GRUPA ROBOCZA ART. 29

16/PL
WP 243 rev.01

Wytyczne dotyczące inspektorów ochrony danych („DPO”)

Przyjęte w dniu 13 grudnia 2016 r.

Ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r.

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

Obsługę sekretariatu zapewnia Dyrekcja C (prawa podstawowe i praworządność) Komisji Europejskiej, Dyrekcja Generalna ds. Sprawiedliwości i Konsumentów, B-1049 Bruksela, Belgia, biuro nr MO59 03/068.

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 30 tej dyrektywy,

uwzględniając swój regulamin wewnętrzny,

PRZYJMUJE NINIEJSZE WYTYCZNE:

Spis treści

1 Wprowadzenie

W ogólnym rozporządzeniu o ochronie danych („RODO”)[1], które ma wejść w życie w dniu 25 maja 2018 r., przewidziano zmodernizowane ramy na rzecz przestrzegania przepisów w zakresie ochrony danych w Europie opierające się na zasadzie rozliczalności. W przypadku wielu organizacji kluczowym elementem tych nowych ram prawnych będą inspektorzy ochrony danych („DPO”) odpowiedzialni za podejmowanie działań ułatwiających przestrzeganie przepisów RODO.

Przepisy RODO nakładają na niektórych administratorów i na niektóre podmioty przetwarzające obowiązek wyznaczenia DPO[2]. Obowiązek ten będzie spoczywał na wszystkich organach i podmiotach publicznych (niezależnie od rodzaju przetwarzanych przez nie danych), a także na innych organizacjach, które – w ramach swojej głównej działalności – zajmują się systematycznym monitorowaniem osób fizycznych na dużą skalę lub przetwarzają szczególne kategorie danych osobowych na dużą skalę.

Organizacje mogą niekiedy dobrowolnie wyznaczyć DPO nawet w przypadku, gdy w RODO nie ustanowiono wymogu wyznaczenia DPO. Grupa Robocza Art. 29 zachęca do podejmowania dobrowolnych wysiłków w tym obszarze.

Koncepcja DPO nie jest nową koncepcją. Choć w dyrektywie 95/46/WE[3] na żadną organizację nie nałożono wymogu wyznaczenia DPO, praktyka wyznaczania DPO wykształciła się mimo to na przestrzeni lat w szeregu państw członkowskich.

Przed przyjęciem RODO Grupa Robocza Art. 29 argumentowała, że DPO pełni kluczową rolę w procesie zapewniania rozliczalności oraz że wyznaczenie DPO może ułatwić przestrzeganie obowiązujących przepisów, zapewniając tym samym przedsiębiorstwom przewagę konkurencyjną[4]. Poza ułatwianiem przestrzegania obowiązujących przepisów poprzez wdrażanie narzędzi rozliczalności (np. usprawnianie procesu przeprowadzania ocen skutków dla ochrony danych i przeprowadzanie lub ułatwianie przeprowadzania audytów) DPO pełnią funkcję pośredników między

[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), (Dz.U. L 119 z 4.5.2016). RODO ma znaczenie dla EOG i będzie miało zastosowanie po jego włączeniu do Porozumienia EOG.

[2] Właściwe organy są również zobowiązane do wyznaczenia DPO zgodnie z art. 32 dyrektywy Parlamentu Europejskiego i Rady (UE) 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 uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89–131) i zgodnie z krajowymi przepisami implementacyjnymi. Choć niniejsze wytyczne koncentrują się na DPO, o których mowa w RODO, mają również zastosowanie w odniesieniu do DPO, o których mowa w dyrektywie 2016/680, z uwagi na podobieństwo przepisów tych dwóch aktów prawnych.

[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. L 281 z 23.11.1995, s. 31).

[4] Zob. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

odpowiednimi zainteresowanymi stronami (np. organami nadzorczymi, osobami, których dane dotyczą, i oddziałami w ramach danej organizacji).

DPO nie ponosi osobistej odpowiedzialności za przypadki naruszenia przepisów RODO. RODO wyraźnie stanowi, że obowiązek zagwarantowania i wykazania, iż przetwarzanie danych odbywa się zgodnie z jego przepisami, spoczywa na administratorze lub podmiocie przetwarzającym (art. 24 ust. 1). Obowiązek zapewnienia zgodności środków w zakresie ochrony danych z przepisami rozporządzenia spoczywa na administratorze lub podmiocie przetwarzającym.

Administrator lub podmiot przetwarzający odgrywają również kluczową rolę w zapewnianiu DPO możliwości skutecznego wywiązywania się z powierzonych mu zadań. Wyznaczenie DPO to zaledwie pierwszy krok, ponieważ DPO należy również zapewnić wystarczający stopień autonomii i wystarczające zasoby, aby mógł on skutecznie wywiązywać się z powierzonych mu zadań.

W RODO uznano kluczową rolę DPO w nowym systemie zarządzania danymi i ustanowiono warunki dotyczące sposobu jego wyznaczania, jego statusu oraz spoczywających na nim obowiązków. Celem niniejszych wytycznych jest wyjaśnienie odpowiednich przepisów RODO, nie tylko aby ułatwić administratorom i podmiotom przetwarzającym przestrzeganie obowiązujących przepisów, ale również aby zapewnić DPO wsparcie w wywiązywaniu się z powierzonych im obowiązków. W wytycznych przedstawiono również zalecenia dotyczące najlepszych praktyk, które opracowano w oparciu o doświadczenia zgromadzone w niektórych państwach członkowskich UE. Grupa Robocza Art. 29 będzie monitorowała wdrażanie niniejszych wytycznych i może w stosownych przypadkach uzupełnić je o dodatkowe informacje.

2 Wyznaczanie DPO

2.1. Obowiązkowe wyznaczenie

Zgodnie z art. 37 ust. 1 RODO DPO należy wyznaczyć w trzech konkretnych przypadkach[5]:

a) jeżeli przetwarzania dokonują organ lub podmiot publiczny[6];
b) jeżeli główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub
c) jeżeli główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych[7] albo[8] danych osobowych dotyczących wyroków skazujących i naruszeń prawa[9].

[5] Należy zwrócić uwagę na fakt, że art. 37 ust. 4 i przepisy obowiązujące w Unii lub w państwach członkowskich mogą wymagać wyznaczenia DPO również w innych sytuacjach.
[6] Z wyjątkiem sądów w ramach sprawowania przez nie wymiaru sprawiedliwości. Zob. art. 32 dyrektywy (UE) 2016/680.
[7] Zgodnie z art. 9 obejmuje to przetwarzanie danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.
[8] W art. 37 ust. 1 lit. c) użyto sformułowania „oraz". Aby uzyskać dodatkowe informacje na temat przyczyn, dla których zdecydowano się zastosować słowo „albo" zamiast słowa „oraz", zob. sekcja 2.1.5.
[9] Art. 10.

W poniższych podsekcjach Grupa Robocza Art. 29 przedstawiła wytyczne dotyczące kryteriów i terminologii zastosowanych w art. 37 ust. 1.

Grupa Robocza Art. 29 zaleca, aby – poza przypadkami, w których dana organizacja z oczywistych względów nie jest zobowiązana wyznaczyć DPO – administratorzy i podmioty przetwarzające dokumentowali przebieg prowadzonej przez siebie analizy wewnętrznej w celu ustalenia, czy w danym przypadku należy wyznaczyć DPO, aby mogli wykazać, że należycie uwzględnili stosowne czynniki[10]. Wspomniana analiza stanowi jeden z elementów procesu dokumentowania zgodnie z zasadą rozliczalności. Organ nadzorczy może zażądać przeprowadzenia tej analizy; ponadto – w stosownych przypadkach – należy ją aktualizować, np. w sytuacji, gdy administratorzy lub podmioty przetwarzające rozpoczną prowadzenie nowego rodzaju działalności lub świadczenie nowych usług, które mogą spełniać kryteria ustanowione w art. 37 ust. 1.

Jeżeli organizacja wyznaczyła DPO na zasadzie dobrowolności, wymogi przewidziane w art. 37–39 będą regulowały kwestie związane z wyznaczeniem takiego DPO, jego statusem i spoczywającymi na nim obowiązkami, tak jak gdyby został on wyznaczony w ramach obowiązku wyznaczenia DPO.

Nic nie stoi na przeszkodzie, aby organizacja, która zgodnie z obowiązującymi przepisami nie jest zobowiązana do wyznaczenia DPO i która nie chce wyznaczyć DPO na zasadzie dobrowolności, zatrudniła pracowników lub konsultantów zewnętrznych i powierzyła im zadania w obszarze ochrony danych osobowych. W takim przypadku należy zadbać o to, by nazwa stanowiska piastowanego przez daną osobę, jej pozycja i zakres powierzonych jej obowiązków nie wzbudzały żadnych wątpliwości. Dlatego też we wszelkich komunikatach publikowanych w ramach przedsiębiorstwa, a także we wszelkich komunikatach adresowanych do organów ochrony danych, osób, których dane dotyczą, i ogólnie rozumianej opinii publicznej, należy jednoznacznie wskazać, że taki pracownik lub konsultant nie pełni funkcji inspektora ochrony danych (DPO)[11].

DPO – niezależnie od tego, czy jego wyznaczenie było obowiązkowe, czy też został on wyznaczony na zasadzie dobrowolności – jest odpowiedzialny za wszystkie operacje przetwarzania prowadzone przez danego administratora lub przez dany podmiot przetwarzający.

2.1.1 „ORGAN LUB PODMIOT PUBLICZNY”

W RODO nie zawarto definicji pojęcia „organ lub podmiot publiczny”. W opinii Grupy Roboczej Art. 29 pojęcie to powinno zostać zdefiniowane w ustawodawstwie krajowym. Za organy i podmioty publiczne uznaje się zatem organy na szczeblu krajowym, regionalnym i lokalnym, ale zgodnie z obowiązującymi przepisami krajowymi pojęcie to obejmuje również zazwyczaj szereg innych podmiotów podlegających przepisom prawa publicznego[12]. W takich przypadkach wyznaczenie DPO jest obowiązkowe.

Zadanie wykonywane w interesie publicznym może być realizowane, a władza publiczna może być sprawowana[13], nie tylko przez organy lub podmioty publiczne, ale również przez inne osoby fizyczne lub prawne podlegające przepisom prawa publicznego lub prywatnego w sektorach takich jak –

[10] Zob. art. 24 ust. 1.

[11] Dotyczy to również głównych urzędników ds. prywatności lub innych osób zawodowo zajmujących się kwestiami związanymi z prywatnością, którzy pracują już w niektórych przedsiębiorstwach i którzy mogą nie spełniać kryteriów ustanowionych w RODO, np. jeżeli chodzi o ilość dostępnych zasobów lub gwarancje niezależności – w takim przypadku nie można uznać ich za DPO ani określać ich tym mianem.

zgodnie z przepisami krajowymi obowiązującymi w poszczególnych państwach członkowskich – sektor usług transportu publicznego, sektor zaopatrzenia w wodę i energię, sektor infrastruktury drogowej, sektor publicznej działalności nadawczej, sektor mieszkalnictwa publicznego lub sektor organów dyscyplinarnych sprawujących nadzór nad prawidłowością wykonywania zawodów regulowanych.

W takich przypadkach osoby, których dane dotyczą, mogą znaleźć się w sytuacji bardzo podobnej do sytuacji, w której dochodziłoby do przetwarzania dotyczących ich danych przez organy lub podmioty publiczne. W szczególności dane można przetwarzać w podobnych celach, a osoby fizyczne niejednokrotnie mają równie niewielki wpływ na to, czy i w jaki sposób ich dane będą przetwarzane, lub wręcz w ogóle nie mają na to wpływu, co z kolei może wiązać się z koniecznością zapewnienia dodatkowej ochrony poprzez wyznaczenie DPO.

Choć wyznaczenie DPO nie jest obowiązkowe w takich przypadkach, Grupa Robocza Art. 29 zaleca, aby organizacje prywatne realizujące zadania wykonywane w interesie publicznym lub sprawujące władzę publiczną wyznaczały DPO na zasadzie dobrej praktyki. Taki DPO jest odpowiedzialny za wszystkie operacje przetwarzania, uwzględniając również operacje, które nie są związane z realizacją zadania wykonywanego w interesie publicznym ani z pełnieniem obowiązków urzędowych (np. zarządzanie bazą danych pracowników).

2.1.2 „GŁÓWNA DZIAŁALNOŚĆ"

W art. 37 ust. 1 lit. b) i c) RODO wspomina się o „głównej działalności administratora lub podmiotu przetwarzającego". W motywie 97 doprecyzowano, że „przetwarzanie danych osobowych jest główną działalnością administratora, jeżeli oznacza jego zasadnicze, a nie poboczne czynności". „Główna działalność" oznacza kluczowe operacje, które administrator lub podmiot przetwarzający muszą podjąć, aby osiągnąć swoje cele.

Pojęcie „główna działalność" nie powinno jednak być interpretowane jako wykluczające czynności, w przypadku których przetwarzanie danych stanowi nieodłączny element działalności prowadzonej przez administratora lub podmiot przetwarzający. Na przykład główną działalnością szpitala jest świadczenie usług w zakresie opieki zdrowotnej. Szpital nie mógłby jednak świadczyć tych usług w bezpieczny i skuteczny sposób, gdyby nie przetwarzał danych dotyczących zdrowia, takich jak dokumentacja medyczna pacjentów. Z tego względu przetwarzanie takich danych powinno zostać uznane za jeden z elementów głównej działalności każdego szpitala, co oznacza, że szpitale są zobowiązane wyznaczyć DPO.

Inny przykład, jaki można przywołać w tym miejscu, dotyczy prywatnej firmy ochroniarskiej zajmującej się sprawowaniem nadzoru nad szeregiem prywatnych centrów handlowych i obiektów publicznych. Sprawowanie nadzoru stanowi główną działalność tego przedsiębiorstwa, której wykonywanie nieodłącznie wiąże się z koniecznością przetwarzania danych osobowych. Dlatego też również to przedsiębiorstwo musi wyznaczyć DPO.

---

[12] Zob. np. definicje terminów „organ sektora publicznego" i „podmiot prawa publicznego" zawarte w art. 2 pkt 1 i 2 dyrektywy 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz.U. L 345 z 31.12.2003, s. 90).

[13] Art. 6 ust. 1 lit. e).

Wszystkie organizacje podejmują natomiast określonego rodzaju działania, na przykład przy wypłacaniu wynagrodzeń swoim pracownikom lub przy podejmowaniu standardowych czynności w zakresie wsparcia IT. Są to przykłady funkcji wspierających, które mają kluczowe znaczenie dla głównej działalności lub głównego obszaru zainteresowań danej organizacji. Choć działania w tym zakresie są niezbędne i kluczowe, zazwyczaj uznaje się je za działania pomocnicze, a nie za element głównej działalności.

2.1.3 „NA DUŻĄ SKALĘ"

Zgodnie z art. 37 ust. 1 lit. b) i c) obowiązek wyznaczenia DPO pojawia się w przypadku, gdy przetwarzanie danych osobowych ma odbywać się na dużą skalę. W RODO nie zawarto definicji pojęcia „przetwarzanie na dużą skalę", choć w motywie 91 przedstawiono pewne wskazówki w tym zakresie[14].

Przedstawienie precyzyjnych danych liczbowych dotyczących ilości przetwarzanych danych albo liczby zainteresowanych osób, które można byłoby zastosować we wszystkich sytuacjach, nie jest możliwe. Nie wyklucza to jednak możliwości wypracowania – w miarę upływu czasu – standardowej praktyki umożliwiającej bardziej precyzyjne lub w większym stopniu zorientowane ilościowo identyfikowanie elementów, które można uznać za świadczące o działaniu „na dużą skalę", w różnego rodzaju powszechnych czynnościach przetwarzania. Grupa Robocza Art. 29 również planuje wnieść wkład w działania w tym zakresie, udostępniając i publikując przykłady odpowiednich progów, po przekroczeniu których powstaje obowiązek wyznaczenia DPO.

W każdym razie Grupa Robocza Art. 29 zaleca, aby przy ustalaniu, czy przetwarzanie danych odbywa się na dużą skalę, wziąć pod uwagę w szczególności następujące czynniki:

- liczbę osób, których dane dotyczą – wyrażoną jako konkretna wartość albo jako odsetek populacji odniesienia;
- ilość danych lub zakres poszczególnych przetwarzanych pozycji danych;
- czas trwania lub trwałość czynności przetwarzania danych;
- zakres geograficzny czynności przetwarzania.

[14] Zgodnie z treścią tego motywu pojęcie to obejmowałoby w szczególności „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". W motywie tym stwierdzono natomiast wprost, 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". Należy zwrócić uwagę na fakt, że choć w motywie przedstawiono skrajne przykłady (tj. zestawiono przetwarzanie danych przez pojedynczego lekarza z przetwarzaniem danych na szczeblu całego państwa lub całej Europy), między tymi dwiema skrajnymi sytuacjami występuje wiele mniej jednoznacznych przypadków. Ponadto należy pamiętać, że przywołany motyw dotyczy ocen skutków dla ochrony danych. Oznacza to, że niektóre z wymienionych w nim elementów mogą być specyficzne dla tego kontekstu, dlatego też proces wyznaczania DPO niekoniecznie musi przebiegać w dokładnie taki sam sposób.

Przykłady przetwarzania na dużą skalę obejmują:

- przetwarzanie danych pacjentów przez szpital w ramach prowadzonej przez niego działalności;
- przetwarzanie danych o podróży osób fizycznych korzystających z miejskiego systemu transportu publicznego (np. śledzenie za pośrednictwem biletów elektronicznych);
- przetwarzanie danych określających położenie geograficzne klientów międzynarodowej sieci restauracji typu fast-food w czasie rzeczywistym do celów statystycznych przez podmiot przetwarzający specjalizujący się w świadczeniu tego typu usług;
- przetwarzanie danych klientów przez zakład ubezpieczeń lub bank w ramach prowadzonej przez te podmioty działalności gospodarczej;
- przetwarzanie danych osobowych przez wyszukiwarkę internetową na potrzeby reklamy behawioralnej;
- przetwarzanie danych (treść, przepływ danych, lokalizacja) przez dostawców usług telefonicznych lub internetowych.

Przykłady działań, które nie stanowią przetwarzania na dużą skalę:

- przetwarzanie danych pacjenta przez pojedynczego lekarza;
- przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa przez pojedynczego prawnika.

2.1.4 „REGULARNE I SYSTEMATYCZNE MONITOROWANIE"

Choć pojęcie regularnego i systematycznego monitorowania osób, których dane dotyczą, nie zostało zdefiniowane w RODO, w motywie 24 wspomniano o pojęciu „monitorowania zachowania osób, których dane dotyczą"[15], które w oczywisty sposób obejmuje wszystkie formy śledzenia i profilowania w internecie na potrzeby reklamy behawioralnej.

Pojęcie monitorowania nie ogranicza się jednak wyłącznie do aktywności prowadzonej w internecie, a zjawisko śledzenia w internecie należy traktować wyłącznie jako przykładową metodę monitorowania zachowania osób, których dane dotyczą[16].

Zgodnie z wykładnią dokonaną przez Grupę Roboczą Art. 29, aby dane działanie można było uznać za „regularne", musi ono posiadać przynajmniej jedną z następujących cech:

- być aktualnie w toku lub być podejmowane w regularnych odstępach czasu w danym okresie;
- być prowadzone cyklicznie lub powtarzać się w określonych momentach;
- być prowadzone stale lub okresowo.

[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] Należy zwrócić uwagę na fakt, że motyw 24 dotyczy transgranicznego stosowania RODO. Ponadto istnieje również różnica między brzmieniem terminu „monitorowanie ich zachowania" (art. 3 ust. 2 lit. b)) a brzmieniem terminu „regularne i systematyczne monitorowanie osób, których dane dotyczą" (art. 37 ust. 1 lit. b)), co może być postrzegane jako przesłanka świadcząca o tym, że wspomniane dwa terminy odnoszą się do różnych pojęć.

Zgodnie z wykładnią dokonaną przez Grupę Roboczą Art. 29, aby dane działanie można było uznać za „systematyczne", musi ono posiadać przynajmniej jedną z następujących cech:

- być przeprowadzane w ramach określonego systemu;
- być wcześniej zaplanowane, zorganizowane lub mieć metodyczny charakter;
- odbywać się w ramach ogólnego planu gromadzenia danych;
- być realizowane jako część strategii.

Przykłady działań, które można uznać za działania stanowiące regularne i systematyczne monitorowanie osób, których dane dotyczą: obsługa sieci telekomunikacyjnej; świadczenie usług telekomunikacyjnych; przekierowywanie wiadomości e-mail; działalność marketingowa oparta na danych; profilowanie i przyznawanie punktów na potrzeby oceny ryzyka (np. na potrzeby punktowej oceny kredytowej, ustanowienia składek ubezpieczeniowych, zwalczania nadużyć finansowych i wykrywania przypadków prania pieniędzy); śledzenie zmian lokalizacji, na przykład za pomocą aplikacji mobilnych; programy lojalnościowe; reklama behawioralna; monitorowanie samopoczucia, parametrów fizycznych i danych dotyczących zdrowia za pomocą urządzeń do noszenia na ciele; telewizja przemysłowa; urządzenia podłączone do internetu, np. inteligentne liczniki, inteligentne samochody, urządzenia związane z technologią automatyki domowej itp.

2.1.5 SZCZEGÓLNE KATEGORIE DANYCH I DANE DOTYCZĄCE WYROKÓW SKAZUJĄCYCH I NARUSZEŃ PRAWA

Art. 37 ust. 1 lit. c) dotyczy przetwarzania szczególnych kategorii danych osobowych, o których mowa w art. 9, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o których mowa w art. 10. Choć w literze tej pojawia się słowo „oraz", nie istnieje żadne uzasadnienie polityczne przemawiające za jednoczesnym stosowaniem tych dwóch kryteriów. Dlatego też przepis ten należy interpretować w taki sposób, jak gdyby zawierał sformułowanie „albo".

2.2. DPO podmiotu przetwarzającego

Przepisy art. 37 mają zastosowanie zarówno do administratorów[17], jak i do podmiotów przetwarzających[18], w kontekście wyznaczania DPO. W niektórych przypadkach obowiązek wyznaczenia DPO spoczywa wyłącznie na administratorze lub wyłącznie na podmiocie przetwarzającym, natomiast w innych przypadkach obowiązek ten spoczywa na obydwu z nich (w takiej sytuacji powinni oni współpracować ze sobą), w zależności od tego, który z tych podmiotów spełnia kryteria obowiązkowego wyznaczenia DPO.

Należy zwrócić uwagę na fakt, że nawet w przypadku, gdy administrator spełnia kryteria obowiązkowego wyznaczenia, obowiązek ten niekoniecznie musi rozciągać się również na jego podmiot przetwarzający. Nałożenie na podmiot przetwarzający obowiązku wyznaczenia DPO w takim przypadku można jednak uznać za dobrą praktykę.

Przykłady:

- Niewielkie przedsiębiorstwo rodzinne zajmujące się dystrybucją urządzeń gospodarstwa domowego w jednej miejscowości korzysta z usług podmiotu przetwarzającego, którego główna działalność polega na świadczeniu internetowych usług analitycznych oraz udzielaniu wsparcia w zakresie reklamy ukierunkowanej i marketingu ukierunkowanego. Działalność prowadzona przez przedsiębiorstwo rodzinne i klientów tego przedsiębiorstwa nie wiąże się z przetwarzaniem danych „na dużą skalę" z uwagi na niewielką liczbę klientów i stosunkowo ograniczony zakres prowadzonej przez nich działalności. Jednak działalność prowadzona przez podmiot przetwarzający, który posiada wielu klientów podobnych do tego małego przedsiębiorstwa, w łącznym ujęciu kwalifikuje się do uznania jej za wiążącą się z przetwarzaniem danych na dużą skalę. Podmiot przetwarzający musi zatem wyznaczyć DPO zgodnie z art. 37 ust. 1 lit. b). Jednocześnie samo przedsiębiorstwo rodzinne nie jest zobowiązane do wyznaczenia DPO.

- Średniej wielkości zakład produkcyjny zleca podwykonawstwo w zakresie usług opieki zdrowotnej w miejscu pracy zewnętrznemu podmiotowi przetwarzającemu, który posiada wielu podobnych klientów. Zgodnie z przepisami art. 37 ust. 1 lit. c) wspomniany podmiot przetwarzający jest zobowiązany wyznaczyć DPO, jeżeli przetwarza dane na dużą skalę. Sam zakład produkcyjny nie musi być jednak zobowiązany do wyznaczenia DPO.

DPO wyznaczony przez podmiot przetwarzający nadzoruje również działalność prowadzoną przez organizację podmiotu przetwarzającego w sytuacji, w której organizacja ta sama występuje w roli administratora danych (np. kwestie kadrowe, kwestie związane z IT, kwestie logistyczne).

2.3. Wyznaczenie jednego DPO dla szeregu organizacji

Zgodnie z art. 37 ust. 2 grupa przedsiębiorstw może wyznaczyć jednego DPO, o ile można będzie „łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej". Pojęcie „dostępność" odnosi się do

[17] Zgodnie z definicją przedstawioną w art. 4 pkt 7 administrator oznacza osobę lub podmiot, który ustala cele i sposoby przetwarzania.

[18] Zgodnie z definicją przedstawioną w art. 4 pkt 8 podmiot przetwarzający oznacza osobę lub podmiot, który przetwarza dane w imieniu administratora.

zadań DPO pełniącego funkcję punktu kontaktowego w odniesieniu do osób, których dane dotyczą[19], i organu nadzorczego[20], ale także – wewnętrznie – w ramach organizacji, biorąc pod uwagę fakt, że jedno z zadań DPO polega na „informowaniu administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia”[21].

Aby zapewnić dostępność DPO – niezależnie od tego, czy pełni on funkcję wewnętrzną czy zewnętrzną – należy upewnić się, że dane kontaktowe tego DPO zostały udostępnione zgodnie z wymogami RODO[22].

DPO musi mieć możliwość sprawnego komunikowania się z osobami, których dane dotyczą[23], oraz prowadzenia skutecznej współpracy[24] z odpowiednimi organami nadzorczymi, w razie potrzeby z pomocą zespołu. Oznacza to również, że komunikacja musi odbywać się w języku lub językach wykorzystywanych przez organy nadzorcze i odpowiednie osoby, których dane dotyczą. Dostępność DPO (niezależnie od tego, czy przebywa on w tym samym miejscu co pracownicy, czy też pracuje za pośrednictwem gorącej linii lub innego zabezpieczonego sposobu komunikacji) ma kluczowe znaczenie dla zagwarantowania osobom, których dane dotyczą, możliwości nawiązania kontaktu z DPO.

Zgodnie z art. 37 ust. 3 dla kilku organów lub podmiotów publicznych można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego DPO. W takim przypadku obowiązują analogiczne zasady dotyczące zasobów i komunikowania. Biorąc pod uwagę fakt, że DPO jest odpowiedzialny za wykonywanie różnego rodzaju zadań, administrator lub podmiot przetwarzający musi zapewnić, aby pojedynczy DPO – w stosownych przypadkach przy wsparciu zespołu – był w stanie skutecznie wykonywać te zadania pomimo tego, że wyznaczono go dla szeregu organów i podmiotów publicznych.

2.4. Dostępność i lokalizacja DPO

[19] Art. 38 ust. 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] Art. 39 ust. 1 lit. 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 wszystkich innych sprawach”.

[21] Art. 39 ust. 1 lit. a).

[22] Zob. również sekcja 2.6 poniżej.

[23] Art. 12 ust. 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] Art. 39 ust. 1 lit. d): „współpraca z organem nadzorczym”.

Zgodnie z sekcją 4 RODO należy zapewnić dostępność DPO.

Aby zagwarantować dostępność DPO, Grupa Robocza Art. 29 zaleca, aby DPO znajdował się na terytorium Unii Europejskiej, niezależnie od tego, czy administrator lub podmiot przetwarzający ma swoją jednostkę organizacyjną w Unii Europejskiej.

Nie można jednak wykluczyć, że w niektórych przypadkach, w których administrator lub podmiot przetwarzający nie ma swojej jednostki organizacyjnej na terytorium Unii Europejskiej[25], DPO może skuteczniej wywiązywać się z powierzonych mu obowiązków w przypadku, gdy będzie znajdował się poza UE.

2.5. Wiedza fachowa i umiejętności DPO

Art. 37 ust. 5 stanowi, że DPO „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 stanowi, że 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 został precyzyjnie określony, ale musi odpowiadać on wrażliwości, złożoności i ilości danych przetwarzanych przez organizację. Na przykład, jeżeli dana czynność przetwarzania danych jest szczególnie złożona lub jeżeli zachodzi konieczność przetworzenia dużej ilości danych wrażliwych, DPO może potrzebować dodatkowej wiedzy fachowej i wsparcia. Znaczenie ma również to, czy dana organizacja systematycznie przekazuje dane osobowe poza Unię Europejską, czy też do przekazywania danych osobowych poza obszar UE dochodzi sporadycznie. Dlatego też DPO należy wybrać starannie, po należytym uwzględnieniu kwestii związanych z ochroną danych w danej organizacji.

- **Kwalifikacje zawodowe**

Choć w art. 37 ust. 5 nie określono kwalifikacji zawodowych, które należy wziąć pod uwagę przy wyznaczaniu DPO, DPO powinien posiadać wiedzę fachową w zakresie krajowych i europejskich przepisów i praktyk w dziedzinie ochrony danych, w tym dogłębną znajomość RODO. Promowanie odpowiednich i regularnych szkoleń dla DPO przez organy nadzorcze również może być przydatne.

Przydatna jest również wiedza na temat sektora, w którym prowadzona jest działalność gospodarcza, i organizacji administratora. DPO powinien również posiadać odpowiednią wiedzę na temat przeprowadzanych operacji przetwarzania danych, systemów informatycznych oraz potrzeb administratora w zakresie bezpieczeństwa danych i ochrony danych.

W przypadku organu lub podmiotu publicznego DPO powinien również posiadać gruntowną wiedzę w zakresie przepisów i procedur administracyjnych stosowanych w organizacji.

[25] Zob. art. 3 RODO dotyczący terytorialnego zakresu stosowania.

- **Umiejętność wykonania zadań**

Umiejętność wykonania zadań spoczywających na DPO należy interpretować zarówno przez pryzmat cech osobowych i wiedzy DPO, jak również jego pozycji w strukturach organizacji. Do cech osobowych zaliczyć można np. rzetelne podejście i wysoki poziom etyki zawodowej; priorytetem DPO powinno być zapewnienie przestrzegania RODO. DPO odgrywa kluczową rolę w promowaniu kultury ochrony danych w organizacji i pomaga we wdrażaniu podstawowych elementów RODO, w tym zasad przetwarzania danych[26], praw osób, których dane dotyczą[27], zasad uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych[28], rejestrów czynności przetwarzania[29], bezpieczeństwa przetwarzania[30] oraz zgłaszania i informowania o przypadkach naruszenia ochrony danych[31].

- **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. Gdy umowę zawarto z podmiotem przetwarzającym, istotne jest, aby każdy członek organizacji sprawującej funkcję DPO spełniał wszystkie odpowiednie wymogi wskazane w sekcji 4 RODO (np. istotne jest, aby żaden z członków nie miał 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 organizacji realizującej zadania DPO). Jednocześnie w pracy zespołowej można połączyć indywidualne atuty i umiejętności tak, aby zapewnić wydajniejszą obsługę swoich klientów.

W celu zapewnienia jasności prawa, dobrej organizacji i uniknięcia konfliktów interesów wśród członków zespołu zalecane jest wyraźne podzielenie obowiązków w ramach zespołu DPO oraz wyznaczenie jednej osoby jako wiodącej osoby kontaktowej i osoby „odpowiedzialnej" za każdego klienta. Z reguły wskazane byłoby również określenie tych kwestii w umowie o świadczenie usług.

2.6. Publikowanie danych kontaktowych DPO i zawiadamianie o tych danych

Zgodnie z art. 37 ust. 7 RODO administrator lub podmiot przetwarzający jest zobowiązany do:

- opublikowania danych kontaktowych DPO oraz
- zawiadomienia właściwych organów nadzorczych o danych kontaktowych DPO.

Celem tych wymogów jest zapewnienie, aby osoby, których dane dotyczą, (zarówno wewnątrz, jak i spoza organizacji) i organy nadzorcze mogły mieć łatwy i bezpośredni kontakt z DPO, bez konieczności kontaktowania się z innymi podmiotami organizacji. Poufność jest równie istotna: na przykład pracownicy mogą niechętnie składać skargi do DPO, jeżeli nie zostanie zagwarantowana poufność ich komunikacji.

[26] Rozdział II.
[27] Rozdział III.
[28] Art. 25.
[29] Art. 30.
[30] Art. 32.
[31] Art. 33 i 34.

DPO związany jest tajemnicą lub poufnością dotyczącą wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego (art. 38 ust. 5).

Dane kontaktowe DPO powinny zawierać informacje umożliwiające osobom, których dane dotyczą, i organom nadzorczym łatwe nawiązanie kontaktu z DPO (adres korespondencyjny, dedykowany numer telefonu lub dedykowany adres e-mail). W stosownych przypadkach, do celów komunikacji ze społeczeństwem, mogą zostać zapewnione również inne środki komunikacji, np. dedykowana gorąca linia lub dedykowany formularz kontaktowy skierowany do DPO na stronie internetowej organizacji.

Zgodnie z art. 37 ust. 7 nie jest konieczne, aby publikowane dane kontaktowe zawierały imię i nazwisko DPO. Podczas gdy wskazanie tych informacji może być dobrą praktyką, to decyzja o tym, czy w określonych okolicznościach udostępnienie tych danych może być konieczne lub pomocne, zależeć będzie od administratora lub podmiotu przetwarzającego i DPO[32].

Przekazanie organowi nadzorczemu imienia i nazwiska DPO jest jednak niezbędne dla sprawowania przez DPO funkcji punktu kontaktowego pomiędzy organizacją a organem nadzorczym (art. 39 ust. 1 lit. e)).

W ramach dobrej praktyki Grupa Robocza Art. 29 zaleca również, aby organizacja podawała swoim pracownikom imię i nazwisko oraz dane kontaktowe DPO. Imię i nazwisko oraz dane kontaktowe DPO mogą zostać udostępnione wewnętrznie, np. poprzez intranet, w wewnętrznej książce telefonicznej oraz w ramach rozpisanej struktury organizacyjnej.

3 Status DPO

3.1. Udział DPO we wszystkich sprawach dotyczących ochrony danych osobowych

[32] Należy zauważyć, że w przeciwieństwie do art. 37 ust. 7 w art. 33 ust. 3 lit. b) opisującym informacje, które należy przekazać organowi nadzorczemu i osobom, których dane dotyczą, w przypadku naruszenia ochrony danych osobowych, wymaga się również podania imienia i nazwiska (a nie tylko danych kontaktowych) DPO, którego zawiadamia się o naruszeniu.

Art. 38 RODO stanowi, że „administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych".

Istotne jest włączanie DPO lub jego zespołu we wszystkie sprawy dotyczące ochrony danych osobowych na jak najwcześniejszym etapie. W odniesieniu do oceny skutków dla ochrony danych w RODO wyraźnie przewidziano udział DPO na wczesnym etapie oraz określono, że dokonując takiej oceny skutków, administrator konsultuje się z inspektorem ochrony danych[33]. Zapewnienie informowania DPO i konsultowania się z nim od samego początku ułatwi przestrzeganie RODO, promowanie podejścia zakładającego uwzględnienie ochrony prywatności w fazie projektowania, a zatem powinno być standardową procedurą w ramach zarządzania organizacją. Ponadto ważne jest, aby DPO był postrzegany w organizacji jako partner w dyskusji i był włączany w prace grup roboczych wykonujących czynności przetwarzania danych w organizacji.

W związku z tym organizacja powinna zapewnić m.in., aby:

- DPO był zapraszany do regularnego udziału w posiedzeniach kadry kierowniczej wyższego i średniego szczebla;
- uczestniczył w podejmowaniu decyzji mających wpływ na ochronę danych. Wszystkie niezbędne informacje należy udostępnić DPO odpowiednio wcześniej, umożliwiając mu zajęcie stanowiska;
- opinia inspektora ochrony danych musi być zawsze należycie uwzględniana. W przypadku braku porozumienia Grupa Robocza Art. 29 zaleca, jako dobrą praktykę, dokumentowanie powodów niezastosowania się do porady inspektora ochrony danych;
- w przypadku stwierdzenia naruszenia ochrony danych lub innego incydentu należy niezwłocznie skonsultować się z DPO.

W razie potrzeby administrator lub podmiot przetwarzający może opracować wytyczne lub programy dotyczące ochrony danych, w których określi kiedy należy skonsultować się z DPO.

3.2. Niezbędne zasoby

W art. 38 ust. 2 RODO na organizację nakłada się obowiązek wspierania DPO „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". W szczególności należy wziąć pod uwagę następujące aspekty:

- aktywne wsparcie DPO ze strony kadry kierowniczej wyższego szczebla przy pełnieniu powierzonej mu funkcji (np. na poziomie zarządu);
- czas wystarczający do tego, by DPO mógł się wywiązać z przydzielonych mu obowiązków. Jest to szczególnie istotne, jeżeli wewnętrzny DPO jest zatrudniony w niepełnym wymiarze czasu pracy lub jeżeli zewnętrzny DPO łączy obowiązki w zakresie ochrony danych z innymi zadaniami. W przeciwnym razie sprzeczne priorytety mogłyby doprowadzić do zaniedbania obowiązków przez DPO. Bardzo ważne jest, aby DPO posiadał wystarczająco dużo czasu na

[33] Art. 35 ust. 2.

wywiązanie się ze swoich obowiązków. Dobrą praktyką jest ustalenie odsetka czasu dla DPO na wywiązanie się z obowiązków, gdy nie jest on zatrudniony w pełnym wymiarze godzin. Dobrą praktyką jest również określenie czasu potrzebnego na wypełnienie obowiązków, odpowiedniej kolejności wykonywania obowiązków DPO oraz sporządzenie planu prac w przypadku DPO (lub organizacji);

- w stosownych przypadkach wsparcie w postaci zasobów finansowych, infrastruktury (pomieszczenia, urządzenia, wyposażenie) oraz pracowników;
- oficjalne powiadomienie wszystkich pracowników o wyznaczeniu DPO w celu zapewnienia, aby wszyscy w organizacji wiedzieli o jego istnieniu i pełnionej przez niego funkcji;
- niezbędny dostęp do innych służb, np. działu zasobów ludzkich, działu prawnego, informatycznego i ochrony itd., aby DPO mógł otrzymywać niezbędne wsparcie, dane wejściowe i informacje;
- doskonalenie zawodowe. DPO musi mieć możliwość ciągłego aktualizowania wiedzy na temat postępów poczynionych w dziedzinie ochrony danych. Celem powinno być ciągłe poszerzanie wiedzy DPO oraz zachęcanie go do udziału w kursach szkoleniowych poświęconych ochronie danych i innych formach doskonalenia zawodowego, takich jak udział w prywatnych forach, warsztatach itp.;
- w zależności od rozmiaru i struktury organizacji konieczne może być powołanie zespołu DPO (DPO i jego pracowników). W takich przypadkach należy jasno określić wewnętrzną strukturę zespołu oraz zadania i obowiązki poszczególnych członków. Podobnie, jeżeli funkcję DPO pełni zewnętrzny usługodawca, zadania DPO może skutecznie wykonywać zespół osób fizycznych pracujących dla tego usługodawcy i działających pod nadzorem wyznaczonej głównej osoby odpowiedzialnej za danego klienta.

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

3.3. Instrukcje oraz „wykonywanie obowiązków i zadań w sposób niezależny”

W art. 38 ust. 3 ustanowiono pewne podstawowe gwarancje, aby umożliwić DPO wykonywanie zadań przy zachowaniu wystarczającego stopnia autonomii w organizacji. W szczególności administratorzy / podmioty przetwarzające muszą zapewnić, by DPO „nie otrzymywał instrukcji dotyczących wykonywania [jego] zadań”. W motywie 97 dodaje się, że DPO – „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 swoich zadań zgodnie z art. 39 DPO nie może otrzymywać instrukcji dotyczących sposobu rozpatrywania sprawy, np. instrukcji dotyczących wyników, jakie należy osiągnąć, sposobu rozpatrywania skargi lub tego, czy należy przeprowadzić konsultacje z organem nadzorczym. Ponadto nie mogą zostać zobligowani do przyjęcia określonego stanowiska w sprawie przepisów dotyczących ochrony danych, np. określonej wykładni przepisów.

Niezależność DPO nie oznacza jednak, że DPO posiada uprawnienia decyzyjne wykraczające poza zadania określone w art. 39.

Administrator lub podmiot przetwarzający pozostają odpowiedzialni za przestrzeganie przepisów dotyczących ochrony danych i muszą być w stanie wykazać, że są one przestrzegane[34]. Jeżeli administrator lub podmiot przetwarzający podejmą decyzje niezgodne z RODO i zaleceniami DPO, DPO powinien mieć możliwość jasnego przedstawienia swojej odrębnej opinii najwyższemu kierownictwu i podmiotom, które podjęły takie decyzje. W tym kontekście art. 38 ust. 3 stanowi, że DPO „bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego". Taka bezpośrednia sprawozdawczość zapewnia kadrze kierowniczej wyższego szczebla (np. zarządowi) wiedzę na temat porad i zaleceń DPO w ramach wypełniania zadania polegającego na informowaniu i doradzaniu administratorowi lub podmiotowi przetwarzającemu. Kolejnym przykładem bezpośredniej sprawozdawczości jest sporządzenie rocznego sprawozdania z działalności DPO i przekazanie go najwyższemu kierownictwu.

3.4. Odwołanie lub kara za wypełnianie zadań DPO

Zgodnie z art. 38 ust. 3 DPO nie powinien być „odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań".

Wymóg ten zwiększa niezależność DPO i pozwala zapewnić im wykonywanie zadań w sposób niezależny oraz pozwala korzystać z odpowiedniej ochrony przy wykonywaniu zadań z zakresu ochrony danych.

Na mocy RODO kary są niedozwolone tylko w przypadkach, gdy są nałożone w związku z wypełnianiem przez DPO swoich zadań. Na przykład DPO może uznać określone przetwarzanie za wysoce ryzykowne i doradzić administratorowi lub podmiotowi przetwarzającemu przeprowadzenie oceny skutków dla ochrony danych, przy czym administrator lub podmiot przetwarzający może nie zgodzić się z oceną DPO. W takiej sytuacji DPO nie może zostać odwołany za udzielenie określonej porady.

Kary mogą przybierać różne formy i mogą mieć charakter bezpośredni lub pośredni. Mogą opierać się np. na braku lub opóźnieniu awansu; utrudnieniu rozwoju zawodowego; odmowie 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, aby utrudnić DPO wykonanie jego zadań.

Zgodnie ze zwykłą zasadą zarządzania, a także podobnie jak w przypadku każdego innego pracownika lub wykonawcy, na podstawie i z zastrzeżeniem mających zastosowanie krajowych przepisów dotyczących zobowiązań, prawa pracy lub przepisów karnych, DPO może zostać odwołany zgodnie z prawem z przyczyn innych niż wykonywanie zadań jako DPO (np. kradzież, nękanie fizyczne i psychiczne lub molestowanie seksualne lub inne podobne wykroczenia).

W tym kontekście należy zauważyć, że w RODO nie określono jak i kiedy DPO może zostać odwołany lub zastąpiony inną osobą. Im stabilniejsza umowa z DPO i szerszy zakres ochrony przed niesprawiedliwym odwołaniem, tym większa szansa, że DPO będzie wykonywał swoje zadania w sposób niezależny. Grupa Robocza Art. 29 zaleca zatem organizacjom stosowanie takiej praktyki.

[34] Art. 5 ust. 2.

3.5. Konflikt interesów

Na mocy art. 38 ust. 6 DPO „może wykonywać inne zadania i obowiązki". Zgodnie z tym artykułem organizacja musi jednak „zapewnić, by takie zadania i obowiązki nie powodowały konfliktu interesów".

Wymóg niepowodowania konfliktu interesów jest ściśle związany z wymogiem wykonywania zadań w sposób niezależny. Chociaż DPO zezwala się na pełnienie innych funkcji, te dodatkowe zadania i obowiązki można im powierzyć tylko wówczas, gdy nie powodują konfliktów interesów. Oznacza to przede wszystkim, że DPO nie może piastować stanowiska w organizacji, które zapewniałoby mu dostęp do informacji pozwalających mu ustalić cele i sposoby przetwarzania danych osobowych. Biorąc pod uwagę specyficzną strukturę organizacyjną poszczególnych organizacji, kwestie te należy rozstrzygać w odniesieniu do indywidualnych przypadków.

Ogólnie rzecz biorąc, stanowiska w organizacji, w przypadku których dochodzi do konfliktu interesów, mogą obejmować stanowiska w strukturze kadry kierowniczej wyższego szczebla (takie jak dyrektor generalny, dyrektor ds. operacyjnych, dyrektor ds. finansowych, dyrektor ds. medycznych, kierownik departamentu marketingu, kierownik działu kadr lub kierownik departamentów IT), ale również inne stanowiska na niższych szczeblach struktury organizacyjnej, jeżeli piastowanie tych stanowisk lub pełnienie tych funkcji zapewnia możliwość ustalenia celów i sposobów przetwarzania. Ponadto konflikt interesów może powstać również wtedy, gdy np. zewnętrzny DPO zostanie poproszony o reprezentowanie administratora lub podmiotu przetwarzającego przed sądem w sprawie dotyczącej ochrony danych.

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

- określenie stanowisk niezgodnych z funkcją DPO;
- opracowanie wewnętrznych zasad pozwalających uniknąć konfliktu interesów;
- zapewnienie bardziej ogólnego wyjaśnienia dotyczącego konfliktów interesów;
- zadeklarowanie, że DPO nie ma konfliktu interesów w odniesieniu do pełnionej przez siebie funkcji DPO, celem zwiększenia świadomości na temat tego wymogu;
- wprowadzenie zabezpieczeń do wewnętrznych zasad organizacji oraz zapewnienie, by ogłoszenie o naborze na stanowisko DPO lub umowa o świadczenie usług były wystarczająco jasne i precyzyjne, aby uniknąć konfliktu interesów. W tym kontekście należy również mieć na uwadze, że konflikty interesów mogą przybierać różne formy w zależności od tego, czy rekrutacja na stanowisko DPO ma charakter wewnętrzny lub zewnętrzny.

4 Zadania DPO

4.1. Monitorowanie przestrzegania RODO

Na mocy art. 39 ust. 1 lit. b) na DPO nakłada się m.in. obowiązek monitorowania przestrzegania RODO. W motywie 97 określono ponadto, że „w monitorowaniu wewnętrznego przestrzegania niniejszego rozporządzenia administrator lub podmiot przetwarzający powinni być wspomagani" przez DPO.

W ramach przedmiotowych obowiązków w zakresie monitorowania przestrzegania DPO może w szczególności:

- gromadzić informacje pozwalające zidentyfikować czynności przetwarzania;
- analizować czynności przetwarzania i sprawdzać ich zgodność z przepisami rozporządzenia;
- przekazywać administratorowi lub podmiotowi przetwarzającemu informacje, udzielać im porad lub publikować skierowane do nich zalecenia.

Monitorowanie przestrzegania nie oznacza, że DPO jest osobiście odpowiedzialny w przypadkach nieprzestrzegania RODO. RODO wyraźnie stanowi, że to administrator, a nie DPO „wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać" (art. 24 ust. 1). Społeczny obowiązek zapewnienia zgodności środków w zakresie ochrony danych z przepisami rozporządzenia spoczywa na administratorze, a nie DPO.

4.2. Rola DPO w ramach oceny skutków dla ochrony danych

Zgodnie z art. 35 ust. 1 przeprowadzanie, w razie potrzeby, oceny skutków dla ochrony danych jest obowiązkiem administratora, a nie DPO. DPO może jednak odegrać bardzo ważną i użyteczną rolę we wspieraniu administratora. Zgodnie z zasadą uwzględnienia ochrony danych w fazie projektowania w art. 35 ust. 2 wyraźnie zobowiązano administratora do „konsultowania się" z DPO podczas prowadzenia oceny skutków dla ochrony danych. Z kolei zgodnie z art. 39 ust. 1 lit. c) obowiązkiem DPO jest „udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35".

Grupa Robocza Art. 29 zaleca, aby administrator zasięgnął opinii DPO m.in. w następujących kwestiach[35]:

- konieczności przeprowadzenia oceny skutków dla ochrony danych;
- metody, jaką należy zastosować przy przeprowadzaniu oceny skutków dla ochrony danych;
- ustalenia, czy ocena skutków dla ochrony danych powinna zostać przeprowadzona wewnątrz przedsiębiorstwa, czy też zlecona podmiotowi zewnętrznemu;
- ustalenia, jakie gwarancje (uwzględniając środki techniczne i organizacyjne) należy zastosować w celu ograniczenia wszelkiego rodzaju zagrożeń dla praw i interesów osób, których dane dotyczą;
- ustalenia, czy ocena skutków dla ochrony danych została przeprowadzona w prawidłowy sposób i czy jej wyniki (wnioski dotyczące tego, czy należy kontynuować przetwarzanie danych, oraz tego, jakie zabezpieczenia należy zastosować) są zgodne z przepisami RODO.

[35] W art. 39 ust. 1 wymieniono zadania DPO i określono, że DPO „ma" następujące zadania. W związku z tym nic nie stoi na przeszkodzie, aby administrator mógł przydzielić DPO zadania inne niż te wyraźnie wspomniane w art. 39 ust. 1 lub aby mógł określić te zadania bardziej szczegółowo.

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

Ponadto Grupa Robocza Art. 29 zaleca, aby administrator jasno wskazał – np. w umowie z DPO, ale również w informacjach przekazywanych pracownikom, kierownikom (i innym zainteresowanym stronom) – dokładny zakres obowiązków DPO, w szczególności w kontekście przeprowadzania oceny skutków dla ochrony danych.

4.3. Współpraca z organem nadzorczym i pełnienie funkcji punktu kontaktowego

Zgodnie z art. 39 ust. 1 lit. d) i e) DPO powinien „współpracować z organem nadzorczym" i „pełnić funkcję 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".

Zadania te odnoszą się do „pomocniczej" roli DPO, o której mowa we wstępie do niniejszych wytycznych. DPO ma pełnić funkcję punktu kontaktowego, by ułatwić organowi nadzorczemu dostęp do dokumentów i informacji w celu wypełnienia zadań, o których mowa w art. 57, oraz wykonywania uprawnień w zakresie prowadzonych postępowań, uprawnień naprawczych, uprawnień w zakresie wydawania zezwoleń oraz uprawnień doradczych, o których mowa w art. 58. Jak już wspomniano powyżej, DPO związany jest tajemnicą lub poufnością dotyczącą wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego (art. 38 ust. 5). Obowiązek zachowania tajemnicy/poufności nie zabrania jednak DPO kontaktowania się z organem nadzorczym i zwracania się do niego po poradę. Art. 39 ust. 1 lit. e) stanowi, że w stosownych przypadkach DPO może konsultować się z organem nadzorczym we wszelkich innych sprawach.

4.4. Podejście oparte na analizie ryzyka

Zgodnie z art. 39 ust. 2 DPO musi wypełniać swoje zadania „z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania".

W artykule tym przywołuje się ogólną, zdroworozsądkową zasadę, którą DPO może odnieść do wielu aspektów swojej codziennej pracy. Wymaga to od DPO ustalenia priorytetów w odniesieniu do prowadzonych działań i skupienia się na aspektach pociągających za sobą większe ryzyko w zakresie ochrony danych. Nie oznacza to, że powinni oni zaniedbywać monitorowanie przestrzegania operacji przetwarzania danych o relatywnie niższym poziomie ryzyka, a jedynie wskazuje, że powinni oni skupić się przede wszystkim na obszarach podwyższonego ryzyka.

To selektywne i pragmatyczne podejście powinno ułatwić DPO udzielanie porad administratorowi w zakresie metodyki, jaką należy zastosować podczas oceny skutków dla ochrony danych, obszarów, które należy objąć wewnętrznym lub zewnętrznym audytem w zakresie ochrony danych,

[36] Art. 24 ust. 1 stanowi, że „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 przeglądom i uaktualniane".

wewnętrznych szkoleń oferowanych pracownikom lub kierownikom odpowiedzialnym za wykonywanie czynności przetwarzania danych oraz operacji przetwarzania, na które trzeba przeznaczyć więcej czasu i zasobów.

4.5. Rola DPO w rejestrowaniu czynności przetwarzania

Zgodnie z art. 30 ust. 1 i 2 to administrator lub podmiot przetwarzający, a nie DPO „prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają" lub „prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora".

W praktyce DPO często tworzą spis inwentarza i prowadzą rejestry czynności przetwarzania w oparciu o dane otrzymane od różnych działów organizacji odpowiedzialnych za przetwarzanie danych osobowych. Taka praktyka została ustalona na mocy wielu obowiązujących przepisów krajowych oraz na mocy przepisów o ochronie danych obowiązujących w instytucjach i organach UE[37].

W art. 39 ust. 1 zawarto minimalny wykaz zadań, które musi wykonać DPO. Nic nie stoi zatem na przeszkodzie, aby administrator lub podmiot przetwarzający powierzył DPO zadanie prowadzenia rejestru operacji przetwarzania pod nadzorem administratora lub podmiotu przetwarzającego. Taki rejestr powinien być traktowany jako jedno z narzędzi zapewniających DPO możliwość wywiązywania się z powierzonych mu zadań w zakresie monitorowania przestrzegania, przekazywania informacji i udzielania porad administratorowi lub podmiotowi przetwarzającemu.

W każdym razie taki rejestr, którego prowadzenia wymaga się na mocy art. 30, należy również uznać za narzędzie umożliwiające administratorowi i organowi nadzorczemu zapoznanie się na żądanie ze wszystkimi działaniami związanymi z przetwarzaniem danych osobowych, jakie prowadzi organizacja. Rejestr stanowi zatem warunek wstępny przestrzegania przepisów, a sam w sobie stanowi skuteczne narzędzie rozliczania.

[37] Art. 24 ust. 1 lit. d) rozporządzenia (WE) nr 45/2001.

5 ZAŁĄCZNIK – WYTYCZNE DOTYCZĄCE DPO: CO TRZEBA WIEDZIEĆ?

Celem niniejszego załącznika jest udzielenie odpowiedzi – w prostej i przejrzystej formie – na niektóre kluczowe pytania, jakie organizacje mogą zadawać w związku z ustanowieniem nowych wymogów w zakresie wyznaczania DPO w ogólnym rozporządzeniu o ochronie danych (RODO).

Wyznaczenie DPO

1 Które organizacje są zobowiązane wyznaczyć DPO?

Wyznaczenie DPO jest obowiązkowe:

- jeżeli przetwarzania dokonują organ lub podmiot publiczny (niezależnie od rodzaju przetwarzanych danych);
- jeżeli główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę;
- jeżeli główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

Należy zwrócić uwagę na fakt, że przepisy obowiązujące w Unii lub w państwach członkowskich mogą wymagać wyznaczenia DPO również w innych sytuacjach. Ponadto nawet jeżeli wyznaczenie DPO nie jest obowiązkowe, organizacje mogą niekiedy uznać za przydatne wyznaczenie DPO na zasadzie dobrowolności. Grupa Robocza Art. 29 zachęca do podejmowania dobrowolnych wysiłków w tym obszarze. Jeżeli organizacja wyznaczyła DPO na zasadzie dobrowolności, kwestie związane z wyznaczeniem takiego DPO, jego statusem i spoczywającymi na nim obowiązkami będą regulowały te same wymogi, jak gdyby został on wyznaczony w ramach obowiązku wyznaczenia DPO.

Źródło: art. 37 ust. 1 RODO.

2 Co oznacza pojęcie „główna działalność”?

„Główna działalność” oznacza kluczowe operacje, które administrator lub podmiot przetwarzający podejmują, aby osiągnąć swoje cele. Pojęcie to obejmuje również wszystkie czynności, w przypadku których przetwarzanie danych stanowi nieodłączny element działalności prowadzonej przez administratora lub podmiot przetwarzający. Na przykład przetwarzanie danych dotyczących zdrowia, takich jak dokumentacja medyczna pacjenta, powinno zostać uznane za jeden z elementów głównej działalności każdego szpitala, dlatego też szpitale są zobowiązane wyznaczyć DPO.

Wszystkie organizacje podejmują natomiast określonego rodzaju działania wspierające, na przykład przy wypłacaniu wynagrodzeń swoim pracownikom lub przy podejmowaniu standardowych czynności w zakresie wsparcia IT. Są to przykłady funkcji wspierających, które mają kluczowe znaczenie dla głównej działalności lub głównego obszaru zainteresowań danej organizacji. Choć działania w tym zakresie są niezbędne i kluczowe, zazwyczaj uznaje się je za działania pomocnicze, a nie za element głównej działalności.

Źródło: art. 37 ust. 1 lit. b) i c) RODO.

3 Co oznacza pojęcie „na dużą skalę”?

W RODO nie zawarto definicji pojęcia „przetwarzanie na dużą skalę”. Grupa Robocza Art. 29 zaleca, aby przy ustalaniu, czy przetwarzanie danych odbywa się na dużą skalę, wziąć pod uwagę w szczególności następujące czynniki:

- liczbę osób, których dane dotyczą – wyrażoną jako konkretna wartość albo jako odsetek populacji odniesienia;
- ilość danych lub zakres poszczególnych przetwarzanych pozycji danych;
- czas trwania lub trwałość czynności przetwarzania danych;
- zakres geograficzny czynności przetwarzania.

Przykłady przetwarzania na dużą skalę obejmują:

- przetwarzanie danych pacjentów przez szpital w ramach prowadzonej przez niego działalności;
- przetwarzanie danych o podróży osób fizycznych korzystających z miejskiego systemu transportu publicznego (np. śledzenie za pośrednictwem biletów elektronicznych);
- przetwarzanie danych określających położenie geograficzne klientów międzynarodowej sieci restauracji typu fast-food w czasie rzeczywistym do celów statystycznych przez podmiot przetwarzający specjalizujący się w podejmowaniu takich działań;
- przetwarzanie danych klientów przez zakład ubezpieczeń lub bank w ramach prowadzonej przez te podmioty działalności gospodarczej;
- przetwarzanie danych osobowych przez wyszukiwarkę internetową na potrzeby reklamy behawioralnej;
- przetwarzanie danych (treść, przepływ danych, lokalizacja) przez dostawców usług telefonicznych lub internetowych.

Przykłady działań, które nie stanowią przetwarzania na dużą skalę:

- przetwarzanie danych pacjenta przez pojedynczego lekarza;
- przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa przez pojedynczego prawnika.

Źródło: art. 37 ust. 1 lit. b) i c) RODO.

4 Co oznacza pojęcie „regularne i systematyczne monitorowanie”?

Choć pojęcie regularnego i systematycznego monitorowania osób, których dane dotyczą, nie zostało zdefiniowane w RODO, w oczywisty sposób obejmuje ono wszystkie formy śledzenia i profilowania w internecie na potrzeby reklamy behawioralnej. Pojęcie monitorowania nie ogranicza się jednak wyłącznie do aktywności prowadzonej w internecie.

Przykłady działań, które można uznać za działania stanowiące regularne i systematyczne monitorowanie osób, których dane dotyczą: obsługa sieci telekomunikacyjnej; świadczenie usług telekomunikacyjnych; przekierowywanie wiadomości e-mail; działalność marketingowa oparta na danych; profilowanie i przyznawanie punktów na potrzeby oceny ryzyka (np. na potrzeby punktowej oceny kredytowej, ustanowienia składek ubezpieczeniowych, zwalczania nadużyć finansowych i wykrywania przypadków prania pieniędzy); śledzenie zmian lokalizacji, na przykład za pomocą aplikacji mobilnych; programy lojalnościowe; reklama behawioralna; monitorowanie samopoczucia, parametrów fizycznych i danych dotyczących zdrowia za pomocą urządzeń do noszenia na ciele;

telewizja przemysłowa; urządzenia podłączone do internetu, np. inteligentne liczniki, inteligentne samochody, urządzenia związane z technologią automatyki domowej itp.

Zgodnie z wykładnią dokonaną przez Grupę Roboczą Art. 29, aby dane działanie można było uznać za „regularne", musi ono posiadać przynajmniej jedną z następujących cech:

- być aktualnie w toku lub być podejmowane w regularnych odstępach czasu w danym okresie;
- być prowadzone cyklicznie lub powtarzać się w określonych momentach;
- być prowadzone stale lub okresowo.

Zgodnie z wykładnią dokonaną przez Grupę Roboczą Art. 29, aby dane działanie można było uznać za „systematyczne", musi ono posiadać przynajmniej jedną z następujących cech:

- być przeprowadzane w ramach określonego systemu;
- być wcześniej zaplanowane, zorganizowane lub mieć metodyczny charakter;
- odbywać się w ramach ogólnego planu gromadzenia danych;
- być realizowane jako część strategii.

Źródło: art. 37 ust. 1 lit. b) RODO.

5 Czy organizacje mogą wspólnie wyznaczyć DPO? Jeżeli tak, to na jakich warunkach?

Tak. Grupa przedsiębiorstw może wyznaczyć jednego DPO, o ile można będzie „łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej". Pojęcie „dostępność" odnosi się do zadań DPO pełniącego funkcję punktu kontaktowego w odniesieniu do osób, których dane dotyczą, organów nadzorczych, a także – wewnętrznie – w ramach organizacji. Aby zapewnić dostępność DPO – niezależnie od tego, czy pełni on funkcję wewnętrzną czy zewnętrzną – należy upewnić się, że dane kontaktowe tego DPO zostały udostępnione. DPO musi mieć możliwość sprawnego komunikowania się z osobami, których dane dotyczą, oraz prowadzenia skutecznej współpracy z odpowiednimi organami nadzorczymi, w razie potrzeby z pomocą zespołu. Oznacza to, że komunikacja musi odbywać się w języku lub językach wykorzystywanych przez organy nadzorcze i odpowiednie osoby, których dane dotyczą. Dostępność DPO (niezależnie od tego, czy przebywa on w tym samym miejscu co pracownicy, czy też pracuje za pośrednictwem gorącej linii lub innego zabezpieczonego sposobu komunikacji) ma kluczowe znaczenie dla zagwarantowania osobom, których dane dotyczą, możliwości nawiązania kontaktu z DPO.

Dla kilku organów lub podmiotów publicznych można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego DPO. W takim przypadku obowiązują analogiczne zasady dotyczące zasobów i komunikowania. Biorąc pod uwagę fakt, że DPO jest odpowiedzialny za wykonywanie różnego rodzaju zadań, administrator lub podmiot przetwarzający musi zapewnić, aby pojedynczy DPO – w stosownych przypadkach przy wsparciu zespołu – był w stanie skutecznie wykonywać te zadania pomimo tego, że wyznaczono go dla szeregu organów i podmiotów publicznych.

Źródło: art. 37 ust. 2 i 3 RODO.

6 Gdzie powinna znajdować się siedziba DPO?

Aby zagwarantować dostępność DPO, Grupa Robocza Art. 29 zaleca, aby DPO znajdował się na terytorium Unii Europejskiej, niezależnie od tego, czy administrator lub podmiot przetwarzający ma swoją jednostkę organizacyjną w Unii Europejskiej. Nie można jednak wykluczyć, że w niektórych

przypadkach, w których administrator lub podmiot przetwarzający nie ma swojej jednostki organizacyjnej na terytorium Unii Europejskiej, DPO może skuteczniej wywiązywać się z powierzonych mu obowiązków w przypadku, gdy będzie znajdował się poza UE.

7 Czy można wyznaczyć zewnętrznego DPO?

Tak. DPO może być członkiem personelu administratora lub podmiotu przetwarzającego (wewnętrzny DPO) lub „wykonywać zadania na podstawie umowy o świadczenie usług". Oznacza to, że DPO może być zewnętrznym DPO – w takim przypadku pełni on powierzoną mu funkcję na podstawie umowy o świadczenie usług zawartej z daną osobą fizyczną lub organizacją.

Jeżeli funkcję DPO pełni zewnętrzny usługodawca, zadania DPO może skutecznie wykonywać zespół osób fizycznych pracujących dla tego usługodawcy działających pod nadzorem wyznaczonej głównej osoby odpowiedzialnej za kontakty oraz „osoby odpowiedzialnej" za danego klienta. W takiej sytuacji kluczowe znaczenie ma zagwarantowanie, aby wszyscy członkowie organizacji zewnętrznej pełniący funkcje DPO spełniali obowiązujące wymogi RODO.

W wytycznych zaleca się wyraźne podzielenie obowiązków w ramach zespołu zewnętrznego DPO i wyznaczenie jednej osoby jako osoby odpowiedzialnej za kontakty oraz za danego klienta w umowie o świadczenie usług w celu zapewnienia jasności prawa i dobrej organizacji oraz w celu uniknięcia konfliktów interesów wśród członków zespołu.

Źródło: art. 37 ust. 6 RODO.

8 Jakie kwalifikacje zawodowe powinien posiadać DPO?

DPO jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań.

Niezbędny poziom wiedzy fachowej należy ustalić w szczególności w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają przetwarzane dane osobowe. Na przykład, jeżeli dana czynność przetwarzania danych jest szczególnie złożona lub jeżeli zachodzi konieczność przetworzenia dużej ilości danych wrażliwych, DPO może potrzebować dodatkowej wiedzy fachowej i wsparcia.

Odpowiednie umiejętności i odpowiednia wiedza fachowa obejmują:

- wiedzę fachową w zakresie krajowych i europejskich przepisów i praktyk w dziedzinie ochrony danych, w tym dogłębną znajomość RODO;
- wiedzę na temat przeprowadzanych operacji przetwarzania;
- znajomość technologii informacyjnych i zasad bezpieczeństwa danych;
- wiedzę na temat sektora, w którym prowadzona jest działalność gospodarcza, oraz na temat danej organizacji;
- umiejętność promowania kultury ochrony danych w organizacji.

Źródło: art. 37 ust. 5 RODO.

9 Jakie zasoby administrator lub podmiot przetwarzający powinni zapewnić DPO?

DPO musi posiadać zasoby niezbędne do wykonywania swoich zadań.

W zależności od specyfiki operacji przetwarzania oraz działalności prowadzonej przez organizację i jej wielkości DPO należy zapewnić:

- aktywne wsparcie ze strony kadry kierowniczej wyższego szczebla przy pełnieniu powierzonej mu funkcji;
- czas wystarczający do tego, by mógł się on wywiązać z przydzielonych mu obowiązków;
- w stosownych przypadkach wsparcie w postaci zasobów finansowych, infrastruktury (pomieszczenia, urządzenia, wyposażenie) oraz pracowników;
- oficjalne powiadomienie wszystkich pracowników o jego wyznaczeniu;
- dostęp do innych służb w ramach organizacji, aby mógł on otrzymywać niezbędne wsparcie, dane wejściowe lub informacje;
- doskonalenie zawodowe.

Źródło: art. 38 ust. 2 RODO.

10 Jakie gwarancje należy ustanowić, aby zapewnić DPO możliwość samodzielnego wykonywania powierzonych mu zadań? Co oznacza pojęcie „konflikt interesów”?

Istnieje szereg gwarancji zapewniających DPO możliwość samodzielnego wykonywania powierzonych mu zadań:

- zakaz instruowania DPO w zakresie sposobu wykonywania powierzonych mu zadań przez administratorów lub podmioty przetwarzające;
- zakaz odwołania DPO ze stanowiska lub nałożenia na niego sankcji przez administratora w związku z wykonywanymi przez niego zadaniami;
- brak konfliktu interesów, jeżeli chodzi o inne potencjalne zadania i obowiązki.

Inne zadania i obowiązki DPO nie mogą prowadzić do konfliktu interesów. Oznacza to, po pierwsze, że DPO nie może piastować stanowiska w organizacji, które zapewniałoby mu dostęp do informacji pozwalających mu ustalić cele i sposoby przetwarzania danych osobowych. Biorąc pod uwagę specyficzną strukturę organizacyjną poszczególnych organizacji, kwestie te należy rozstrzygać w odniesieniu do indywidualnych przypadków.

Ogólnie rzecz biorąc, stanowiska w organizacji, w przypadku których dochodzi do konfliktu interesów, mogą obejmować stanowiska w strukturze kadry kierowniczej wyższego szczebla (takie jak dyrektor generalny, dyrektor ds. operacyjnych, dyrektor ds. finansowych, dyrektor ds. medycznych, kierownik departamentu marketingu, kierownik działu kadr lub kierownik departamentów IT), ale również inne stanowiska na niższych szczeblach struktury organizacyjnej, jeżeli piastowanie tych stanowisk lub pełnienie tych funkcji zapewnia możliwość ustalenia celów i sposobów przetwarzania. Ponadto konflikt interesów może powstać również wtedy, gdy np. zewnętrzny DPO zostanie

poproszony o reprezentowanie administratora lub podmiotu przetwarzającego przed sądem w sprawie dotyczącej ochrony danych.

Źródło: art. 38 ust. 3 i 6 RODO.

Zadania DPO

11 Co oznacza termin „monitorowanie przestrzegania”?

W ramach przedmiotowych obowiązków w zakresie monitorowania przestrzegania DPO może w szczególności:

- gromadzić informacje pozwalające zidentyfikować czynności przetwarzania;
- analizować czynności przetwarzania i sprawdzać ich zgodność z przepisami rozporządzenia;
- przekazywać administratorowi lub podmiotowi przetwarzającemu informacje, udzielać im porad lub publikować skierowane do nich zalecenia.

Źródło: art. 39 ust. 1 lit. b) RODO.

12 Czy DPO ponosi osobistą odpowiedzialność za przypadki naruszenia wymogów dotyczących ochrony danych?

Nie, DPO nie ponosi osobistej odpowiedzialności za przypadki naruszenia wymogów dotyczących ochrony danych. Obowiązek zagwarantowania i wykazania, iż przetwarzanie danych odbywa się zgodnie z przepisami rozporządzenia, spoczywa na administratorze lub podmiocie przetwarzającym. Obowiązek zapewnienia zgodności środków w zakresie ochrony danych z przepisami rozporządzenia spoczywa na administratorze lub podmiocie przetwarzającym.

13 Jaką rolę pełni DPO w procesie oceny skutków dla ochrony danych i rejestru czynności przetwarzania danych osobowych?

Jeżeli chodzi o ocenę skutków dla ochrony danych, administrator lub podmiot przetwarzający powinien zasięgnąć opinii DPO m.in. w następujących kwestiach:

- konieczności przeprowadzenia oceny skutków dla ochrony danych;
- metody, jaką należy zastosować przy przeprowadzaniu oceny skutków dla ochrony danych;
- ustalenia, czy ocena skutków dla ochrony danych powinna zostać przeprowadzona wewnątrz przedsiębiorstwa, czy też zlecona podmiotowi zewnętrznemu;
- ustalenia, jakie gwarancje (uwzględniając środki techniczne i organizacyjne) należy zastosować w celu ograniczenia wszelkiego rodzaju zagrożeń dla praw i interesów osób, których dane dotyczą;
- ustalenia, czy ocena skutków dla ochrony danych została przeprowadzona w prawidłowy sposób i czy jej wyniki (wnioski dotyczące tego, czy należy kontynuować przetwarzanie danych, oraz tego, jakie zabezpieczenia należy zastosować) są zgodne z wymogami w zakresie ochrony danych.

Jeżeli chodzi o rejestry czynności przetwarzania, odpowiedzialność za monitorowanie procesu rejestrowania operacji przetwarzania spoczywa na administratorze lub podmiocie przetwarzającym, a nie na DPO. Nic nie stoi jednak na przeszkodzie, aby administrator lub podmiot przetwarzający powierzył DPO zadanie prowadzenia rejestrów operacji przetwarzania pod nadzorem administratora lub podmiotu przetwarzającego. Takie rejestry powinny być traktowane jako jedno z narzędzi zapewniających DPO możliwość wywiązywania się z powierzonych mu zadań w zakresie monitorowania przestrzegania, przekazywania informacji i udzielania porad administratorowi lub podmiotowi przetwarzającemu.

Źródło: art. 39 ust. 1 lit. c) i art. 30 RODO.

Sporządzono w Brukseli dnia 13 grudnia 2016 r.

W imieniu Grupy Roboczej
Przewodnicząca

Isabelle FALQUE-PIERROTIN

Ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r.

W imieniu Grupy Roboczej
Przewodnicząca

Isabelle FALQUE-PIERROTIN