GRUPA ROBOCZA ART. 29 DS. OCHRONY DANYCH

**17/EN**
**WP 248**

# Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679

**Przyjęte w dniu 4 kwietnia 2017 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 MO-59 05/35.

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

# I. Wprowadzenie

Rozporządzenie 2016/679[1] (RODO) będzie miało zastosowanie od dnia 25 maja 2018 r. Artykuł 35 RODO wprowadza pojęcie oceny skutków dla ochrony danych (DPIA); czyni to również dyrektywa 2016/680[2].

DPIA to proces mający opisać przetwarzanie, ocenić niezbędność i proporcjonalność przetwarzania oraz pomóc w zarządzaniu ryzykiem naruszenia praw lub wolności osób fizycznych wynikającym z przetwarzania danych osobowych[3] (oceniając ryzyko i ustalając środki mające mu zaradzić). Oceny skutków dla ochrony danych to narzędzia istotne dla celów rozliczalności, ponieważ pomagają administratorom nie tylko w przestrzeganiu wymogów RODO, ale również w wykazaniu, że podjęto odpowiednie środki w celu zapewnienia zgodności z rozporządzeniem (patrz także artykuł 24)[4]. Innymi słowy, DPIA to proces służący do zapewnienia i wykazania zgodności.

Zgodnie z RODO nieprzestrzeganie wymogów DPIA może doprowadzić do nałożenia kar przez właściwy organ nadzorczy. Niedokonanie oceny skutków dla ochrony danych, gdy przetwarzanie podlega takiej ocenie (artykuł 35 ust. 1 i 3), przeprowadzenie DPIA w nieprawidłowy sposób (art. 35 ust. 2 i 7) lub nieskonsultowanie się z właściwym organem nadzorczym, gdy jest to wymagane (artykuł 36 ust. 3 lit. e), może skutkować nałożeniem kary pieniężnej w wysokości do 10 milionów EURO, a w przypadku przedsiębiorstwa – w wysokości do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

Uwaga: termin „ocena skutków dla ochrony prywatności" (PIA) jest często używany w innych kontekstach w odniesieniu do tego samego pojęcia.

---

[1] Rozporządzenie (UE) 2016/679 Parlamentu Europejskiego i Rady 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] Artykuł 27 dyrektywy (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 również stanowi, że konieczna jest ocena skutków dla ochrony danych, jeżeli *„przetwarzanie z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych*"

[3] RODO nie definiuje formalnie pojęcia DPIA jako takiego, ale
- minimalny zakres DPIA jest określony w artykule 35 ust. 7 jako obejmujący:
a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1; oraz
d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy;
- znaczenie i rola DPIA określono w motywie 84: *„Aby poprawić przestrzeganie niniejszego rozporządzenia, gdy operacje przetwarzania mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, należy zobowiązać administratora do dokonania oceny skutków dla ochrony danych w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi tego ryzyka*".

[4] Patrz także motyw 84: *„Wyniki oceny należy uwzględnić przy określaniu odpowiednich środków, które należy zastosować, by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z niniejszym rozporządzeniem*".

## II. Zakres wytycznych

Wytyczne biorą pod uwagę:
- Oświadczenie Grupy Roboczej Artykułu 29 ds. Ochrony Danych (GR Art. 29) 14/EN WP 218[5];
- Wytyczne GR Art. 29 dotyczące inspektora ochrony danych 16/EN WP 243[6];
- Wytyczne GR Art. 29 w sprawie ograniczenia celu 13/EN WP 203[7];
- międzynarodowe standardy[8].

Zgodnie z podejściem opartym na ryzyku wyrażonym w GDPR, dokonanie DPIA nie jest obowiązkowe dla każdej operacji przetwarzania. DPIA jest wymagana tylko, gdy przetwarzanie „*z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych*" (artykuł 35 ust. 1). W celu zapewnienia spójnej interpretacji okoliczności, w których DPIA jest obowiązkowa (artykuł 35 ust. 3) niniejsze wytyczne po pierwsze dążą do wyjaśnienia tego pojęcia i zapewnienia kryteriów do wykazów, które mają być przyjęty przez organy ochrony danych na mocy artykułu 35 ust. 4.

Zgodnie z artykułem 70 ust. 1 lit. e) Europejska Rada Ochrony Danych (EROD) będzie mogła wydawać wytyczne, zalecenia oraz określa najlepsze praktyki, by zachęcić do spójnego stosowania niniejszego rozporządzenia. Celem niniejszego dokumentu jest przewidzenie takiej przyszłej pracy EROD i w związku z tym wyjaśnienie istotnych przepisów RODO, aby pomóc administratorom w przestrzeganiu prawa i zapewnienia pewności prawnej dla administratorów, którzy są zobowiązani do przeprowadzenia DPIA.

Wytyczne dążą również do propagowania rozwoju:
- wspólnego wykazu Unii Europejskiej operacji przetwarzania, dla których DPIA jest obowiązkowa (artykuł 35 ust. 4);
- wspólnego wykazu UE operacji przetwarzania, dla których DPIA nie jest konieczna (artykuł 35 ust. 5);
- wspólnych kryteriów dotyczących metodologii przeprowadzenia DPIA (artykuł 35 ust. 5);
- wspólnych kryteriów określenia, kiedy należy się konsultować z organem nadzorczym (artykuł 36 ust. 1);
- zaleceń, gdy możliwe opartych na doświadczeniu zdobytym przez państwa członkowskie UE.

---

[5] Oświadczenie GR Art. 29 WP 218 dotyczące roli opartego na ryzyku podejścia do ram prawnych ochrony danych przyjęte 30 maja 2014 r. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

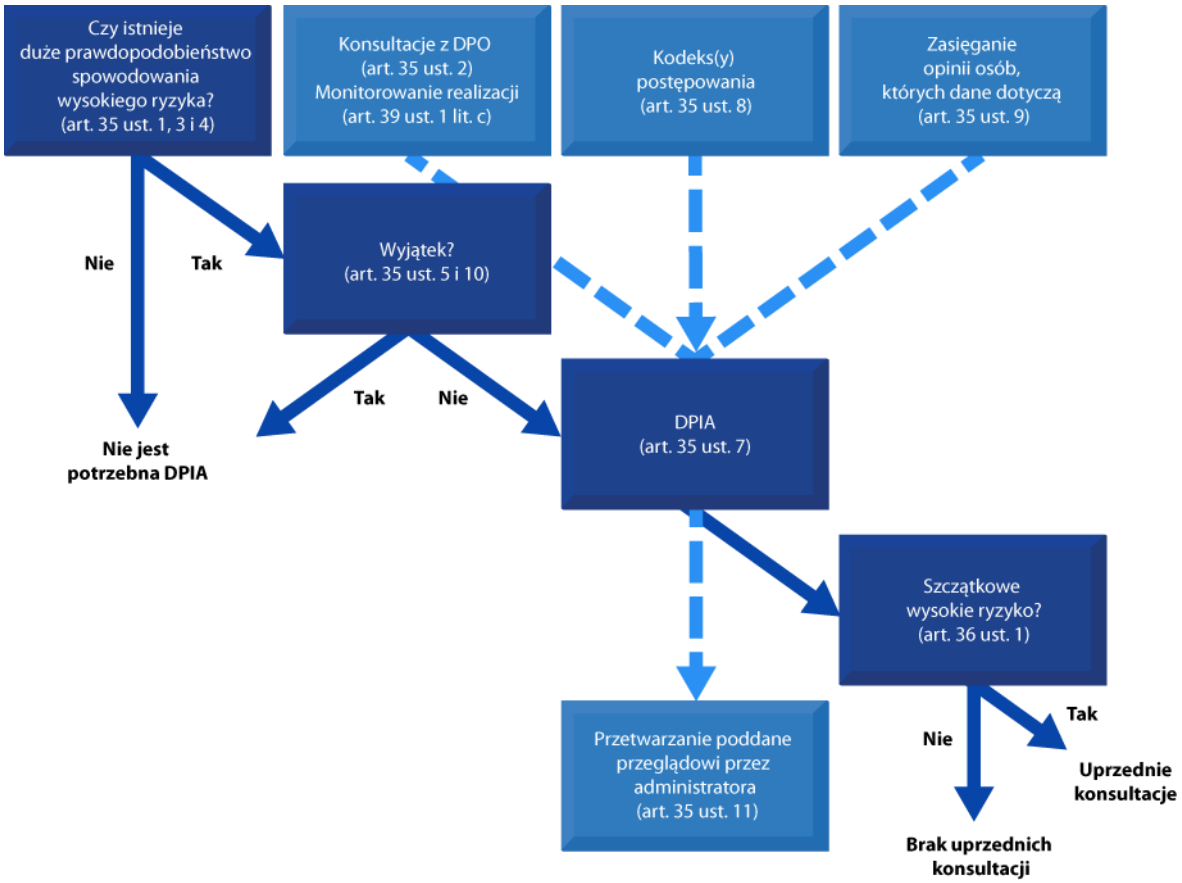
[6] Wytyczne GR Art. 29 dotyczące inspektora ochrony danych 16/EN WP 243 przyjęte 13 grudnia 2016 r. http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[7] Opinia GR Art. 29 03/2013 w sprawie ograniczenia celu 13/EN WP 2013 przyjęta 2 kwietnia 2013 r. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[8] Np. ISO 31000:2009, *Zarządzanie ryzykiem – Zasady i wytyczne,* Międzynarodowa Organizacja Normalizacyjna (ISO); ISO/IEC 29134 (projekt), IT – Techniki bezpieczeństwa – Ocena skutków dla ochrony prywatności – Wytyczne, Międzynarodowa Organizacja Normalizacyjna (ISO).

## III. DPIA: wyjaśnienie w rozporządzeniu

Poniższy wykres ilustruje podstawowe zasady dotyczące DPIA w RODO:




### A. Czego dotyczy DPIA? Pojedynczej operacji przetwarzania lub (zestawu) podobnych operacji przetwarzania

DPIA może dotyczyć pojedynczej operacji przetwarzania. Jednak artykuł 35 ust. 1 stanowi, że: *„Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę."* Motyw 92 dodaje, że *„W niektórych okolicznościach rozsądnie i korzystnie byłoby nie ograniczać oceny skutków dla ochrony danych do pojedynczego projektu, na przykład w przypadkach, gdy organy lub podmioty publiczne zamierzają ustanowić wspólną aplikację lub platformę przetwarzania lub gdy kilku administratorów planuje wprowadzić wspólną aplikację lub środowisko przetwarzania obejmujące sektor lub segment gospodarki lub szeroko rozpowszechnioną działalność horyzontalną*".

Oznacza to, że pojedynczą DPIA można wykorzystać do oceny wielu operacji przetwarzania, które są podobne pod względem ryzyka z nimi związanego, pod warunkiem odpowiedniego uwzględnienia szczególnego charakteru, zakresu, kontekstu i celów przetwarzania. Może to oznaczać przypadek, gdy podobna technologia jest wykorzystywana do zbierania takiego samego rodzaju danych do tych samych celów. Na przykład grupa organów lokalnych, które

tworzą podobny system telewizji przemysłowej, mogłaby dokonać pojedynczej DPIA obejmującej przetwarzanie przez tych odrębnych administratorów lub operator kolejowy (pojedynczy administrator) mógłby objąć zakresem jednej DPIA nadzór wideo na wszystkich swoich stacjach kolejowych.

Gdy operacja przetwarzania dotyczy współadministratorów, muszą oni dokładnie określić swoje odnośne obowiązki. Ich DPIA powinna wskazywać, która strona jest odpowiedzialna za różne środki przewidziane do zaradzenia ryzyku oraz do ochrony praw osób, których dane dotyczą.

DPIA może być również przydatna do oceny skutków dla ochrony danych produktu technologicznego, na przykład sprzętu lub oprogramowania, gdy istnieje prawdopodobieństwo wykorzystania go przez różnych administratorów danych do przeprowadzenia różnych operacji przetwarzania. Oczywiście administrator danych wdrażający produkt nadal jest zobowiązany do dokonania własnej DPIA w odniesieniu do określonego wdrożenia, ale informacji do tego może dostarczyć DPIA przygotowana przez dostawcę produktu, jeżeli to właściwe. Przykładem może być relacja między producentami inteligentnych liczników a przedsiębiorstwami użyteczności publicznej.

## B. Jakie operacje przetwarzania podlegają DPIA?

W tej części opisano, kiedy DPIA jest obowiązkowa, kiedy jest wymagana ze względu na prawdopodobieństwo spowodowania wysokiego ryzyka oraz co należy zrobić w przypadku istniejących operacji przetwarzania.

### a) Kiedy DPIA jest obowiązkowa? W przypadku gdy przetwarzanie *„z dużym prawdopodobieństwem może powodować wysokie ryzyko”.*

RODO nie wymaga dokonywania DPIA w przypadku każdej operacji przetwarzania, które może powodować ryzyko naruszenia praw lub wolności osób fizycznych. Dokonanie DPIA jest obowiązkowe tylko, gdy przetwarzanie „*z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych”* (artykuł 35 ust. 1, zilustrowany artykułem 35 ust. 3 i uzupełniony artykułem 35 ust. 4). Jest to szczególnie istotne, gdy wprowadzana jest nowa technologia przetwarzania danych[9].

W przypadkach, gdy nie jest jasne, czy wymagana jest DPIA, GR Art. 29 zaleca, żeby jednak dokonać DPIA, ponieważ DPIA jest przydatnym narzędziem, które może pomóc administratorom danych w zapewnieniu zgodności z prawem ochrony danych.

Mimo że DPIA mogłaby być wymagana w innych okolicznościach, artykuł 35 ust. 3 przedstawia kilka przykładów przypadków, gdy przetwarzanie „*z dużym prawdopodobieństwem może powodować wysokie ryzyko*”:

- *„(a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną[10];*

- *(b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10[11]; lub*

- *(c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.”*

Jak wskazują słowa „*w szczególności*” we wprowadzającym zdaniu artykułu 35 ust. 3 RODO, chodzi tu o niewyczerpujący wykaz. Mogą istnieć operacje przetwarzania o „wysokim ryzyku”, które nie są objęte tym wykazem, ale jednak wiążą się z podobnym wysokim ryzykiem. Takie operacje przetwarzania również powinny podlegać DPIA. Z tego względu opracowane kryteria przedstawione poniżej czasami wykraczają poza zwykłe wyjaśnienie, co należy rozumieć przez trzy przykłady podane w artykule 35 ust. 3 RODO.

W celu zapewnienia bardziej konkretnego zestawu operacji przetwarzania, które wymagają dokonania DPIA ze względu na związane z nimi wysokie ryzyko, biorąc pod uwagę określone elementy artykułów 35 ust. 1 i art. 35 ust. 3 lit. a) do c), wykaz, który ma być przyjęty na poziomie krajowym na mocy artykułu 35 ust. 4 oraz motywy 71, 75 i 91, oraz

[9] Patrz motywy 89, 91 i artykuł 35 ust. 1 i 3 – dalsze przykłady.

[10] Patrz motyw 71: *„w szczególności analizować lub prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą - w celu tworzenia lub wykorzystywania profili osobistych”*.

[11] Patrz motyw 75: *„jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa”*.

inne odniesienia RODO do przetwarzania, które „*z dużym prawdopodobieństwem może powodować wysokie ryzyko”*[12], należy uwzględnić następujące kryteria:

1. Ewaluacja lub ocena, w tym profilowanie i przewidywanie, szczególnie „*aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą”* (motywy 71 i 91). Przykładami mogą być np. bank, który sprawdza swoich klientów w bazie informacji kredytowej lub przedsiębiorstwo biotechnologiczne oferujące testy genetyczne bezpośrednio konsumentom w celu oceny i przewidywania ryzyka wystąpienia choroby lub zagrożenia dla zdrowia, bądź też przedsiębiorstwo tworzące profile behawioralne lub marketingowe w oparciu o zakres korzystania ze strony internetowej.

2. Zautomatyzowane podejmowanie decyzji wywołujących skutki prawne lub podobne istotne skutki: przetwarzanie mające na celu podejmowanie decyzji dotyczących osób, których dane dotyczą, wywołujących „*skutki prawne wobec osoby fizycznej”* lub „*w podobny sposób znacząco wpływających na osobę fizyczną*” (artykuł 35 ust. 3 lit. a). Na przykład przetwarzanie może prowadzić do wyłączenia lub dyskryminacji osób. Przetwarzanie wywołujące niewielkie skutki lub niewywołujące skutków wobec osób nie odpowiada temu konkretnemu kryterium. Dalsze wyjaśnienia tych pojęć zostaną przedstawione w przygotowywanych Wytycznych GR Art. 29 dotyczących profilowania.

3. Systematyczne monitorowanie: przetwarzanie wykorzystywane do obserwacji, monitorowania i kontroli osób, których dane dotyczą, w tym dane zbierane poprzez *„systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie”* (artykuł 35 ust. 3 lit. c)[13]. Ten rodzaj monitorowania jest kryterium, ponieważ dane osobowe mogą być zbierane w okolicznościach, gdy osoby, których dane dotyczą, mogą nie być świadome faktu, kto zbiera ich dane i jak będą wykorzystane. Ponadto może być niemożliwe uniknięcie przez osoby fizyczne bycia przedmiotem takiego przetwarzania w często uczęszczanych (lub publicznie dostępnych) miejscach.

4. Dane wrażliwe[14]: obejmują szczególne kategorie danych określonych w artykule 9 (na przykład informacje na temat poglądów politycznych osób fizycznych), jak również dane dotyczące wyroków skazujących i naruszeń prawa. Przykładem może być szpital ogólny prowadzący dokumentację medyczną pacjentów lub prywatny detektyw przechowujący dane dotyczące przestępców. Kryterium to obejmuje również dane, które mogą być bardziej ogólnie uznane za zwiększające możliwe ryzyko naruszenia praw lub wolności osób fizycznych, takie jak dane dotyczące komunikacji elektronicznej, dane dotyczące lokalizacji, dane finansowe (które mogłyby być wykorzystane w celu oszustw płatniczych). W tym

[12] Patrz np. motywy 75, 76, 92, 116.

[13] GR Art. 29 interpretuje *„systematyczne”* jako jedno lub więcej z poniższych pojęć (patrz Wytyczne GR Art. 29 dotyczące inspektora ochrony danych 16/EN WP 243):

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

GR Art. 29 interpretuje *„miejsce dostępne publicznie*” jako każde miejsce dostępne dla każdego członka społeczeństwa, na przykład plac, centrum handlowe, ulica lub biblioteka publiczna.

[14] Niemniej jeżeli dane wrażliwe nie są przetwarzane systematycznie i na dużą skalę, ich przetwarzanie nie stanowi automatycznie wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą. Na przykład administrator danych, który organizuje wydarzenie firmowe chciałby wiedzieć, na jakiego rodzaju dania typu fast food mają alergię jego goście, mógłby wyjątkowo przetwarzać te dane wrażliwe, i musiałby dokonać DPIA. Podobnie przetwarzanie danych szczególnych kategorii przez lekarza medycyny w ramach jednoosobowej praktyki nie powinno być uznane jako przetwarzanie *„na dużą skalę” (*motyw 91).

zakresie istotny może być fakt, czy dane już zostały publicznie udostępnione przez osobę, której dane dotyczą, lub przez strony trzecie. Fakt, że dane osobowe są publicznie dostępne, może być uznany za czynnik przy ocenie, czy spodziewano się dalszego wykorzystania danych do określonych celów. Kryterium to może również obejmować informacje przetwarzane przez osobę fizyczną w ramach działań o czysto osobistym lub domowym charakterze (jak np. usługi przetwarzania w chmurze do zarządzania dokumentami osobistymi, usługi poczty elektronicznej, kalendarze, e-czytniki wyposażone w funkcje robienia notatek oraz różne aplikacje typu „life-logging", które mogą zawierać informacje o bardzo osobistym charakterze), których ujawnienie lub przetwarzanie do celów innych niż czynności o charakterze domowym może być uznane za bardzo ingerujące.

5. Dane przetwarzane na dużą skalę: RODO nie definiuje pojęcia dużej skali, choć motyw 91 przedstawia pewne wskazówki. W każdym przypadku GR Art. 29 zaleca uwzględnianie w szczególności następujących czynników przy określaniu, czy przetwarzanie jest prowadzone na dużą skalę[15].

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

6. Dokonano porównania lub połączenia zestawów danych: na przykład pochodzących z dwóch lub większej liczby operacji przetwarzania prowadzonych w różnych celach i/lub przez różnych administratorów danych w sposób, który wykracza poza racjonalne oczekiwania osoby, której dane dotyczą[16].

7. Dane dotyczące osób wymagających szczególnej opieki (patrz motyw 75): przetwarzanie tego rodzaju danych może wymagać DPIA ze względu na zwiększony brak równowagi sił między osobą, której dane dotyczą, a administratorem danych, co oznacza, że osoba może nie być w stanie wyrazić zgody na przetwarzanie jej danych lub sprzeciwić się mu. Na przykład pracownicy często napotykają poważne trudności w wyrażeniu sprzeciwu wobec przetwarzania prowadzonego przez ich pracodawcę, gdy jest powiązane z zarządzaniem zasobami ludzkimi. Podobnie, dzieci można uznać za niebędące w stanie świadomie i rozważnie wyrazić sprzeciw lub zgodę na przetwarzanie ich danych. Dotyczy to także wymagającej szczególne opieki i ochrony części społeczeństwa, na przykład osób chorych psychicznie, osób ubiegających się o azyl lub osób starszych, pacjentów, lub w każdym przypadku, gdy można ustalić brak równowagi w relacji między pozycją osoby, której dane dotyczą, a administratora.

8. Innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych, jak na przykład połączenie wykorzystania odcisków palców i rozpoznawania twarzy do usprawnienia fizycznej kontroli dostępu, etc. RODO wyjaśnia (artykuł 35 ust. 1 i motywy 89 i 91), że wykorzystanie nowej technologii może wywołać potrzebę dokonania DPIA. Jest tak, ponieważ wykorzystanie takiej technologii może obejmować nowoczesne formy zbierania i wykorzystywania danych, potencjalnie mogących wywołać wysokie ryzyko naruszenia praw lub wolności osób fizycznych. W istocie osobiste i społeczne konsekwencje zastosowania nowej technologii mogą być nieznane. DPIA pomoże administratorowi danych zrozumieć takie rodzaje ryzyka i zaradzić im. Na przykład określone

[15] Patrz Wytyczne GR Art. 29 dotyczące inspektora ochrony danych 16/EN WP 243.
[16] Patrz wyjaśnienie w Opinii GR Art. 29 w sprawie ograniczenia celu 13/EN WP 203, str. 24.

aplikacje „Internetu Przedmiotów" mogłyby mieć znaczny wpływ na codzienne życie osób i ich prywatność; i w związku z tym wymagają dokonania DPIA.

9. Transgraniczne przekazywanie danych poza Unię Europejską (motyw 116), biorąc pod uwagę, między innymi, przewidywany kraj lub kraje przeznaczenia, możliwość dalszego przekazywania lub prawdopodobieństwo operacji przekazywania opartych na wyłączeniach dla określonych sytuacji przewidzianych w RODO.

10. Gdy przetwarzanie samo w sobie *„uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystania z usługi lub umowy"* (artykuł 22 i motyw 91). Dotyczy to przetwarzania prowadzonego w miejscu publicznym, którego przechodzący ludzie nie mogą uniknąć, lub przetwarzania, którego celem jest umożliwienie, zmiana lub odmowa dostępu osób, których dane dotyczą, do usługi lub zawarcia umowy. Przykładem jest sytuacja, gdy bank sprawdza swoich klientów w bazie informacji kredytowej, aby podjąć decyzję o zaproponowaniu im pożyczki.

GR Art. 29 uważa, że im więcej kryteriów jest spełnionych przez przetwarzanie, tym większe jest prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą, i w związku z tym wymagana jest DPIA. Co do zasady, operacja przetwarzania spełniająca mniej niż dwa kryteria może nie wymagać DPIA ze względu na niższy poziom ryzyka. Na przykład:

| **Przykłady przetwarzania** | **Możliwe istotne kryteria** | **Czy DPIA jest wymagana?** |
|---|---|---|
| Szpital przetwarzający dane genetyczne i dane dotycząca zdrowia swoich pacjentów (system informacyjny szpitala) | - Dane wrażliwe<br>- Dane dotyczące osób, których dane dotyczą, wymagających szczególnej opieki | Tak |
| Wykorzystanie systemu kamer do monitorowania zachowania kierowców na autostradach. Administrator zakłada wykorzystanie inteligentnego systemu analizy wideo w celu wyodrębnienia samochodów i automatycznego rozpoznania tablic rejestracyjnych. | - Systematyczne monitorowania<br>- Innowacyjne wykorzystanie lub zastosowanie rozwiązań technicznych lub organizacyjnych | |
| Przedsiębiorstwo monitorujące działania swoich pracowników, w tym stanowiska pracy pracowników, działania w Internecie, etc. | - Systematyczne monitorowanie<br>- Dane dotyczące osób, których dane dotyczą, wymagających szczególnej opieki | |
| Gromadzenie danych z profili na publicznych mediach społecznościowych, które mają być wykorzystane przez prywatne przedsiębiorstwa generujące profile do katalogów kontaktów. | - Ewaluacja i ocena<br>- Dane przetwarzane na dużą skalę | |

| | | |
|---|---|---|
| Magazyn online wykorzystujący listę mailingową do wysyłania codziennej porcji ogólnych wiadomości do swoich abonentów. | - (brak) | Nie koniecznie |
| Strona internetowa handlu elektronicznego wyświetla ogłoszenia dotyczące części samochodów zabytkowych, w tym ograniczone profilowanie oparte na wcześniejszych zachowaniach zakupowych w określonych częściach strony internetowej. | - Ewaluacja lub ocena, ale nie systematyczna i nie obszerna | |

Jednak w niektórych przypadkach przetwarzanie spełniające tylko jedno z tych kryteriów wymagać będzie dokonania DPIA. Z drugiej strony, jeżeli administrator uważa, że mimo faktu, że przetwarzanie spełnia co najmniej dwa kryteria, uznaje się, że nie ma „prawdopodobieństwa wysokiego ryzyka", musi on dokładnie udokumentować powody niedokonania DPIA.

Ponadto administrator danych podlegający obowiązkowi dokonania DPIA *„prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada"*, obejmujący między innymi cele przetwarzania, opis kategorii danych i odbiorców danych oraz „*jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1* (artykuł 30 ust. 1) oraz musi ocenić, czy wysokie ryzyko jest prawdopodobne, nawet jeżeli ostatecznie postanowi nie przeprowadzać DPIA.

Uwaga: organy nadzorcze są zobowiązane do ustanowienia i podania do publicznej wiadomości wykazu rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych oraz przekazania tego wykazu Europejskiej Radzie Ochrony Danych (EROD) (artykuł 35 ust. 4)[17]. Kryteria określone powyżej mogą pomóc organom nadzorczym w ustanowieniu takiego wykazu, z możliwością dodawania z czasem dalszych konkretnych treści, w razie potrzeby. Na przykład przetwarzanie wszelkiego rodzaju danych biometrycznych lub danych dotyczących dzieci również można uznać za istotne do ustanowienia wykazu zgodnie z artykułem 35 ust. 4.

### b) Kiedy dokonanie DPIA nie jest wymagane? Kiedy przetwarzanie *„z dużym prawdopodobieństwem nie spowoduje wysokiego ryzyka"* lub już zostało zatwierdzone lub posiada podstawę prawną.

DPIA nie jest wymagana w następujących przypadkach:

- przetwarzanie „*z dużym prawdopodobieństwem nie spowoduje wysokiego ryzyka naruszenia praw lub wolności osób fizycznych"* (artykuł 35 ust. 1);

[17] W tym kontekście *„Jeżeli wykazy takie obejmują czynności przetwarzania związane z oferowaniem towarów lub usług osobom, których dane dotyczą, lub z monitorowaniem ich zachowania w kilku państwach członkowskich lub mogące znacznie wpłynąć na swobodny przepływ danych osobowych w Unii, przed przyjęciem takich wykazów właściwy organ nadzorczy stosuje mechanizm spójności, o którym mowa w art. 63"* (artykuł 35 ust. 6)

- charakter, zakres, kontekst i cele przetwarzania są bardzo podobne to przetwarzania, dla którego została dokonana DPIA. W takich przypadkach mogą być wykorzystane wyniki DPIA przeprowadzonej dla podobnego przetwarzania (artykuł 35 ust. 1)[18];

- gdy operacja przetwarzania ma podstawę prawną w prawie UE lub państwie członkowskiego i wstępna DPIA nie musi być przeprowadzana, gdy prawo reguluje określoną operację przetwarzania oraz gdy DPIA, zgodnie ze standardami RODO, już została dokonana w ramach ustanowienia tej podstawy prawnej (artykuł 35 ust. 10)[19];

- gdy przetwarzanie uwzględnione jest w opcjonalnym wykazie (ustanowionym przez organ nadzorczy) operacji przetwarzania niepodlegających wymogowi dokonania DPIA (artykuł 35 ust. 5)[20]. Taki wykaz może zawierać czynności przetwarzania, które są zgodne z warunkami określonymi przez ten organ, w szczególności poprzez wytyczne, określone decyzje lub upoważnienia, zasady zapewnienia zgodności, etc. (np. we Francji upoważnienia, wyłączenia, uproszczone zasady, pakiety zapewniania zgodności…). W takich przypadkach, oraz z zastrzeżeniem dokonania ponownej oceny przez właściwy organ nadzorczy, DPIA nie jest wymagana, ale tylko wówczas, gdy przetwarzanie ściśle wchodzi w zakres właściwych procedur wskazanych w wykazie i nadal w pełni zapewnia zgodność z istotnymi wymogami.

### c) A co z już istniejącymi operacjami przetwarzania? Oceny skutków dla ochrony danych są niezbędne dla operacji prowadzonych po 25 maja 2018 r. lub operacji, które zostały znacząco zmienione.

Wymóg dokonania DPIA dotyczy operacji przetwarzania spełniających kryteria wskazane w artykule 35 i rozpoczętych po tym, jak RODO zacznie mieć zastosowanie w dniu 25 maja 2018 r.

GR Art. 29 zdecydowanie zaleca dokonanie DPIA dla operacji przetwarzania już trwających przed 25 maja 208 r. Ponadto, gdy to konieczne, *„W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych*" (artykuł 35 ust. 11)[21].

Ponadto miałoby to miejsce, gdyby została dokonana znacząca zmiana w operacji przetwarzania[22] po 25 maja 2018 r., na przykład ponieważ została wprowadzona do użytku nowa technologia lub ponieważ dane osobowe są wykorzystywane w innym celu. W tego typu przypadkach przetwarzanie staje się w rezultacie nową operacją przetwarzania danych i może wymagać DPIA.

DPIA należy oczywiście poddać przeglądowi, gdy zmienia się ryzyko wynikające z operacji przetwarzania (artykuł 35 ust. 11).

---

[18] *„Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę"*

[19] Proszę zauważyć, że gdy DPIA została dokonana na etapie propozycji podstawy prawnej, z dużym prawdopodobieństwem będzie wymagała przeglądu przed rozpoczęciem operacji, ponieważ przyjęta podstawa prawna może różnić się od propozycji w sposób, który wpływa na skutki dla ochrony danych i prywatności.

[20] W tym zakresie *„Jeżeli wykazy takie obejmują czynności przetwarzania związane z oferowaniem towarów lub usług osobom, których dane dotyczą, lub z monitorowaniem ich zachowania w kilku państwach członkowskich lub mogące znacznie wpłynąć na swobodny przepływ danych osobowych w Unii, przed przyjęciem takich wykazów właściwy organ nadzorczy stosuje mechanizm spójności, o którym mowa w art. 63"* (artykuł 35 ust. 6)

[21] Artykuł 35 ust. 10 wyraźnie wyklucza tylko zastosowanie artykułu 35 ust. 1 – 7.

[22] W zakresie kontekstu, ryzyka, celów, przetwarzanych danych osobowych, odbiorców, połączenia danych, środków bezpieczeństwa lub międzynarodowego przekazywania.

Ryzyko może się zmienić w rezultacie zmiany jednego z komponentów operacji przetwarzania (dane, środki wspierające, źródła ryzyka, potencjalny wpływ, zagrożenia, etc.) lub ponieważ ewoluuje kontekst przetwarzania (cel, funkcjonalności, etc.). Systemy przetwarzania danych mogą ewoluować szybko i mogą powstać nowe słabe strony. W związku z tym należy zauważyć, że przegląd DPIA jest nie tylko przydatny dla ciągłego usprawniania, ale również kluczowy do utrzymania poziomu ochrony danych w zmieniającym się środowisku przez długi czas.

I wreszcie DPIA może również stać się konieczna, ponieważ zmienił się kontekst organizacyjny i społeczny czynności przetwarzania, na przykład dlatego, że skutki określonych zautomatyzowanych decyzji stały się ważniejsze, nowe kategorie osób fizycznych stają się podatne na dyskryminację lub dane mają być przekazywane odbiorcom zlokalizowanym w kraju, który wyszedł z UE.

W ramach dobrych praktyk, DPIA należy nieustannie dokonywać dla istniejących czynności przetwarzania. Jednak należy dokonać ponownej oceny po 3 latach, być może wcześniej, w zależności od charakteru przetwarzania i stopnia zmiany operacji przetwarzania lub ogólnych okoliczności. Taka ocena jest również zalecana dla przetwarzania danych, które było prowadzone przed 25 maja 2018 r. i w związku z tym nie podlegało DPIA, aby zapewnić, że 3 lata po tej dacie lub wcześniej, w zależności od kontekstu, ryzyko naruszenia praw lub wolności nadal będzie zminimalizowane.

## C. Jak przeprowadzić DPIA?

### a. W jakim momencie powinna zostać przeprowadzona DPIA? Przed rozpoczęciem przetwarzania.

DPIA powinna zostać przeprowadzona *„przed rozpoczęciem przetwarzania”* (artykuł 35 ust. 1, 35 ust. 10, motyw 90 i 93). Jest to zgodne z ochroną danych w fazie projektowania oraz domyślną ochroną danych (artykuł 25 i motyw 78).

DPIA powinna zostać rozpoczęta tak wcześnie jak jest to praktyczne w projektowaniu operacji przetwarzania danych, nawet jeśli niektóre operacje przetwarzania będą wciąż nieznane. Aktualizowanie DPIA przez cały cykl życia projektu zapewni, iż ochrona danych osobowych wzięta będzie brana pod uwagę i wspierane będą procesy tworzenia rozwiązań zapewniających przestrzeganie rozporządzenia. Może być konieczne powtórzenie poszczególnych etapów oceny w miarę postępów, ponieważ wybór określonych środków technicznych i organizacyjnych może wpłynąć na wagę lub prawdopodobieństwo wystąpienia ryzyka wynikającego z przetwarzania.

Fakt, że DPIA może wymagać aktualizacji po rozpoczęciu przetwarzania nie jest zasadnym powodem odroczenia lub niepodjęcia DPIA. W niektórych przypadkach DPIA będzie ciągłym procesem. Na przykład gdy operacja przetwarzania jest dynamiczna i podlega ciągłym zmianom. Przeprowadzenie DPIA to ciągły proces, a nie czynność jednorazowa.

### b. Kto jest zobowiązany do przeprowadzenia DPIA? Administrator danych, z DPO i podmiotem przetwarzającym (podmiotami przetwarzającymi).

Administrator jest odpowiedzialny za zapewnienie przeprowadzenia DPIA (artykuł 35 ust. 2). Przeprowadzenie DPIA może zostać dokonane przez kogoś innego, wewnątrz albo na zewnątrz organizacji, natomiast to administrator pozostaje ostatecznie odpowiedzialny za to zadanie.

Dokonując oceny skutków dla ochrony danych, administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony (artykuł 35 ust. 2) i ta konsultacja, jak również decyzja podjęta, powinna zostać udokumentowana w DPIA. DPO powinien również monitorować wykonanie DPIA (artykuł 39 ust. 1 lit. c.) Dalsze wytyczne wskazane są w wytycznych Grupy Roboczej dotyczących inspektora ochrony danych 16/EN WP 243.

Jeśli przetwarzanie danych dokonywane jest całkowicie albo częściowo przez podmiot przetwarzający, podmiot ten powinien uczestniczyć w przeprowadzeniu DPIA i udzielać niezbędnych informacji.

Administrator powinien *„zasięgnąć opinii osób, których dane dotyczą, lub ich przedstawicieli* (artykuł 35 ust. 9) *„w stosownych przypadkach”*. GR Art. 29 stoi na stanowisku, że:

- opinii tych można szukać w różny sposób, zależnie od kontekstu (np. wewnętrzne lub zewnętrzne badania dotyczące celu i środków przetwarzania, formalne pytanie do przedstawicieli pracowników lub związków zawodowych lub badanie przesłane przyszłym klientom administratora);
- jeśli ostateczna decyzja administratora różni się od poglądów osób, których dane dotyczą, powody wykonania albo niewykonania decyzji powinny zostać udokumentowane;
- podmiot przetwarzający powinien również udokumentować uzasadnienie, aby nie zasięgać opinii osób, których dane dotyczą, jeśli uzna, że nie jest to właściwe.

Wreszcie dobrą praktyką jest definiowanie i dokumentowanie innych szczególnych ról i obowiązków, w zależności od polityki wewnętrznej, procesów i zasad, np.:

- w przypadku gdy poszczególne jednostki biznesowe mogą zaproponować przeprowadzenie DPIA, jednostki te powinny następnie dostarczyć wkład do DPIA i być zaangażowane w proces walidacji;

- w stosownych przypadkach zaleca się zasięganie opinii niezależnych ekspertów różnych zawodów[23] (prawnicy, technicy, eksperci ds. bezpieczeństwa, socjologowie, etycy itp.);

- role i obowiązki podmiotów przetwarzających muszą być określone w umowie; a DPIA musi być przeprowadzona z pomocą podmiotu przetwarzającego, biorąc pod uwagę charakter przetwarzania i informacje dostępne dla podmiotu przetwarzającego (artykuł 28 ust. 3 lit. f);

- DPO może zasugerować, aby administrator przeprowadził DPIA dla konkretnych operacji przetwarzania, powinien pomagać zainteresowanym stronom w zakresie metodologii, pomagać dokonać ewaluacji jakości oceny ryzyka, pomagać ocenić czy ryzyko szczątkowe jest dopuszczalne oraz przyczyniać się do wiedzy odpowiedniej w kontekście administratora;

- Jeśli zostanie wyznaczony, główny urzędnik ds. bezpieczeństwa 9Chief Information Security Officer - CISO) i/lub dział IT, powinni wspomóc administratora i mogą zaproponować dokonanie DPIA dla określonej operacji przetwarzania, w zależności od potrzeb związanych z bezpieczeństwem lub potrzebami operacyjnymi.

### c. Jaka jest metoda przeprowadzania DPIA? Różne metody, ale wspólne kryteria.

RODO określa minimalny zakres DPIA (art. 35 ust. 7 i motywy 84 i 90):

- *„opis planowanych operacji przetwarzania i celów przetwarzania”;*

- *„ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne”;*

- *„ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą”;*

- *„środki planowane w celu:*

  - *zaradzenia ryzyku,*

  - *przestrzegania rozporządzenia”.*

Poniższy rysunek ilustruje ogólny proces iteracyjny przeprowadzania DPIA[24]:

[23] Zalecenia dotyczące ram oceny wpływu na prywatność w Unii Europejskiej, Dokument D3: Http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

[24] Należy podkreślić, że przedstawiony tutaj proces jest iteracyjny: w praktyce prawdopodobne jest, że każdy z etapów jest wielokrotnie ponownie poddawany przeglądowi przed zakończeniem DPIA.


Zgodność z kodeksem postępowania (artykuł 40) powinna być wzięta pod uwagę (artykuł 38 ust. 8) podczas oceniania skutków przetwarzania danych. Może to być przydatne do wykazania, że zostały wybrane lub wprowadzone odpowiednie środki, pod warunkiem że kodeks postępowania jest odpowiedni do danej operacji przetwarzania.

Wszystkie istotne wymogi określone w RODO stanowią szerokie, ogólne ramy projektowania i dokonywania DPIA. Praktyczne wdrożenie DPIA będzie zależeć od wymagań określonych w RODO, które mogą być uzupełnione bardziej szczegółowymi wskazówkami praktycznymi. To otwiera drogę do skalowalności, co oznacza, że nawet mały administrator danych może zaprojektować i wdrożyć odpowiednią DPIA.

Motyw 90 RODO wymienia szereg elementów DPIA, która pokrywają się z dobrze zdefiniowanymi elementami zarządzania ryzykiem ( np. ISO 31000[25]). W zakresie zarządzania ryzykiem DPIA ma na celu "zarządzanie ryzykiem" w odniesieniu do praw i wolności osób fizycznych przy użyciu następujących trzech procesów:

- ustalenie kontekstu: *„uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz źródła ryzyka”;*
- ocena ryzyka: *„ocenić konkretne prawdopodobieństwo i powagę tego wysokiego ryzyka*”;

[25] Procesy zarządzania ryzykiem: komunikacja i konsultacje, określanie kontekstu, ocena ryzyka, zarządzanie ryzykiem, monitorowanie i przegląd (zob. definicje oraz spis treści w podglądzie ISO 31000: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

- przeciwdziałanie ryzyku: *„minimalizować to ryzyko*", *"zapewniać ochronę danych osobowych"* i *„wykazać przestrzeganie niniejszego rozporządzenia".*

Uwaga: DPIA zgodnie z RODO jest narzędziem zarządzania ryzykiem naruszenia praw osób, których dane dotyczą, a tym samym przyjmuje stanowisko tych osób, jak to ma miejsce w innych dziedzinach (np. zabezpieczenia społeczne). Natomiast zarządzanie ryzykiem w innych dziedzinach (np. bezpieczeństwo informacji) skierowane jest na organizację. „Ryzyko" jest scenariuszem opisującym wydarzenie i jego konsekwencje szacowane pod względem stopnia wagi zdarzenia i prawdopodobieństwa. Artykuł 35 odnosi się do wysokiego ryzyka naruszenia *„praw lub wolności osób fizycznych".* Jak wskazano w Oświadczeniu Grupy Roboczej Artykułu 29 ds. Ochrony Danych (GR Art. 29) 14/EN WP218 (str. 4), odniesienie do "*praw i wolności*" osób, których dane dotyczą, dotyczy przede wszystkim prawa do prywatności, ale może także obejmować inne podstawowe prawa, takie jak wolność słowa, wolność myśli, swoboda przemieszczania się, zakaz dyskryminacji, prawo do wolności, sumienia i religii.

RODO zapewnia administratorom danych elastyczność w określeniu dokładnej struktury i formy DPIA, aby umożliwić dostosowanie do istniejących praktyk zawodowych. W UE i na świecie istnieją różne ustalone procesy uwzględniające elementy opisane w motywie 90. Jednakże, niezależnie od jej formy, DPIA musi być realną oceną ryzyka, umożliwiającą administratorom podejmowanie działań mających na celu ich rozwiązanie.

Mogą być wykorzystane różne metodologie postępowania (w Załączniku 1 zobacz przykłady metodologii ochrony danych i metod oceny skutków dla ochrony danych) w celu realizacji podstawowych wymagań określonych w RODO.

By umożliwić istnienie różnych podejść, przy jednoczesnym umożliwieniu administratorom zapewnienia zgodności z RODO, ustalono wspólne kryteria (patrz załącznik 2). Wyjaśniają one podstawowe wymogi rozporządzenia, ale zapewniają wystarczający zakres dla różnych form wdrożenia. Kryteria te można wykorzystać do wykazania, że określona metodologia DPIA spełnia standardy wymagane przez RODO.

GR Art. 29 zachęca do opracowania sektorowych ram DPIA. Wynika to z tego, że mogąc korzystać z wiedzy sektorowej, DPIA może dotyczyć specyfiki konkretnego typu operacji przetwarzania (np.: poszczególnych rodzajów danych, aktywów przedsiębiorstwa, potencjalnych skutków, ryzyk, środków). Oznacza to, że DPIA może rozwiązywać problemy, które pojawiają się w danym sektorze gospodarczym lub podczas korzystania z określonych technologii albo przy określonych operacjach przetwarzania.

### d. Czy DPIA powinna zostać opublikowana? Tak, albo w całości albo w części, ponadto powinna zostać przekazane organowi nadzorczemu w przypadku uprzednich konsultacji.

Publikowanie DPIA nie jest wymagane przepisami RODO. Pozostaje w gestii administratora. Administratorzy danych powinni jednak rozważyć, co najmniej częściowe, opublikowanie DPIA. Celem takiego działania byłoby przyczynienie się do zwiększenia zaufania w stosunku do operacji przetwarzania danych u administratora, a także wykazanie rozliczalności i przejrzystości. Szczególnie dobrą praktyką jest publikowanie wyników DPIA w przypadku, w którym operacja przetwarzania ma wpływ na społeczeństwo. Może to być szczególnie możliwe w przypadku, gdy organ publiczny przeprowadza DPIA.

Opublikowana DPIA nie musi zawierać całej oceny, zwłaszcza gdy DPIA mogłaby przedstawić konkretne informacje dotyczące zagrożeń dla bezpieczeństwa administratora danych lub ujawnić

tajemnice handlowe lub poufne informacje handlowe. Mogłaby się składać tylko z podsumowania najważniejszych ustaleń DPIA.

Ponadto, gdy DPIA ujawnia wysokie ryzyko szczątkowe, administrator danych będzie zmuszony zwrócić się o uprzednie konsultacje w celu przetwarzania do organu nadzorczego (art. 36 ust. 1). W ramach tej procedury należy dostarczyć DPIA (art. 36 ust. 3 lit. e).

## D. Kiedy należy skonsultować się z organem nadzorczym? Gdy ryzyko szczątkowe jest wysokie.

Jak wyjaśniono powyżej:

- DPIA jest wymagana gdy przetwarzanie danych *„może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych”* (artykuł 35 ust. 1, zobacz III.B.a). Dla przykładu, przetwarzanie danych dotyczących stanu zdrowia na dużą skalę, może powodować wysokie ryzyko i wymaga DPIA;

- Następnie obowiązkiem administratora jest ocena ryzyka naruszenia praw lub wolności osób fizycznych i zidentyfikować środki[26] mające zminimalizować to ryzyko do dopuszczalnych poziomów i wykazać przestrzeganie RODO (artykuł 35 ust. 7, zobacz III.C.c). Przykładem może być przechowywanie danych osobowych na komputerach przenośnych z odpowiednimi technicznymi i organizacyjnymi środkami bezpieczeństwa (skuteczne szyfrowanie całego dysku, efektywne zarządzanie kluczami, odpowiednia kontrola dostępu, zabezpieczone kopie zapasowe itp.) dodatkowo do istniejących polityk (zawiadomienie, zgoda, prawo dostępu, prawa do sprzeciwu itp.).

W powyższym przykładzie z komputerami przenośnymi ryzyko było zarządzane przez administratora danych i po zapoznaniu się z art. 36 ust. 1 oraz motywami 84 i 94, przetwarzanie może nastąpić bez konsultacji z organem nadzorczym. To w przypadkach, gdy administratorzy danych nie mogą w wystarczającym stopniu zniwelować zidentyfikowanego ryzyka (tj. ryzyko szczątkowe pozostaje wysokie), administrator danych musi skonsultować się z organem nadzorczym.

Przykład niedopuszczalnego wysokiego ryzyka szczątkowego obejmuje przypadki, w których osoby, których dotyczą dane, mogą napotkać znaczące, a nawet nieodwracalne konsekwencje, których nie mogą pokonać lub gdy wydaje się oczywiste, że wystąpi ryzyko.

Gdy administrator danych nie może znaleźć wystarczających środków (tj. gdy ryzyko szczątkowe jest nadal wysokie), konieczna będzie konsultacja z organem nadzorczym.

Ponadto administrator będzie musiał skontaktować się z organem nadzorczym w każdym przypadku, gdy prawo państwa członkowskiego wymaga, aby administratorzy konsultowali się z organem nadzorczym i/lub uzyskiwali jego uprzednią zgodę na przetwarzanie danych osobowych przez administratora do celów wykonania zadania realizowanego przez administratora w interesie publicznym, w tym przetwarzania w związku z ochroną socjalną i zdrowiem publicznym (artykuł 36 ust. 5)

Należy jednak stwierdzić, że niezależnie od tego, czy wymagana jest konsultacja z organem w zależności od poziomu ryzyka szczątkowego, nadal istnieć może obowiązek zachowania rejestru DPIA i aktualizowania DPIA w odpowiednim czasie.

[26] Uwzględniając istniejące wytyczne EROD i organów nadzorczych, biorąc pod uwagę aktualny stan wiedzy i koszty wdrożenia, zgodnie z art. 35 ust. 1.

## IV. Wnioski i Rekomendacje

Dla administratorów danych DPIA są użytecznym sposobem na wdrożenie systemów przetwarzania danych zgodnych z RODO i mogą być obowiązkowe dla niektórych rodzajów przetwarzania. Są skalowalne i mogą przyjmować różne formy, ale RODO określa podstawowe wymagania skutecznej DPIA. Administratorzy danych powinni postrzegać DPIA jako użyteczną i pozytywną czynność, która pomaga w zapewnieniu zgodności z prawem.

Artykuł 24 ust. 1 określa podstawowy zakres odpowiedzialności administratora danych za zgodność z RODO:

*„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."*

DPIA jest kluczowym elementem przestrzegania rozporządzenia, w którym planowane jest lub ma miejsce przetwarzanie danych obarczone wysokim ryzykiem. Oznacza to, że administratorzy danych powinni używać kryteriów określonych w niniejszym dokumencie, aby ustalić, czy DPIA musi być przeprowadzona. Polityka wewnętrzna administratora danych może rozszerzyć tę listę poza wymagania prawne wskazane w RODO. Takie zachowanie powinno spowodować zwiększenie zaufania osób, których dane dotyczą i innych administratorów.

Gdy istnieje duże prawdopodobieństwo przetwarzania obarczonego wysokim ryzykiem administrator musi:

- wybrać metodologię przeprowadzenia DPIA (przykłady w Załączniku 1), która spełni kryteria wskazane w Załączniku 2, albo określić i wdrożyć systematyczny proces DPIA, który:
    - jest zgodny z kryteriami w Załączniku 2;
    - jest zintegrowany z istniejącymi procesami projektowania, rozwoju, zmian, ryzyka i przeglądu operacyjnego zgodnie z wewnętrznymi procedurami, kontekstem i kulturą;
    - angażuje odpowiednie zainteresowane strony i jasno określa ich obowiązki (administrator, DPO, osoby, których dane dotyczą lub ich przedstawiciele, przedsiębiorstwa, usługi techniczne, podmioty przetwarzające, urzędnicy ds. bezpieczeństwa informacji itp.);
- dostarczyć sprawozdanie z DPIA do właściwego organu nadzorczego, jeśli jest to wymagane;
- skonsultować się z organem nadzorczym, jeśli nie zdołał określić wystarczających środków w celu zminimalizowania ryzyka;
- przeanalizować poddawać okresowym przeglądom DPIA i procesy przetwarzania, których dotyczyło, przynajmniej w przypadku zmiany ryzyka związanego z operacją przetwarzania;
- dokumentować podjęte decyzje.

# Załącznik 1 - Przykłady istniejących ram DPIA w Unii Europejskiej

RODO nie określa, który proces DPIA powinien być stosowany, lecz umożliwia administratorom danych wprowadzenie ram, które pasują do istniejącej praktyki zawodowej, pod warunkiem uwzględnienia elementów opisanych w art. 35 ust. 7. Takie ramy mogą być dostosowane do administratora danych lub wspólne w danej branży. Poprzednio opublikowane ramy opracowane przez organy ochrony danych UE i ramy sektorowe UE obejmują (ale nie ograniczają się do):

Przykłady ogólnych ram UE:

- DE: Standard Data Protection Model, V.1.0 – Trial version, 2016[27].
  https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD), Agencia española de protección de datos (AGPD), 2014.
  https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR: Privacy Impact Assessment (PIA), Commission nationale de l'informatique et des libertés (CNIL), 2015.
  https://www.cnil.fr/fr/node/15798
- UK: Conducting privacy impact assessments code of practice, Information Commissioner's Office (ICO), 2014.
  https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Przykłady unijnych ram sektorowych:

- Privacy and Data Protection Impact Assessment Framework for RFID Applications[28].
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems[29]
  http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

[27] Jednomyślnie i pozytywnie potwierdzone (przy wstrzymaniu się od głosu Bawarii) przez 92. Konferencję niezależnych organów ochrony danych federacji i krajów związkowych w Kühlungsborn w dniach 9-10 listopada 2016 r.

[28] Zobacz również:
- Zalecenie Komisji z dnia 12 maja 2009 r. w sprawie wdrażania zasad ochrony prywatności i ochrony danych w zastosowaniach wspieranych identyfikacją radiową,
  https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
- Opinia 9/2011 na temat zmienionej propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID,
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_en.pdf

[29] Zobacz Opinię 7/2013 w sprawie szablonu oceny skutków w zakresie ochrony danych na potrzeby inteligentnych sieci i inteligentnych systemów pomiarowych, opracowanego przez grupę ekspertów nr 2 w ramach grupy zadaniowej Komisji ds. inteligentnych sieci,

Międzynarodowa norma również dostarczy wytyczne dotyczące metodologii stosowanych przy dokonywaniu DPIA (ISO / IEC 29134[30]).

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf

[30] ISO/IEC 29134 (projekt), Information technology – Security techniques - Metodyka szacowania skutków dla prywatności, Międzynarodowa Organizacja Normalizacyjna (ISO)

## Załącznik 2 - Kryteria dopuszczalnej DPIA

GR Art. 29 proponuje następujące kryteria, które administratorzy danych mogą wykorzystać do oceny, czy DPIA lub metodologia przeprowadzania DPIA są wystarczająco obszerne, aby zapewnić zgodność z RODO:

- ☐ Zapewniony jest systematyczny opis planowanych operacji przetwarzania (artykuł 35 ust. 7):
  - ☐ charakter, zakres, kontekst i cele przetwarzania są uwzględnione (Motyw 90);
  - ☐ dokumentowane dane osobowe, odbiorcy oraz okres przechowywania danych osobowych;
  - ☐ dostarczony jest funkcjonalny opis operacji przetwarzania;
  - ☐ zidentyfikowane są aktywa, na których opierają się dane osobowe (sprzęt, oprogramowanie, sieci, ludzie, dokumenty papierowe lub papierowe kanały transmisji);
  - ☐ uwzględnia się zgodność z zatwierdzonymi kodeksami postępowania (art. 35 ust. 8);
- ☐ Ocena niezbędności i proporcjonalności (artykuł 35 ust. 7 lit. b):
  - ☐ Określono środki mające na celu spełnienie wymogów rozporządzenia (art. 35 ust. 7 lit. d) i motyw 90), biorąc pod uwagę:
    - ☐ Środki wpływające na niezbędność i proporcjonalność przetwarzania w oparciu o:
      - ☐ konkretny, wyraźny i prawnie uzasadniony cel(e) (artykuł 5 ust. 1 lit. b);
      - ☐ Zgodność przetwarzania z prawem (artykuł 6);
      - ☐ adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów (artykuł 5 ust. 1 lit. c);
      - ☐ ograniczenie okresu przechowywania (artykuł 5 ust. 1 lit. e);
    - ☐ Środki przyczyniające się do praw osób, których dane dotyczą:
      - ☐ informacje udzielone osobie, której dane dotyczą (artykuł 12, 13 i 14);
      - ☐ prawo dostępu i przekazywania danych (artykuł 15 i 20);
      - ☐ prawo do sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu (artykuł 16-19 i 21);
      - ☐ odbiorcy;
      - ☐ podmioty przetwarzające (artykuł 28);
      - ☐ zabezpieczenia dotyczące przekazywania danych (Rozdział V);
      - ☐ uprzednie konsultacje (artykuł 36);
- ☐ Zarządzenie ryzykiem naruszenia praw lub wolności osób (artykuł 35 ust. 7):
  - ☐ Uwzględnienie źródła, charakteru, specyfiki i powagi tego ryzyka (porównaj motyw 84); lub dokładniej, w odniesieniu do każdego ryzyka (nieuprawnionego dostępu, niepożądanej modyfikacji i zniknięcia danych) z punktu widzenia osób, których dane dotyczą:
    - ☐ Uwzględniono źródło ryzyka (motyw 90);
    - ☐ Potencjalne skutki dla praw lub wolności osób, których dane dotyczą, są identyfikowane w przypadku nieuprawnionego dostępu, niepożądanej modyfikacji i zniknięcia danych;
    - ☐ zagrożenia, które mogłyby prowadzić do nieuprawnionego dostępu, niepożądanej modyfikacji i zniknięcia danych;
    - ☐ oszacowano prawdopodobieństwo i powagę tego ryzyka (motyw 90);
  - ☐ ustalono środki planowane w celu zaradzenia ryzyku (artykuł 35 ust. 7 lit. d i Motyw 90);
- ☐ zaangażowanie zainteresowanych stron:

- ☐ zasięgnięto konsultacji DPO (artykuł 35 ust. 2);
- ☐ zasięgnięto opinii osób, których dane dotyczą lub ich przedstawicieli (artykuł 35 ust. 9);