

## WP243 ZAŁĄCZNIK – CZĘSTO ZADAWANE PYTANIA

*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 inspektorów ochrony danych (DPO) w ogólnym rozporządzeniu o ochronie danych (RODO).*

### Wyznaczenie DPO (art. 37)

---

#### 1 Które organizacje są zobowiązane wyznaczyć DPO? (art. 37 ust. 1)

Zgodnie z RODO DPO należy wyznaczyć w trzech konkretnych przypadkach:

- 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; oraz
- 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 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.

*Aby uzyskać dodatkowe informacje na ten temat, zob. sekcja 2.1 wytycznych.*

#### 2 Co oznacza pojęcie „główna działalność”? (art. 37 ust. 1 lit. b) i c))

„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. Te funkcje wspierające 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.

*Aby uzyskać dodatkowe informacje na ten temat, zob. sekcja 2.1.2 wytycznych.*

### **3 Co oznacza pojęcie „na dużą skalę”? (art. 37 ust. 1 lit. b) i c))**

W RODO nie zawarto definicji pojęcia „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.

*Aby uzyskać dodatkowe informacje na ten temat, zob. sekcja 2.1.3 wytycznych.*

### **4 Co oznacza pojęcie „regularne i systematyczne monitorowanie”? (art. 37 ust. 1 lit. b))**

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.

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.

Przykłady: obsługa sieci telekomunikacyjnej; świadczenie usług telekomunikacyjnych; przekierowywanie wiadomości e-mail; 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.

*Aby uzyskać dodatkowe informacje na ten temat, zob. sekcja 2.1.4 wytycznych.*

## **5 Czy organizacje mogą wspólnie wyznaczyć DPO? Jeżeli tak, to jakie warunki muszą zostać spełnione? (art. 37 ust. 2 i 3)**

RODO stanowi, że 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 zgodnie z przepisami RODO. DPO musi mieć możliwość sprawnego komunikowania się z osobami, których dane dotyczą, oraz prowadzenia skutecznej współpracy z odpowiednimi organami nadzorczymi. Oznacza to, że komunikacja musi odbywać się w języku lub językach wykorzystywanych przez organy nadzorcze i odpowiednie osoby, których dane dotyczą. Osobista 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.

*Aby uzyskać dodatkowe informacje na ten temat, zob. sekcja 2.3 wytycznych.*

## **6 Czy można wyznaczyć zewnętrznego DPO (art. 37 ust. 6)?**

Tak. Zgodnie z art. 37 ust. 6 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.

Zewnętrzny DPO podlega wszystkim wymogom ustanowionym w art. 37–39. Zgodnie z treścią wytycznych, 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 odpowiednie 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.

*Aby uzyskać dodatkowe informacje na ten temat, zob. sekcje 2.3, 2.4 i 3.5 wytycznych.*

## **7 Jakie kwalifikacje zawodowe powinien posiadać DPO (art. 37 ust. 5)?**

Zgodnie z wymogami RODO 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”.

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.

Niezbędne umiejętności i niezbędna 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.

*Aby uzyskać dodatkowe informacje na ten temat, zob. sekcja 2.4 wytycznych.*

## **Status DPO (art. 38)**

---

## **8 Jakie zasoby należy zapewnić DPO, aby mógł on skutecznie wywiązywać się z powierzonych mu zadań?**

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 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.

*Aby uzyskać dodatkowe informacje na ten temat, zob. sekcja 3.2 wytycznych.*

## **9 Jakie gwarancje należy ustanowić, aby zapewnić DPO możliwość samodzielnego wykonywania powierzonych mu zadań (art. 38 ust. 3)?**

Istnieje szereg gwarancji zapewniających DPO możliwość samodzielnego wykonywania powierzonych mu zadań zgodnie z motywem 97:

- 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.

*Aby uzyskać dodatkowe informacje na ten temat, zob. sekcje 3.3–3.5 wytycznych.*

## **10 Jakie „inne zadania i obowiązki” DPO mogą doprowadzić do konfliktu interesów (art. 38 ust. 6)?**

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 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.

*Aby uzyskać dodatkowe informacje na ten temat, zob. sekcja 3.5 wytycznych.*

### **11 Co oznacza pojęcie „monitorowanie przestrzegania” przepisów RODO (art. 39 ust. 1 lit. b)?**

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; oraz
- przekazywać administratorowi lub podmiotowi informacje, udzielać im porad lub publikować skierowane do nich zalecenia.

*Aby uzyskać dodatkowe informacje na ten temat, zob. sekcja 4.1 wytycznych.*

### **12 Czy DPO ponosi osobistą odpowiedzialność za przypadki naruszenia przepisów RODO?**

Nie, 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 przepisami rozporządzenia, 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.

### **13 Jaką rolę pełni DPO w procesie oceny skutków dla ochrony danych (art. 37 ust. 1 lit. c) i rejestru czynności przetwarzania danych osobowych (art. 30)?**

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 przepisami RODO.

*Aby uzyskać dodatkowe informacje na ten temat, zob. sekcja 4.2 wytycznych.*

Jeżeli chodzi o rejestr 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 rejestru operacji przetwarzania pod nadzorem administratora.

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.

*Aby uzyskać dodatkowe informacje na ten temat, zob. sekcja 4.4 wytycznych.*