skutków dla ochrony danych;
- Faktu, czy należy przeprowadzić wewnętrzną ocenę czy też zlecić ją podmiotowi zewnętrznemu;

³⁵ Artykuł 39(1) w wersji angielskiej stanowi, że „do obowiązków DPO należy co najmniej” („DPO shall have ‘at least’ the following tasks”). W związku z tym nie ma przeciwskażeń by zwiększyć zakres obowiązków DPO albo doprecyzować te wskazane w art. 39(1). [przypis tłumacza - treść przypisu zmieniona z racji na brak dokładnego tłumaczenia art. 39(1) RODO. Polskie tłumaczenie nie zawiera żadnego zwrotu „co najmniej” albo „między innymi”.]

- Zabezpieczeń (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą;
- Prawidłowości przeprowadzonej oceny skutków dla ochrony danych i zgodności jej wyników z RODO (czy należy kontynuować przetwarzanie czy też nie oraz jakie zabezpieczenia należy zastosować).

Jeśli administrator nie zgadza się z zaleceniami DPO, dokumentacja oceny skutków dla ochrony danych powinna zawierać pisemne uzasadnienie nieuwzględnienia tych zaleceń.³⁶

GR Art. 29 rekomenduje by administrator jasno, np. w umowie z DPO, ale również w informacjach przekazywanych pracownikom, kierownikom i innym, wskazać zakres obowiązków DPO w danej organizacji, w szczególności w kontekście przeprowadzania oceny skutków dla ochrony danych.

4.3 Podejście oparte na analizie ryzyka

Artykuł 39(2) nakłada na DPO obowiązek wypełniania swoje zadania „z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.” Ten przepis przywołuje ogólną, zdroworozsądkową zasadę, którą DPO może odnieść do wielu aspektów swojej codziennej pracy. Wymaga od DPO ustalania priorytetów w swojej pracy i koncentrowania się na aspektach pociągających za sobą większe ryzyko. Nie oznacza to, iż dozwolone jest zaniedbywanie kontroli zgodności operacji przetwarzania danych o niższym ryzyku, a jedynie wskazuje słuszność skupienia się, przede wszystkim, na kwestiach o wyższym ryzyku.

To selektywne i pragmatyczne podejście powinno ułatwić DPO doradzenie administratorowi, jaką metodologię należy zastosować przy przeprowadzeniu oceny skutków dla ochrony danych, które obszary powinny zostać poddane wewnętrznemu albo zewnętrznemu audytowi, jakie szkolenia wewnętrzne przeprowadzić dla pracowników lub kierowników odpowiedzialnych za przetwarzanie danych, i na które operacje przetwarzania u przeznaczyć więcej czasu i zasobów.

4.4 Rola DPO w ewidencjonowaniu

Zgodnie z artykułem 30(1) i (2) to do administratora albo podmiotu przetwarzającego należy obowiązek prowadzenia rejestru „czynności przetwarzania danych osobowych, za które odpowiadają” albo „wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora”.

W praktyce często to DPO często tworzy i prowadzi powyższe rejestry w oparciu o dane otrzymane od pozostałych komórek organizacji. Taka procedura została ustalona na mocy wielu obowiązujących przepisów państw członkowskich i przepisów o ochronie danych osobowych mających zastosowanie do instytucji i organów UE.³⁷

Artykuł 39(1) określa minimalną listę zakresu obowiązków DPO. W związku z tym, nic nie stoi na przeszkodzie by to DPO prowadził, w imieniu administratora, rejestr czynności przetwarzania danych. Taki rejestr powinien być uznany za jeden ze sposobów monitorowania przestrzegania RODO, informowania administratora lub podmiotu przetwarzającego i doradzania im.

³⁶ Zgodnie z artykułem 24(1): „Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i **aby móc to wykazać**. Środki te są w razie potrzeby poddawane przeglądowi i uaktualniane.”

³⁷ Artykuł 24(1)(d), Rozporządzenie (WE) 45/2001.

Niezależnie od powyższego, rejestr prowadzony zgodnie z art. 30 powinien umożliwić administratorowi i organowi nadzorczemu (na wniosek) kontrolę wszystkich procesów przetwarzania danych w danej organizacji. Jest zatem warunkiem niezbędnym w celu zapewnienia zgodności i przydatnym narzędziem przy rozliczalności.