17/PL

WP 248 rev.01

# Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679

**Przyjęte w dniu 4 kwietnia 2017 r.**

**Ostatnio zmienione i przyjęte w dniu 4 października 2017 r.**

**GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH**

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

uwzględniając art. 29 i 30 tej dyrektywy,

uwzględniając swój regulamin wewnętrzny,

**PRZYJMUJE NINIEJSZE WYTYCZNE:**

## Spis treści

## I. Wprowadzenie

Rozporządzenie 2016/679[1] (RODO) będzie obowiązywało od dnia 25 maja 2018 r. W art. 35 RODO – podobnie jak w dyrektywie 2016/680[2]– wprowadzono pojęcie oceny skutków dla ochrony danych[3].

Ocena skutków dla ochrony danych jest procesem pozwalającym opisać przetwarzanie oraz ocenić jego konieczność i proporcjonalność, a także mającym wspomóc zarządzanie ryzykiem naruszenia praw i wolności osób fizycznych wynikającym z przetwarzania danych osobowych[4] poprzez ocenę ryzyka i określenie środków pozwalającym zaradzić tym czynnikom ryzyka. Oceny skutków dla ochrony danych są ważnym narzędziem rozliczalności, ponieważ ułatwiają administratorom nie tylko przestrzeganie wymogów określonych w RODO, ale także wykazanie, że podjęto odpowiednie środki w celu zapewnienia przestrzegania przepisów RODO (zob. również art. 24)[5]. Innymi słowy **ocena skutków dla ochrony danych jest procesem budowania i wykazywania zgodności**.

Na mocy RODO nieprzestrzeganie wymogów dotyczących oceny skutków dla ochrony danych może spowodować nałożenie grzywien przez właściwy organ nadzorczy. Nieprzeprowadzenie oceny skutków dla ochrony danych, gdy przetwarzanie podlega takiej ocenie (art. 35 ust. 1 i 3–4), nieprawidłowe przeprowadzenie oceny skutków dla ochrony danych (art. 35 ust. 2 i 7–9) lub brak

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

[2] W innych kontekstach w odniesieniu do tej samej koncepcji często stosuje się pojęcie „ocena skutków w zakresie prywatności".

[3] Art. 27 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 stanowi również, że ocena skutków w zakresie prywatności jest potrzebna, ponieważ „przetwarzanie [...] może skutkować powstaniem wysokiego ryzyka naruszenia praw i wolności osób fizycznych".

[4] RODO nie zawiera jako takiej formalnej definicji pojęcia „ocena skutków dla ochrony danych", ale

- w art. 35 ust. 7 sprecyzowano, że ocena powinna zawierać co najmniej:
  - „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";
- jego znaczenie i rolę wyjaśniono w motywie 84 w następujący sposób: „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".

[5] Zob. również 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".

konsultacji z właściwym organem nadzorczym, gdy jest to wymagane (art. 36 ust. 3 lit. e)) mogą skutkować nałożeniem administracyjnej kary pieniężnej w wysokości do 10 mln EUR lub, w przypadku przedsiębiorstwa, do 2 % całkowitego rocznego obrotu w skali światowej w poprzednim roku budżetowym, w zależności od tego, która kwota jest wyższa.

## II. Zakres wytycznych

W niniejszych wytycznych uwzględniono:

- oświadczenie 14/EN WP 218 Grupy Roboczej Art. 29[6];
- wytyczne Grupy Roboczej Art. 29 dotyczące inspektora ochrony danych 16/EN WP 243[7];
- opinię Grupy Roboczej Art. 29 w sprawie ograniczenia celu 13/EN WP 203[8];
- normy międzynarodowe[9].

Zgodnie z przewidzianym w RODO podejściem opartym na analizie ryzyka przeprowadzenie oceny skutków dla ochrony danych nie jest obowiązkowe w przypadku każdej operacji przetwarzania. Przeprowadzenia oceny skutków dla ochrony danych wymaga się wyłącznie w przypadku, gdy przetwarzanie „może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych" (art. 35 ust. 1). Aby zapewnić spójną interpretację okoliczności, w których ocena skutków dla ochrony danych jest obowiązkowa (art. 35 ust. 3), niniejsze wytyczne mają na celu przede wszystkim wyjaśnienie tego pojęcia i przedstawienie kryteriów w odniesieniu do wykazów, które zostaną przyjęte przez organy ochrony danych zgodnie z art. 35 ust. 4.

Zgodnie z art. 70 ust. 1 lit. e) Europejska Rada Ochrony Danych będzie mogła wydawać wytyczne, zalecenia i najlepsze praktyki, zachęcając do spójnego stosowania RODO. Celem niniejszego dokumentu jest uprzedzenie takich przyszłych prac Europejskiej Rady Ochrony Danych i tym samym objaśnienie odpowiednich przepisów RODO, aby pomóc administratorom w przestrzeganiu prawa oraz aby zapewnić pewność prawa administratorom, którzy są zobowiązani do przeprowadzenia oceny skutków dla ochrony danych.

Niniejsze wytyczne mają na celu również promowanie opracowania:

- wspólnego unijnego wykazu operacji przetwarzania, w przypadku których ocena skutków dla ochrony danych jest obowiązkowa (art. 35 ust. 4);

---

[6] oświadczenie 14/EN WP 218 Grupy Roboczej Art. 29 dotyczące roli opartego na analizie ryzyka podejścia do ram prawnych w zakresie ochrony danych przyjęte w dniu 30 maja 2014 r.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

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

[8] Opinia Grupy Roboczej Art. 29 nr 03/2013 w sprawie ograniczenia celu 13/EN WP 203 przyjęta w dniu 2 kwietnia 2013 r.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[9] Np. ISO 31000:2009, Zarządzanie ryzykiem – Zasady i wytyczne, Międzynarodowa Organizacja Normalizacyjna (ISO); ISO/IEC 29134 (projekt), IT – Techniki bezpieczeństwa – ocena skutków w zakresie prywatności – Wytyczne, Międzynarodowa Organizacja Normalizacyjna (ISO).

- wspólnego unijnego wykazu operacji przetwarzania, w przypadku których ocena skutków dla ochrony danych nie jest konieczna (art. 35 ust. 5);
- wspólnych kryteriów dotyczących metody przeprowadzania oceny skutków dla ochrony danych (art. 35 ust. 5);
- wspólnych kryteriów dotyczących określania, kiedy należy skonsultować się z organem nadzorczym (art. 36 ust. 1);
- w stosownych przypadkach – zaleceń bazujących na doświadczeniach zgromadzonych w państwach członkowskich UE.

## III. Ocena skutków dla ochrony danych: wyjaśnienia przepisów rozporządzenia

W RODO na administratorów nakłada się obowiązek wdrożenia odpowiednich środków pozwalających zapewnić przestrzeganie przepisów RODO oraz możliwość wykazania przestrzegania tych przepisów, uwzględniając m.in. „ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia" (art. 24 ust. 1). Obowiązek przeprowadzania przez administratorów oceny skutków dla ochrony danych w określonych okolicznościach należy rozumieć w kontekście ich ogólnego obowiązku, jakim jest właściwe zarządzanie ryzykiem[10] związanym z przetwarzaniem danych osobowych.

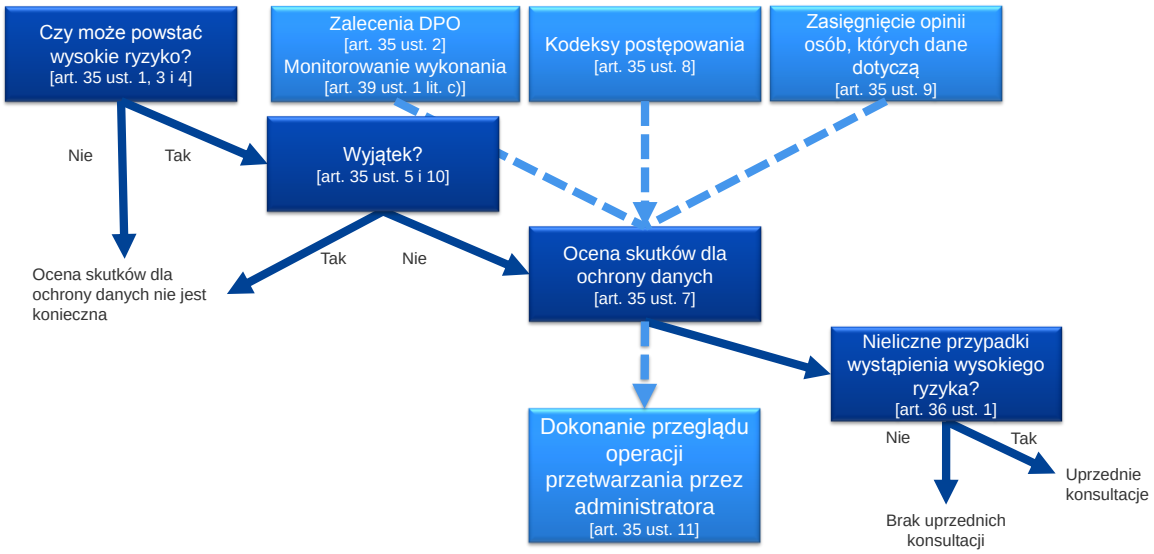
„Ryzyko" jest scenariuszem opisującym zdarzenie i jego konsekwencje, oszacowanym pod względem powagi i prawdopodobieństwa ryzyka. „Zarządzanie ryzykiem" można natomiast zdefiniować jako skoordynowane działania mające na celu kierowanie organizacją i kontrolowanie organizacji pod względem ryzyka.

W art. 35 odniesiono się do prawdopodobnego wysokiego ryzyka „naruszenia praw lub wolności osób fizycznych". Jak wskazano w oświadczeniu Grupy Roboczej Art. 29 dotyczącym roli opartego na analizie ryzyka podejścia do ram prawnych w zakresie ochrony danych, odniesienie do „praw i wolności" osób, których dane dotyczą, dotyczy przede wszystkim prawa do ochrony danych i prywatności, ale może również obejmować inne prawa podstawowe, takie jak wolność słowa, wolność myśli, swoboda poruszania się, zakaz dyskryminacji, prawo do wolności, wolność sumienia i wolność religii.

Zgodnie z przewidzianym w RODO podejściem opartym na analizie ryzyka przeprowadzenie oceny skutków dla ochrony danych nie jest obowiązkowe w przypadku każdej operacji przetwarzania. Przeprowadzenia oceny skutków dla ochrony danych wymaga się natomiast wyłącznie w przypadku, gdy dany rodzaj przetwarzania „może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych" (art. 35 ust. 1). Sam fakt niespełnienia warunków nakładających obowiązek przeprowadzenia oceny skutków dla ochrony danych nie zmniejsza jednak ogólnego obowiązku wdrożenia przez administratorów środków umożliwiających odpowiednie zarządzanie ryzykiem naruszenia prawa i wolności osób, których dane dotyczą. W praktyce oznacza to, że administratorzy muszą stale oceniać ryzyko powodowane przez czynności przetwarzania w celu określenia, kiedy dany rodzaj przetwarzania „może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych".

[10] Należy podkreślić, że aby być w stanie zarządzać ryzykiem naruszenia praw i wolności osób fizycznych, ryzyko to należy określić, przeanalizować, oszacować, ocenić, wyeliminować (np. złagodzić...) oraz poddawać regularnym przeglądom. Administratorzy nie mogą uniknąć odpowiedzialności, zawierając umowy ubezpieczeniowe na wypadek danego ryzyka.

Na poniższym wykresie przedstawiono podstawowe zasady związane z oceną skutków dla ochrony danych, o których mowa w RODO:




A. Czego dotyczy ocena skutków dla ochrony danych? Pojedyncza operacja przetwarzania lub zbiór podobnych operacji przetwarzania.

**Ocena skutków dla ochrony danych może dotyczyć pojedynczej operacji przetwarzania danych**. Art. 35 ust. 1 stanowi jednak, że „dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę". W motywie 92 dodaje się, 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".

**Do oceny wielu operacji przetwarzania**, które są podobne pod względem charakteru, zakresu, kontekstu, celu i ryzyka **można wykorzystać jedną ocenę skutków dla ochrony danych**. Celem ocen skutków dla ochrony danych jest bowiem systematyczne analizowanie nowych sytuacji, które mogłyby prowadzić do wysokiego ryzyka naruszenia praw i wolności osób fizycznych, dlatego nie ma potrzeby przeprowadzania oceny skutków dla ochrony danych (tj. operacji przetwarzania przeprowadzonych w określonym kontekście i w konkretnym celu) w przypadkach, które zostały już przeanalizowane. Może to mieć miejsce w przypadku wykorzystania podobnej technologii do gromadzenia tego samego rodzaju danych do tych samych celów. Na przykład grupa władz miejskich, które instalują podobny system CCTV, może przeprowadzić pojedynczą ocenę skutków dla ochrony danych obejmującą przetwarzanie danych przez oddzielnych administratorów; lub podmiot w branży kolejowej (pojedynczy administrator) może zainstalować nadzór wideo na wszystkich stacjach kolejowych w ramach jednej oceny skutków dla ochrony danych. Może to również dotyczyć podobnych operacji przetwarzania prowadzonych przez różnych administratorów danych. W takich przypadkach należy udostępniać lub upubliczniać referencyjną ocenę skutków dla ochrony danych, wdrożyć środki opisane w ocenie skutków dla ochrony danych oraz przedstawić uzasadnienie przeprowadzenia pojedynczej oceny skutków dla ochrony danych.

Jeżeli operacja przetwarzania obejmuje współadministratorów, muszą oni dokładnie określić swoje obowiązki. W swojej ocenie skutków dla ochrony danych administratorzy powinni określić, która strona ponosi odpowiedzialność za poszczególne środki mające na celu wyeliminowanie ryzyka oraz za ochronę praw i wolności osób, których dane dotyczą. Każdy administrator danych powinien wyrazić swoje potrzeby i dzielić się przydatnymi informacjami bez ujawniania tajemnic (np.: ochrona tajemnicy przedsiębiorstwa, własności intelektualnej, poufnych informacji handlowych) albo słabych stron.

**Ocena skutków dla ochrony danych może być również przydatna do oceny skutków dla ochrony danych wywieranych przez dany produkt technologiczny**, np. sprzęt lub oprogramowanie, gdy istnieje prawdopodobieństwo, że różni administratorzy danych będą korzystać z niego do przeprowadzania różnych operacji przetwarzania. Oczywiście administrator danych wdrażający produkt nadal jest zobowiązany do przeprowadzenia własnej oceny skutków dla ochrony danych w odniesieniu do tego konkretnego procesu wdrażania, ale w stosownych przypadkach może poinformować o tym fakcie za pomocą oceny skutków dla ochrony danych przygotowanej przez dostawcę produktu. Przykładem może być związek między producentami inteligentnych liczników a przedsiębiorstwami użyteczności publicznej. Każdy dostawca produktu lub podmiot przetwarzający powinien dzielić się przydatnymi informacjami bez ujawniania tajemnic i bez stwarzania zagrożeń dla bezpieczeństwa poprzez ujawnienie słabych stron.

B. Które operacje przetwarzania podlegają ocenie skutków dla ochrony danych? Z wyjątkiem operacji, które „mogą powodować wysokie ryzyko".

W niniejszej sekcji opisano sytuacje, w których przeprowadzenie oceny skutków dla ochrony danych jest obowiązkowe oraz sytuacje, w których nie jest to konieczne.

**O ile operacja przetwarzania nie stanowi wyjątku (rozdział III sekcja B lit. a)), ocenę skutków dla ochrony danych należy przeprowadzić wówczas, gdy operacja przetwarzania „może powodować wysokie ryzyko" (rozdział III sekcja B lit. b)).**

a) Kiedy przeprowadzenie oceny skutków dla ochrony danych jest obowiązkowe? Gdy przetwarzanie „może powodować wysokie ryzyko".

W RODO nie wymaga się przeprowadzenia oceny skutków dla ochrony danych w odniesieniu do każdej operacji przetwarzania, która może powodować ryzyko naruszenia praw i wolności osób fizycznych. Przeprowadzenie oceny skutków dla ochrony danych jest obowiązkowe wyłącznie w przypadku, gdy przetwarzanie „może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych" (art. 35 ust. 1 zilustrowany art. 35 ust. 3 i uzupełniony art. 35 ust. 4). Jest to szczególnie istotne przy wprowadzaniu nowej technologii przetwarzania danych[11].

W przypadkach, w których nie jest jasne, czy wymagane jest przeprowadzenie oceny skutków dla ochrony danych, Grupa Robocza Art. 29 zaleca jednak przeprowadzenie takiej oceny, ponieważ stanowi ona przydatne narzędzie ułatwiające administratorom przestrzeganie przepisów o ochronie danych.

[11] Więcej przykładów można znaleźć w motywach 89 i 91 oraz w art. 35 ust. 1 i 3.

Mimo że przeprowadzenie oceny skutków dla ochrony danych może być wymagane w innych okolicznościach, w art. 35 ust. 3 przedstawiono kilka przykładów, gdy operacja przetwarzania „może powodować wysokie ryzyko", w szczególności w przypadku:

- „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[12];
- 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[13]; lub
- c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie".

Jak wskazuje wyrażenie „w szczególności" w zdaniu wprowadzającym w art. 35 ust. 3 RODO, wymienione przykłady nie stanowią wyczerpującego wykazu. Mogą występować operacje przetwarzania „wysokiego ryzyka", których nie uwzględniono w wykazie, lecz stwarzają równie wysokie ryzyko. Wspomniane operacje przetwarzania powinny również podlegać ocenom skutków dla ochrony danych. Z tego powodu kryteria przedstawione poniżej wykraczają niekiedy poza proste wyjaśnienie tego, co należy rozumieć przez trzy przykłady podane w art. 35 ust. 3 RODO.

W celu przedstawienia bardziej konkretnego zbioru operacji przetwarzania wymagających przeprowadzenia oceny skutków dla ochrony danych ze względu na ich nieodłączne wysokie ryzyko, uwzględniając poszczególne elementy art. 35 ust. 1 i art. 35 ust. 3 lit. a)–c), wykaz, który zostanie przyjęty na szczeblu krajowym na mocy art. 35 ust. 4, i motywy 71, 75 i 91 oraz inne wspomniane w RODO odniesienia do operacji przetwarzania, które „mogą powodować wysokie ryzyko"[14], należy wziąć pod uwagę dziewięć następujących kryteriów.

1. Ocena lub punktacja, w tym profilowanie i prognozowanie w szczególności na podstawie „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). Przykładem tego może być instytucja finansowa sprawdzająca swoich klientów w referencyjnej bazie danych kredytowych lub bazie danych w zakresie przeciwdziałania praniu pieniędzy i zwalczania finansowania terroryzmu lub w bazie danych zawierającej informacje o nadużyciach finansowych; przykładem może być również przedsiębiorstwo biotechnologiczne bezpośrednio oferujące konsumentom badania genetyczne w celu oceny i prognozowania ryzyka wystąpienia choroby lub zagrożeń dla zdrowia, a także przedsiębiorstwo tworzące profile zachowań lub profile marketingowe w oparciu o wykorzystanie lub nawigację na swojej stronie internetowej.
2. Automatyczne podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku: przetwarzanie mające na celu podjęcie decyzji w sprawie osób, których dane dotyczą,

[12] Zob. motyw 71: „w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych".

[13] Zob. 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".

[14] Zob. np. motywy 75, 76, 92, 116.

wywołujących „skutki prawne wobec osoby fizycznej" lub decyzji, które „w podobny sposób istotnie na nią wpływają" (art. 35 ust. 3 lit. a)). Przykładowo przetwarzanie może prowadzić do wykluczenia lub dyskryminacji osób fizycznych. Przetwarzanie mające niewielki wpływ na osoby fizyczne lub niemające na nie żadnego wpływu nie spełnia tego konkretnego kryterium. Dalsze wyjaśnienia dotyczące tych pojęć zostaną przedstawione w przyszłych wytycznych Grupy Roboczej Art. 29 dotyczących profilowania.

3. Systematyczne monitorowanie: przetwarzanie wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, których dane dotyczą, w tym danych gromadzonych za pośrednictwem sieci lub ramach „systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie" (art. 35 ust. 3 lit. c))[15]. Ten rodzaj monitorowania stanowi jedno z kryteriów, ponieważ dane osobowe mogą być gromadzone w sytuacji, gdy osoby, których dane dotyczą, nie są świadome tego, kto gromadzi ich dane i w jaki sposób z nich korzysta. Ponadto osoby fizyczne mogą nie być w stanie uniknąć takiego rodzaju przetwarzania w przestrzeni publicznej (lub przestrzeni publicznie dostępnej).
4. Dane wrażliwe lub dane o charakterze wysoce osobistym: obejmują szczególne kategorie danych osobowych określone w art. 9 (np. informacje o poglądach politycznych obywateli) oraz dane osobowe dotyczące wyroków skazujących za przestępstwo lub naruszeń prawa zdefiniowane w art. 10. Przykładem może być szpital przechowujący dokumentację medyczną pacjentów lub prywatny detektyw przechowujący szczegółowe dane przestępców. Oprócz tych przepisów zawartych w RODO niektóre kategorie danych można uznać za zwiększające potencjalne ryzyko naruszenia praw i wolności osób fizycznych. Te dane osobowe uznaje się za szczególnie wrażliwe (zgodnie z powszechnym rozumieniem tego terminu), ponieważ są powiązane z gospodarstwem domowym i działalnością prywatną (taką jak łączność elektroniczna, której poufność należy chronić) lub ponieważ wpływają na wykonanie prawa podstawowego (takie jak dane dotyczące lokalizacji, których gromadzenie jest sprzeczne ze swobodą poruszania się), lub ponieważ ich naruszenie ma wyraźny wpływ na codzienne życie osób, których dane dotyczą (takie jak dane finansowe, które mogą zostać wykorzystane do oszustw płatniczych). W tym względzie może mieć znaczenie fakt, czy dane zostały upublicznione przez osobę, której dane dotyczą, czy przez osoby trzecie. Okoliczność, że dane osobowe są publicznie dostępne, może być uznana za czynnik w ocenie, jeżeli zgodnie z założeniami dane te miały być dalej wykorzystywane do określonych celów. Kryterium to może również obejmować dane takie jak dokumenty osobiste, wiadomości e-mail, pamiętniki, notatki z e-czytników wyposażonych w funkcję notatnika oraz dane mające bardzo osobisty charakter zawarte w aplikacjach rejestrujących codzienną aktywność.
5. Dane przetwarzane na dużą skalę: w RODO nie zawarto definicji pojęcia „przetwarzanie na dużą skalę", choć w motywie 91 przedstawiono pewne wskazówki w tym zakresie. W każdym

[15] Grupa Robocza Art. 29 przypisuje wyrażeniu „systematycznie" jedno lub kilka z poniższych znaczeń (zob. wytyczne Grupy Roboczej Art. 29 dotyczące inspektora ochrony danych 16/EN WP 243):

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

Grupa Robocza Art. 29 interpretuje „miejsca publicznie dostępne" jako miejsca otwarte dla każdego obywatela, np. plac, centrum handlowe, ulica, rynek, stacja kolejowa lub biblioteka publiczna.

razie Grupa Robocza Art. 29 zaleca, aby przy ustalaniu, czy przetwarzanie danych odbywa się na dużą skalę, wziąć pod uwagę w szczególności następujące czynniki[16]:

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

6. Dopasowywanie lub łączenie zbiorów danych np. pochodzących z co najmniej dwóch operacji przetwarzania danych przeprowadzonych w różnych celach lub przez różnych administratorów danych w sposób wykraczający poza uzasadnione oczekiwania osób, których dane dotyczą[17].
7. Dane dotyczące osób wymagających szczególnej opieki, których dane dotyczą (zob. motyw 75): przetwarzanie tego rodzaju danych stanowi jedno z kryteriów ze względu na zwiększoną nierównowagę sił między osobami, których dane dotyczą, a administratorem danych, co oznacza, że osoby fizyczne mogą mieć trudności z wyrażeniem zgody na przetwarzanie swoich danych lub z wyrażeniem sprzeciwu wobec ich przetwarzania, lub mogą mieć trudności z korzystaniem z przysługujących im praw. Do osób wymagających szczególnej opieki, których dane dotyczą, można zaliczyć dzieci (można je uznać za niezdolne do świadomego i przemyślanego sprzeciwienia się przetwarzaniu danych lub do wyrażenia zgody na przetwarzanie danych), pracowników, bardziej wrażliwe grupy społeczne wymagające szczególnej ochrony (osoby chore psychicznie, osoby ubiegające się o azyl lub osoby starsze, pacjenci itp.) oraz w każdą sytuację, gdy można stwierdzić brak równowagi między stanowiskiem osoby, której dane dotyczą, a stanowiskiem administratora.
8. Innowacyjne wykorzystanie lub stosowanie nowych rozwiązań technologicznych lub organizacyjnych, takich jak połączenie technologii rozpoznającej odcisk palca i twarz w celu poprawy fizycznej kontroli dostępu itd. W RODO (art. 35 ust. 1 i motywy 89 i 91) wyjaśniono, że wykorzystanie nowej technologii zdefiniowanej „zgodnie ze stanem wiedzy technicznej" (motyw 91) może sprawić, iż konieczne będzie przeprowadzenie oceny skutków dla ochrony danych. Wynika to z tego, że zastosowanie takiej technologii może wiązać się z nowymi formami gromadzenia i wykorzystania danych, co może stwarzać ryzyko naruszenia praw i wolności osób fizycznych. W istocie osobiste i społeczne skutki wprowadzenia nowej technologii mogą nie być znane. Ocena skutków dla ochrony danych pomoże administratorowi danych zrozumieć takie ryzyko i je wyeliminować. Na przykład niektóre aplikacje „internetu rzeczy" mogą mieć znaczący wpływ na codzienne życie i prywatność osób fizycznych; dlatego wymagane jest przeprowadzenie oceny skutków dla ochrony danych.
9. Gdy samo przetwarzanie „uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy" (art. 22 i motyw 91). Obejmuje to operacje przetwarzania, których celem jest umożliwienie osobom, których dane dotyczą, uzyskania dostępu do usługi lub zawarcia umowy, zmiana tego dostępu lub odmówienie dostępu. Przykładem tego jest sytuacja, w której bank sprawdza swoich klientów w referencyjnej bazie danych kredytowych, aby zdecydować, czy udzielić im kredytu.

[16] Zob. wytyczne Grupy Roboczej Art. 29 dotyczące inspektora ochrony danych 16/EN WP 243.
[17] Zob. wyjaśnienie zawarte w opinii Grupy Roboczej Art. 29 w sprawie ograniczenia celu 13/EN WP 203, s. 24.

W większości przypadków administrator danych może uznać, że przetwarzanie spełniające dwa kryteria będzie wymagało przeprowadzenia oceny skutków dla ochrony danych. Ogólnie rzecz biorąc, Grupa Robocza Art. 29 uważa, że im więcej kryteriów zostanie spełnionych w ramach przetwarzania, tym większe prawdopodobieństwo wystąpienia wysokiego ryzyka naruszenia praw i wolności osób, których dane dotyczą, i dlatego wymaga przeprowadzenia oceny skutków dla ochrony danych, niezależnie od środków, jakie zamierza przyjąć administrator.

W niektórych przypadkach **administrator danych może jednak uznać, że przetwarzanie spełniające tylko jedno z wymienionych kryteriów będzie wymagało przeprowadzenia oceny skutków dla ochrony danych**.

Poniższe przykłady ilustrują, w jaki sposób należy korzystać z kryteriów, aby ocenić, czy dana operacja przetwarzania wymaga przeprowadzenia oceny skutków dla ochrony danych:

| **Przykłady przetwarzania** | **Ewentualne istotne kryteria** | **Czy istnieje prawdopodobieństwo, że wymagane będzie przeprowadzenie oceny skutków dla ochrony danych?** |
|---|---|---|
| Szpital przetwarzający dane genetyczne i dane dotyczące zdrowia pacjenta (system informatyczny szpitala). | - Dane wrażliwe lub dane o charakterze wysoce osobistym.<br>- Dane dotyczące osób wymagających szczególnej opieki, których dane dotyczą.<br>- Dane przetwarzane na dużą skalę. | Tak |
| Zastosowanie systemu kamer monitorujących zachowanie kierowców na drogach. Administrator planuje wykorzystać inteligentny system analizy obrazu do namierzania pojedynczych samochodów i automatycznego rozpoznawania tablic rejestracyjnych. | - Systematyczne monitorowanie.<br>- Innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych. | |
| Przedsiębiorstwo systematycznie monitoruje działania swoich pracowników, m.in. ich stanowiska pracy i aktywność w internecie *itd*. | - Systematyczne monitorowanie.<br>- Dane dotyczące osób wymagających szczególnej opieki, których dane dotyczą. | |
| Gromadzenie publicznych danych z mediów społecznościowych w celu wygenerowania profilu. | - Ocena lub punktacja.<br>- Dane przetwarzane na dużą skalę.<br>- Dopasowanie lub łączenie zbiorów danych.<br>- Dane wrażliwe lub dane o charakterze wysoce osobistym: | |
| Instytucja tworząca krajowy rating kredytowy lub bazę danych zawierającą informacje o nadużyciach finansowych. | - Ocena lub punktacja.<br>- Automatyczne podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku. | |

| Przykłady przetwarzania | Ewentualne istotne kryteria | Czy istnieje prawdopodobieństwo, że wymagane będzie przeprowadzenie oceny skutków dla ochrony danych? |
|---|---|---|
| | - Uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy.<br>- Dane wrażliwe lub dane o charakterze wysoce osobistym: | |
| Przechowywanie do celów archiwizacji wrażliwych danych osobowych opatrzonych pseudonimem dotyczące osób wymagających szczególnej opieki, biorących udział w projektach badawczych lub badaniach klinicznych. | - Dane wrażliwe.<br>- Dane dotyczące osób wymagających szczególnej opieki, których dane dotyczą.<br>- Uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy. | |
| Przetwarzanie „danych osobowych pacjentów lub klientów [...] przez pojedynczego lekarza, innego pracownika służby zdrowia lub prawnika" (motyw 91). | - Dane wrażliwe lub dane o charakterze wysoce osobistym.<br>- Dane dotyczące osób wymagających szczególnej opieki, których dane dotyczą. | Nie |
| Magazyn internetowy korzystający z listy dystrybucyjnej do wysyłania ogólnej skróconej wiadomości do swoich subskrybentów. | - Dane przetwarzane na dużą skalę. | |
| Strona internetowa poświęcona handlowi elektronicznemu, wyświetlająca reklamy dotyczące części do zabytkowych samochodów i korzystająca z ograniczonego profilowania w oparciu o elementy przeglądane lub kupione na tej stronie internetowej. | - Ocena lub punktacja. | |

**Odwrotnie, operacja przetwarzania może odpowiadać wyżej wymienionym przypadkom i nadal być uznawana przez administratora za „mogącą powodować wysokie ryzyko". W takich przypadkach administrator powinien uzasadnić i udokumentować powody, dla których nie przeprowadzono oceny skutków dla ochrony danych, oraz załączyć/zapisać poglądy inspektora ochrony danych.**

Ponadto w ramach zasady rozliczalności każdy administrator danych „prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada" obejmujący m.in. 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" (art. 30 ust. 1), a także musi ocenić, czy istnieje prawdopodobieństwo wystąpienia wysokiego ryzyka, nawet jeśli ostatecznie zdecyduje się nie przeprowadzać oceny skutków dla ochrony danych.

Uwaga: organy nadzorcze są zobowiązane ustanowić, podać do publicznej wiadomości i przekazać Europejskiej Radzie Ochrony Danych wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych (art. 35 ust. 4)[18]. Kryteria określone powyżej mogą pomóc organom nadzorczym w utworzeniu takiego wykazu, który w razie potrzeby można z czasem wzbogacić o bardziej szczegółowe treści. Na przykład przetwarzanie wszelkiego rodzaju danych biometrycznych lub danych dotyczących dzieci również można uznać za istotne dla opracowania wykazu zgodnego z art. 35 ust. 4.

b) Kiedy przeprowadzenie oceny skutków dla ochrony danych nie jest obowiązkowe? W przypadku, gdy nie jest prawdopodobne, aby operacja przetwarzania „mogła powodować wysokie ryzyko", gdy przeprowadzono już podobną ocenę skutków dla ochrony danych, gdy operację zatwierdzono przed majem 2018 r., lub gdy posiada podstawę prawną lub znajduje się w wykazie operacji przetwarzania, które nie podlegają ocenie skutków dla ochrony danych.

Grupa Robocza Art. 29 uważa, że ocena skutków dla ochrony danych nie jest wymagana w następujących przypadkach:

- **gdy nie jest prawdopodobne, aby operacja przetwarzania „mogła powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych"** (art. 35 ust. 1);
- **gdy charakter, zakres, kontekst i cele przetwarzania są bardzo podobne do operacji przetwarzania, w przypadku których przeprowadzono ocenę skutków dla ochrony danych**. W takich przypadkach można wykorzystać wyniki oceny skutków dla ochrony danych przeprowadzonej w odniesieniu do podobnych operacji przetwarzania (art. 35 ust. 1[19]);
- gdy operacje przetwarzania zostały sprawdzone przez organ nadzorczy przed majem 2018 r. w szczególnych warunkach, które nie uległy zmianie[20] (zob. rozdział III sekcja C);
- **jeżeli operacja przetwarzania**, zgodnie z art. 6 ust. 1 lit. c) lub e), **ma podstawę prawną** w prawie UE lub w prawie państwa członkowskiego, które reguluje daną operację przetwarzania, **oraz jeżeli oceny skutków dla ochrony danych dokonano już** w związku z przyjęciem tej podstawy prawnej (art. 35 ust. 10)[21], chyba że państwo członkowskie uznało za niezbędne dokonanie oceny skutków dla ochrony danych przed rozpoczęciem czynności przetwarzania;

[18] W tym kontekście „jeżeli wykazy [...] 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" (art. 35 ust. 6).

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

[20] „Decyzje przyjęte przez Komisję oraz zezwolenia wydane przez organy nadzorcze na podstawie dyrektywy 95/46/WE pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia" (motyw 171).

[21] Jeżeli ocena skutków dla ochrony danych przeprowadzana jest na etapie opracowywania prawodawstwa zapewniającego podstawę prawną dla przetwarzania, przegląd będzie prawdopodobnie wymagany przed rozpoczęciem operacji, ponieważ przyjęte prawodawstwo może się różnić od proponowanego w sposób, który wpływa na kwestie związane z prywatnością i ochroną danych. Ponadto w momencie przyjmowania prawodawstwa mogą nie być dostępne wystarczające szczegóły techniczne dotyczące faktycznego przetwarzania danych, nawet jeżeli przeprowadzono ocenę skutków dla ochrony danych. W takich przypadkach nadal konieczne może być dokonanie określonej oceny skutków dla ochrony danych przed rozpoczęciem rzeczywistych czynności przetwarzania.

- **jeżeli operacje przetwarzania zostały umieszczone w opcjonalnym wykazie (utworzonym przez organ nadzorczy) operacji przetwarzania** niepodlegających wymogowi dokonania oceny skutków dla ochrony danych (art. 35 ust. 5). Taki wykaz może zawierać czynności przetwarzania zgodne z warunkami określonymi przez ten organ, w szczególności poprzez wytyczne, konkretne decyzje lub zezwolenia, zasady zgodności itd. (np. we Francji: zezwolenia, zwolnienia, uproszczone zasady, pakiety zgodności itd.).W takich przypadkach i z zastrzeżeniem przeprowadzenia ponownej oceny przez właściwy organ nadzorczy przeprowadzenie oceny skutków dla ochrony danych nie jest wymagane, ale tylko wtedy, gdy przetwarzanie danych ściśle podlega zakresowi odpowiedniej procedury wymienionej w wykazie i nadal jest w pełni zgodne ze wszystkimi wymogami określonymi w RODO.

C. A co z już istniejącymi operacjami przetwarzania? W pewnych okolicznościach wymagane jest przeprowadzenie ocen skutków dla ochrony danych.

**Wymóg przeprowadzenia oceny skutków dla ochrony danych dotyczy istniejących operacji przetwarzania, które mogą powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych oraz w przypadku których nastąpiła zmiana rodzaju ryzyka, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania danych.**

Przeprowadzenie oceny skutków dla ochrony danych nie jest wymagane w przypadku operacji przetwarzania, które zostały skontrolowane przez organ nadzorczy lub urzędnika odpowiedzialnego za ochronę danych zgodnie z art. 20 dyrektywy 95/46/WE oraz które przeprowadzono w taki sam sposób jak przed kontrolą wstępną. W istocie „decyzje przyjęte przez Komisję oraz zezwolenia wydane przez organy nadzorcze na podstawie dyrektywy 95/46/WE pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia" (motyw 171).

Z drugiej strony oznacza to, że oceną skutków dla ochrony danych należy objąć wszelkie operacje przetwarzania danych, w odniesieniu do których od czasu przeprowadzenia kontroli wstępnej przez organ nadzorczy lub urzędnika odpowiedzialnego za ochronę danych zmieniły się warunki wdrażania (zakres, cel, zgromadzone dane osobowe, tożsamość administratorów danych lub odbiorców, okres zatrzymywania danych, środki techniczne i organizacyjne itd.) i które mogą powodować wysokie ryzyko.

Ponadto przeprowadzenie oceny skutków dla ochrony danych może być wymagane po zmianie rodzaju ryzyka związanego z operacją przetwarzania[22], np. z powodu wykorzystania nowej technologii lub dlatego, że dane osobowe wykorzystywane są w innym celu. Operacje przetwarzania danych mogą szybko ewoluować i mogą pojawić się nowe zagrożenia. Należy zatem zauważyć, że przegląd oceny skutków dla ochrony danych jest użyteczny nie tylko dla ciągłego doskonalenia, ale ma również kluczowe znaczenie dla utrzymania w przyszłości poziomu ochrony danych w zmieniającym się środowisku. Przeprowadzenie oceny skutków dla ochrony danych może być również konieczne ze względu na zmianę kontekstu organizacyjnego lub społecznego czynności przetwarzania, np. ponieważ skutki niektórych automatycznie podjętych decyzji stały się bardziej znaczące lub ponieważ nowe kategorie osób, których dane dotyczą, są narażone na dyskryminację. Każdy z tych przykładów może być elementem prowadzącym do zmiany ryzyka związanego z daną czynnością przetwarzania.

[22] Pod względem kontekstu, zgromadzonych danych, celów, funkcji, przetwarzanych danych osobowych, odbiorców, kombinacji danych (aktywa pomocnicze, źródła ryzyka, potencjalne skutki, zagrożenia itd.), środków bezpieczeństwa i międzynarodowego przekazywania danych.

Z drugiej strony niektóre zmiany mogłyby również zmniejszyć ryzyko. Na przykład operacja przetwarzania może ewoluować w taki sposób, że decyzje nie będą już podejmowane automatycznie, lub działania monitorujące przestaną być realizowane systematycznie. W tym przypadku przegląd przeprowadzonej analizy ryzyka może wykazać, że nie ma już potrzeby przeprowadzenia oceny skutków dla ochrony danych.

Dobrą praktyką powinno być **stałe przeprowadzanie przeglądu oceny skutków dla ochrony danych i regularne przeprowadzanie ponownej oceny**. W związku z powyższym, nawet jeżeli w dniu 25 maja 2018 r. nie wymaga się przeprowadzenia oceny skutków dla ochrony danych, administrator będzie musiał w odpowiednim momencie przeprowadzić taką ocenę w ramach swoich ogólnych obowiązków w zakresie rozliczalności.

D. Jak przeprowadzić ocenę skutków dla ochrony danych?

a) W jakim momencie należy przeprowadzić ocenę skutków dla ochrony danych? Przed rozpoczęciem przetwarzania.

**Ocenę skutków dla ochrony danych należy przeprowadzić „przed rozpoczęciem przetwarzania" (art. 35 ust. 1 i 10, motywy 90 i 93)[23]. Jest to zgodne z zasadami dotyczącymi uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych (art. 25 i motyw 78). Ocenę skutków dla ochrony danych należy postrzegać jako narzędzie wspomagające proces podejmowania decyzji w sprawie przetwarzania danych.**

Ocena skutków dla ochrony danych powinna rozpocząć się jak najwcześniej w fazie projektowania operacji przetwarzania, nawet jeżeli niektóre operacje przetwarzania nadal są nieznane. Aktualizacja oceny skutków dla ochrony danych przez cały cykl trwania projektu zapewni uwzględnienie ochrony danych i prywatności oraz zachęci do tworzenia rozwiązań promujących zgodność. W miarę postępu procesu rozwoju konieczne może być również powtórzenie poszczególnych etapów oceny, ponieważ wybór niektórych środków technicznych lub organizacyjnych może wpłynąć na prawdopodobieństwo wystąpienia zagrożenia wynikającego z przetwarzania lub jego wagę.

Fakt, że aktualizacja oceny skutków dla ochrony danych może okazać się konieczna już po rozpoczęciu procesu przetwarzania, nie uzasadnia odroczenia lub nieprzeprowadzenia oceny skutków dla ochrony danych. Ocena skutków dla ochrony danych jest procesem ciągłym, szczególnie gdy operacja przetwarzania przebiega dynamicznie i podlega ciągłym zmianom. **Prowadzenie oceny skutków dla ochrony danych jest procesem ciągłym, a nie jednorazowym.**

b) Kto jest zobowiązany do przeprowadzenia oceny skutków dla ochrony danych? Administrator, wspólnie z DPO i podmiotem przetwarzającym.

**Administrator jest odpowiedzialny za zapewnienie przeprowadzenia oceny skutków dla ochrony danych (art. 35 ust. 2)**. Ocenę skutków dla ochrony danych może przeprowadzić inny podmiot, zarówno z danej jednostki, jak i spoza niej, jednak ostateczna odpowiedzialność za wykonanie zadania spoczywa na administratorze.

[23] Z wyjątkiem przypadków, gdy jest to już istniejąca operacja przetwarzania, która została poddana kontroli wstępnej przez organ nadzorczy. W takim przypadku ocenę skutków dla ochrony danych należy przeprowadzić przed wprowadzeniem znaczących zmian.

**Administrator musi również konsultować się z inspektorem ochrony danych (DPO),** o ile został on wyznaczony (art. 35 ust. 2), a wyniki konsultacji i podjęte decyzje powinien udokumentować w ramach oceny skutków dla ochrony danych. DPO powinien również monitorować wykonanie oceny skutków dla ochrony danych (art. 39 ust. 1 lit. c)). Dalsze wskazówki można znaleźć w wytycznych Grupy Roboczej Art. 29 dotyczących inspektora ochrony danych 16/EN WP 243.

Jeżeli proces przetwarzania jest całkowicie lub częściowo realizowany przez podmiot przetwarzający dane, **podmiot przetwarzający powinien pomóc administratorowi danych w przeprowadzeniu oceny skutków dla ochrony danych** i dostarczyć wszelkie niezbędne informacje (zgodnie z art. 28 ust. 3 lit. f)).

**„W stosownych przypadkach" administrator musi „zasięgnąć opinii osób, których dane dotyczą, lub ich przedstawicieli" (art. 35 ust. 9)**. Grupa Robocza Art. 29 uważa, że:

- opinie te można zebrać za pomocą różnych środków, w zależności od kontekstu (np. badanie ogólne dotyczące celu i środków operacji przetwarzania, pytanie do przedstawicieli pracowników lub zwykła ankieta wysłana do przyszłych klientów administratora danych), zapewniając, aby administrator miał podstawę prawną do przetwarzania wszelkich danych osobowych wykorzystywanych podczas zbierania takich opinii. Należy jednak zauważyć, że zgoda na przetwarzanie nie jest oczywiście sposobem na uzyskanie opinii osób, których dane dotyczą;
- jeżeli ostateczna decyzja administratora danych różni się od opinii osób, których dane dotyczą, należy udokumentować powody podjęcia, bądź niepodjęcia decyzji;
- administrator powinien również przedstawić uzasadnienie niezasięgnięcia opinii osób, których dane dotyczą, jeżeli uzna to za niewłaściwe, np. w przypadku gdy stanowiłoby ono zagrożenie dla poufności biznesplanów przedsiębiorstw lub byłoby nieproporcjonalne lub niewykonalne.

Ponadto dobrą praktyką jest zdefiniowanie i udokumentowanie innych konkretnych ról i obowiązków, w zależności od polityki wewnętrznej, procesów i zasad np.:

- w przypadku gdy poszczególne jednostki gospodarcze mogą zaproponować przeprowadzenie oceny skutków dla ochrony danych, powinny one dostarczyć dane wejściowe dotyczące tej oceny i powinny uczestniczyć w procesie zatwierdzania oceny;
- w stosownych przypadkach zaleca się zasięgnięcie opinii niezależnych ekspertów reprezentujących różne zawody[24] (prawników, informatyków, ekspertów z zakresu bezpieczeństwa, socjologów, etyków *itp.*);
- role i obowiązki podmiotów przetwarzających muszą zostać określone w umowie; zaś ocenę skutków dla ochrony danych należy przeprowadzić z pomocą podmiotu przetwarzającego, uwzględniając charakter przetwarzania oraz dostępne mu informacje (art. 28 ust. 3 lit. f));
- główny urzędnik ds. bezpieczeństwa informacji, o ile został powołany, oraz DPO mogą zasugerować administratorowi przeprowadzenie oceny skutków dla ochrony danych w odniesieniu do konkretnej operacji przetwarzania oraz powinni pomóc zainteresowanym stronom w opracowaniu metodyki, w ocenie jakości oceny ryzyka, w stwierdzeniu, czy dopuszczalne jest ryzyko szczątkowe, oraz w rozwijaniu wiedzy odpowiedniej dla administratora danych;

[24] *Zalecenia dotyczące ram oceny skutków w zakresie prywatności dla Unii Europejskiej, rezultat D3*: http://www.piafproject.eu/ref/PIAF_D3_final.pdf

- główny urzędnik ds. bezpieczeństwa informacji, o ile został powołany, lub pracownik działu IT, powinien zapewnić pomoc administratorowi oraz może zaproponować przeprowadzenie oceny skutków dla ochrony danych w odniesieniu do konkretnej operacji przetwarzania, w zależności od potrzeb operacyjnych i potrzeb związanych z bezpieczeństwem.

    c) Zgodnie z jaką metodyką przeprowadza się ocenę skutków dla ochrony danych? Różna metodyka, wspólne kryteria.

W RODO określono minimalne cechy, jakie powinna posiadać ocena skutków dla ochrony danych (art. 35 ust. 7 oraz motywy 84 i 90), a mianowicie:

- „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;”
    - „wykazania przestrzegania niniejszego rozporządzenia”.

Na poniższym wykresie przedstawiono generyczny, iteracyjny proces przeprowadzania oceny skutków dla ochrony danych[25]:


Podczas oceny skutków operacji przetwarzania danych należy uwzględnić zgodność (art. 35 ust. 8) z kodeksem postępowania (art. 40). Może to być przydatne w celu wykazania, że wybrano lub wprowadzono odpowiednie środki, pod warunkiem że kodeks postępowania jest odpowiedni dla operacji przetwarzania. Uwzględnić należy również certyfikacje, znaki jakości oraz oznaczenia mające świadczyć o zgodności z RODO operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające (art. 42), a także wiążące reguły korporacyjne.

Wszystkie właściwe wymogi określone w RODO zapewniają szerokie, generyczne ramy służące do opracowania i przeprowadzania oceny skutków dla ochrony danych. Praktyczne wdrożenie oceny skutków dla ochrony danych będzie uzależnione od wymogów określonych w RODO, które można

[25] Należy podkreślić, że przedstawiony tutaj proces ma charakter iteracyjny: w praktyce prawdopodobne jest, że przed zakończeniem oceny skutków dla ochrony danych każdy z etapów będzie wielokrotnie powtarzany.

uzupełnić bardziej szczegółowymi praktycznymi wytycznymi. Wdrożenie oceny skutków dla ochrony danych jest zatem skalowalne. Oznacza to, że nawet administrator danych działający na małą skalę może opracować i wdrożyć ocenę skutków dla ochrony danych, która jest odpowiednia do danych operacji przetwarzania.

W motywie 90 RODO przedstawiono szereg elementów składowych oceny skutków dla ochrony danych, które pokrywają się z dobrze określonymi składowymi zarządzania ryzykiem (np. ISO 31000[26]). Z perspektywy zarządzania ryzykiem ocena skutków dla ochrony danych ma na celu „zarządzanie czynnikami ryzyka" naruszenia praw i wolności osób fizycznych, z wykorzystaniem poniższych procesów, poprzez:

- określanie kontekstu: „uwzględnienie charakteru, zakresu, kontekstu i celów przetwarzania oraz źródeł ryzyka";
- dokonywanie oceny ryzyka: „ocena konkretnego prawdopodobieństwa i powagi tego wysokiego ryzyka";
- traktowanie ryzyka: „minimalizowanie tego ryzyka" i „zapewnienie ochrony danych osobowych", a także „wykazanie przestrzegania niniejszego rozporządzenia".

Uwaga: ocena skutków dla ochrony danych, o której mowa w RODO, stanowi narzędzie służące do zarządzania ryzykiem naruszenia praw osób, których dane dotyczą, a zatem przy jej przeprowadzaniu przyjmuje się ich perspektywę, podobnie jak w przypadku określonych dziedzin (np. bezpieczeństwo społeczne). Z kolei zarządzanie ryzykiem w pozostałych dziedzinach (np. bezpieczeństwa informacji) skupia się na organizacji.

Za pośrednictwem RODO zapewniono administratorom danych elastyczność przy określaniu dokładnej struktury i formy oceny skutków dla ochrony danych w celu umożliwienia jej dopasowania do istniejących praktyk roboczych. W UE i na całym świecie istnieje szereg różnych określonych procesów, w przypadku których uwzględniono elementy składowe opisane w motywie 90. Niezależnie od formy ocena skutków dla ochrony danych musi jednak stanowić rzeczywistą ocenę ryzyka, pozwalając administratorom podjąć działania na rzecz wyeliminowania ryzyka.

Można zastosować różne metodyki (przykłady metodyki ochrony danych i oceny skutków w zakresie prywatności znajdują się załączniku 1), aby wspomóc wdrażanie podstawowych wymogów określonych w RODO. Określono wspólne kryteria mające umożliwić stosowanie tych różnych podejść, a jednocześnie pozwolić administratorom na zachowanie zgodności z RODO (zob. załącznik 2). Za pomocą tych kryteriów uściślono podstawowe wymogi zawarte w rozporządzeniu, lecz przewidziano wystarczający zakres swobody, aby możliwe były różne formy wdrażania. Kryteria te można wykorzystać do wykazania, że konkretna metodyka oceny skutków dla ochrony danych spełnia standardy przewidziane w RODO. **Decyzję o wyborze metodyki podejmuje administrator danych, lecz metodyka ta powinna być zgodna z kryteriami określonymi w załączniku 2.**

Grupa Robocza Art. 29 zachęca do opracowywania ram oceny skutków dla ochrony danych dla poszczególnych sektorów. Wynika to z faktu, że jej członkowie mogą oprzeć się na specyficznej dla danego sektora wiedzy, co oznacza, że ocenę skutków dla ochrony danych można ukierunkować na konkretny rodzaj operacji przetwarzania (np. konkretne rodzaje danych, majątku wspólnego,

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

możliwych skutków, zagrożeń, działań). Oznacza to, że ocena skutków dla ochrony danych może zaradzić problemom, które powstają w konkretnym sektorze gospodarki, przy stosowaniu konkretnych technologii lub przy przeprowadzaniu operacji przetwarzania określonego rodzaju.

Ponadto 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" (art. 35 ust. 11[27]).

d) Czy publikacja oceny skutków dla ochrony danych jest obowiązkowa? Nie, lecz publikacja podsumowania może przyczynić się do zwiększenia zaufania, a pełną treść oceny skutków dla ochrony danych należy przekazać organom nadzorczym, jeżeli miały miejsce uprzednie konsultacje lub jeżeli zwrócił się o to organ ochrony danych.

**RODO nie zawiera prawnego wymogu publikacji oceny skutków dla ochrony danych; decyzja o publikacji należy do administratora. Administratorzy powinni jednakże rozważyć publikację choćby części przeprowadzonych przez nich ocen skutków dla ochrony danych, takich jak podsumowanie lub wnioski.**

Proces taki miałby na celu przyczynienie się do zwiększenia zaufania, którym obdarza się administratora dokonującego operacji przetwarzania, i do wykazania rozliczalności i przejrzystości. Szczególnie dobrą praktyką jest publikowanie oceny skutków dla ochrony danych, jeżeli operacja przetwarzania ma wpływ na społeczeństwo. Może to dotyczyć szczególnie przypadków, w których ocenę skutków dla ochrony danych przeprowadza organ publiczny.

Opublikowana wersja oceny skutków dla ochrony danych nie musi zawierać całej oceny, szczególnie w przypadku, gdy ocena skutków dla ochrony danych mogłaby zawierać szczegółowe informacje na temat rodzajów ryzyka dla bezpieczeństwa odnoszących się do administratora danych lub wyjawiać tajemnice przedsiębiorstwa lub szczególnie chronione informacje handlowe. W takich okolicznościach wersja opublikowana może składać się zaledwie z podsumowania głównych ustaleń dokonanych w toku oceny skutków dla ochrony danych lub wyłącznie z oświadczenia, że przeprowadzono ocenę skutków dla ochrony danych.

Ponadto jeżeli w toku oceny skutków dla ochrony danych ujawniono istnienie wysokiego ryzyka szczątkowego, administrator danych będzie zobowiązany zwrócić się do organu nadzorczego o uprzednie konsultacje dotyczące przetwarzania (art. 36 ust. 1). W ramach tych konsultacji należy przedstawić pełną ocenę skutków dla ochrony danych (art. 36 ust. 3 lit. e)). Organ nadzorczy może udzielić zalecenia[28] i nie naruszy tajemnicy przedsiębiorstwa ani nie ujawni luk w zabezpieczeniach, z zastrzeżeniem mających zastosowanie w każdym państwie członkowskim zasad publicznego dostępu do dokumentów urzędowych.

E. <u>Kiedy należy skonsultować się z organem nadzorczym? Jeżeli ryzyko szczątkowe jest wysokie.</u>

Jak wyjaśniono powyżej:

[27] W art. 35 ust. 10 wyraźnie wyłączono zastosowanie jedynie art. 35 ust. 1–7.

[28] W myśl art. 36 ust. 2 udzielenie administratorowi pisemnego zalecenia jest niezbędne wyłącznie w przypadku, gdy organ nadzorczy jest zdania, że zamierzone przetwarzanie nie jest zgodne z rozporządzeniem.

- przeprowadzenie oceny skutków dla ochrony danych jest wymagane w przypadku, gdy operacja przetwarzania „może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych" (art. 35 ust. 1, zob. rozdział III sekcja B lit. b)). Przykładowo przetwarzanie danych dotyczących zdrowia na dużą skalę uważa się za mogące powodować wysokie ryzyko i wymaga ono przeprowadzenia oceny skutków dla ochrony danych;
- w takim przypadku obowiązkiem administratora danych jest dokonanie oceny ryzyka naruszenia praw i wolności osób, których dane dotyczą, oraz zidentyfikowanie środków[29] planowanych w celu zmniejszenia tego ryzyka do dopuszczalnego poziomu i wykazania przestrzegania RODO (art. 35 ust. 7, zob. rozdział III sekcja C lit. c)). Przykładem, jeżeli chodzi o przechowywanie danych osobowych na laptopach, może być zastosowanie odpowiednich technicznych i organizacyjnych środków bezpieczeństwa (skuteczne szyfrowanie całego dysku, solidne zarządzanie kluczami, odpowiednia kontrola dostępu, zabezpieczone kopie zapasowe, itd.) uzupełniających środki stosowane w ramach istniejącej polityki (zawiadomienie, zgoda, prawo dostępu, prawo wniesienia sprzeciwu, itd.).

Jeżeli w przywołanym powyżej przykładzie dotyczącym laptopa administrator danych uznał ryzyko za dostatecznie ograniczone i można je za takie uznać zgodnie z brzmieniem art. 36 ust. 1 i motywów 84 i 94, przetworzenia można dokonać bez konsultacji z organem nadzorczym. Administrator danych musi skonsultować się z organem nadzorczym w sytuacji, gdy nie może dostatecznie ograniczyć zidentyfikowanego ryzyka (np. utrzymuje się wysokie ryzyko szczątkowe).

Przykład niedopuszczalnego wysokiego ryzyka szczątkowego obejmuje przypadki, w których osoby, których dane dotyczą, mogą ponieść znaczne lub nawet nieodwracalne konsekwencje, z którymi nie będą mogły sobie poradzić (np.: bezprawne uzyskanie dostępu do danych prowadzące do zagrożenia życia osób, których dane dotyczą, zwolnienie, zagrożenie o charakterze finansowym) lub w których wydaje się oczywiste, że wystąpi ryzyko (np.: ograniczenie liczby osób mających dostęp do danych nie jest możliwy ze względu na sposób ich udostępniania, wykorzystywania lub rozprowadzania lub gdy luka w zabezpieczeniach, o której istnieniu wiadomo, nie zostanie usunięta).

**Zawsze gdy administrator danych nie może znaleźć środków wystarczających do zmniejszenia ryzyka do dopuszczalnego poziomu (np. ryzyko szczątkowe wciąż jest wysokie), wymagane są konsultacje z organem nadzorczym[30].**

Ponadto administrator będzie zobowiązany skonsultować się z organem nadzorczym zawsze, gdy prawo państwa członkowskiego wymaga, by administratorzy konsultowali się z organem nadzorczym lub uzyskiwali jego uprzednią zgodę w odniesieniu do przetwarzania danych osobowych przez administratora do celów wykonania zadania realizowanego przez niego w interesie publicznym, w tym przetwarzania w związku z ochroną socjalną i zdrowiem publicznym (art. 36 ust. 5).

Należy jednak zaznaczyć, że niezależnie od tego, czy wymagane są konsultacje z organem nadzorczym na podstawie poziomu ryzyka szczątkowego, obowiązki polegające na przechowywaniu

[29] W tym uwzględnienie istniejących wytycznych od Europejskiej Rady Ochrony Danych i organów nadzorczych oraz uwzględnienie stanu techniki i kosztów wdrażania, jak określono w art. 35 ust. 1.

[30] Uwaga: „pseudonimizacja oraz szyfrowanie danych osobowych" (a także minimalizacja danych, mechanizmu nadzoru itd.) niekoniecznie stanowią odpowiednie środki. Stanowią one jedynie przykłady. W zależności od kontekstu i ryzyka odpowiednie są różne środki, właściwe dla operacji przetwarzania.

dokumentacji związanej z oceną skutków dla ochrony danych i dokonywaniu aktualizacji oceny skutków dla ochrony danych w stosownym terminie, pozostają aktualne.

## IV. Wnioski i zalecenia

Oceny skutków dla ochrony danych stanowią przydatne narzędzie wykorzystywane przez administratorów danych do wdrażania systemów przetwarzania danych, które są zgodne z RODO, a przeprowadzenie tych ocen może okazać się obowiązkowe w przypadku niektórych rodzajów operacji przetwarzania. Oceny skutków dla ochrony danych są skalowalne i mogą przybierać różne formy, lecz w RODO określono podstawowe wymogi skutecznej oceny skutków dla ochrony danych. Administratorzy danych powinni postrzegać dokonywanie oceny skutków dla ochrony danych jako przydatne i pozytywne działanie, które przyczynia się do zachowania zgodności z prawem.

W art. 24 ust. 1 określono podstawowy obowiązek administratora w zakresie zachowania zgodności 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”.

Dokonywanie oceny skutków dla ochrony danych ma zasadnicze znaczenie dla zachowania zgodności z rozporządzeniem, jeżeli planuje się lub odbywa się przetwarzanie danych, z którym wiąże się wysokie ryzyko. Oznacza to, że administratorzy danych powinni stosować kryteria określone w niniejszym dokumencie w celu ustalenia, czy należy dokonać oceny skutków dla ochrony danych. W ramach wewnętrznej polityki stosowanej przez administratorów danych można rozszerzyć ten wykaz poza wymogi prawne zawarte w RODO. Powinno to skutkować większym zaufaniem osób, których dotyczą dane, i pozostałych administratorów danych i uzyskaniem przez nich pewności.

W przypadku gdy planuje się przetwarzanie mogące powodować wysokie ryzyko, administrator danych musi:

- wybrać metodykę dokonywania oceny skutków dla ochrony danych (przykłady podano w załączniku 1), która spełnia kryteria określone w załączniku 2, lub określić i wdrożyć systematyczny proces dokonywania oceny skutków dla ochrony danych, który:
  - jest zgodny z kryteriami zawartymi w załączniku 2;
  - jest zintegrowany z istniejącym procesami projektowania, opracowywania, zmian, ryzyka i przeglądu operacyjnego zgodnie z procesami wewnętrznymi, kontekstem i kulturą;
  - angażuje strony, których sprawa dotyczy, i w ramach, którego jasno określono ich obowiązki (administratora, DPO, osób, których dane dotyczą, lub ich przedstawicieli, przedsiębiorstw, służb technicznych, podmiotów przetwarzających, inspektora ds. bezpieczeństwa informacji, itd.);
- przedłożyć właściwym organom nadzorczym sprawozdanie z oceny skutków dla ochrony danych, gdy jest to wymagane;
- konsultować się z organem nadzorczym, jeżeli określenie środków wystarczających do zminimalizowania wysokiego ryzyka zakończyło się niepowodzeniem;
- okresowo dokonywać przeglądu oceny skutków dla ochrony danych i przetwarzania, którego oceny dokonano w jej ramach, przynajmniej gdy doszło do zmiany ryzyka wynikającego z przetwarzania operacji;
- dokumentować podjęte decyzje.

## Załącznik 1 – Przykłady istniejących unijnych ram dokonywania oceny skutków dla ochrony danych

W RODO nie określono, który proces dokonywania oceny skutków dla ochrony danych należy stosować, ale za to umożliwiono administratorom danych wprowadzanie ram, które uzupełniają dotychczas przez nich stosowane praktyki robocze, o ile uwzględniają one elementy składowe opisane w art. 35 ust. 7. Takie ramy mogą być dopasowane do indywidualnych potrzeb administratora danych lub wspólne dla całej określonej branży. Wcześniej opublikowane ramy, opracowane przez unijne organy ochrony danych oraz stosowane w UE ramy dla poszczególnych sektorów obejmują (m.in.):

przykłady stosowanych w UE ogólnych ram:

- DE: standardowy model ochrony danych, V.1.0 – wersja próbna, 2016 r.[31].
  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 r.
  https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR: ocena skutków w zakresie prywatności, Commission nationale de l'informatique et des libertés (CNIL), 2015 r.
  https://www.cnil.fr/fr/node/15798
- UK: kodeks praktyk w zakresie dokonywania oceny skutków w zakresie prywatności (Conducting privacy impact assessments code of practice), Biuro Komisarza ds. Informacji, 2014 r.
  https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

przykłady stosowanych w UE ram dla poszczególnych sektorów:

- ramy oceny skutków dla ochrony danych i prywatności w zastosowaniach RFID[32].
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- szablon oceny skutków dla ochrony danych na potrzeby inteligentnych sieci i inteligentnych systemów pomiarowych[33]
  http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

---

[31] Zatwierdzony jednomyślnie i przez aklamację (przy wstrzymującej się Bawarii) na 92. konferencji niezależnych organów ochrony danych z federacji i krajów związkowych, która odbyła się w Kühlungsborn w dniach 9–10 listopada 2016 r.

[32] Zob. 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/policies/privacy/docs/wpdocs/2011/wp180_pl.pdf

[33] Zob. również opinia 07/2013 w sprawie szablonu oceny skutków dla ochrony danych na potrzeby inteligentnych sieci i inteligentnych systemów pomiarowych opracowanego przez grupę ekspertów nr 2 w ramach grupy zadaniowej ds. inteligentnych sieci Komisji. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf

W ramach normy międzynarodowej zapewnione zostaną również wytyczne dotyczące metodyk stosowanych do dokonywania oceny skutków dla ochrony danych (ISO/IEC 29134[34]).

[34] ISO/IEC 29134 (projekt), IT – Techniki bezpieczeństwa – ocena skutków w zakresie prywatności – Wytyczne, Międzynarodowa Organizacja Normalizacyjna (ISO).

## Załącznik 2 – Kryteria dopuszczalnej oceny skutków dla ochrony danych

Grupa Robocza Art. 29 proponuje następujące kryteria, z których administratorzy danych mogą korzystać, aby ocenić, czy ocena skutków dla ochrony danych lub metodyka służąca do dokonania oceny skutków dla ochrony danych są wystarczająco kompleksowe do zachowania zgodności z RODO:

- ☐ zapewniono systematyczny opis operacji przetwarzania (art. 35 ust. 7 lit. a)):
  - ☐ uwzględniono charakter, zakres, kontekst i cele przetwarzania (motyw 90);
  - ☐ w rejestrze zamieszczono dane osobowe, informacje o odbiorcach i okresie przechowywania danych osobowych;
  - ☐ przedstawiono funkcjonalny opis operacji przetwarzania;
  - ☐ zidentyfikowano zasoby, z którymi styczność mają dane osobowe (sprzęt komputerowy, oprogramowanie, sieci, osoby, opracowania lub kanały transmisji opracowań);
  - ☐ uwzględniono przestrzeganie zatwierdzonych kodeksów postępowania (art. 35 ust. 8);
- ☐ oceniono niezbędność oraz proporcjonalność (art. 35 ust. 7 lit. b)):
  - ☐ wskazano środki, których podjęcie jest planowane w celu zapewnienia przestrzegania rozporządzenia (art. 35 ust. 7 lit. d) i motyw 90), uwzględniając:
    - ☐ środki przyczyniające się do proporcjonalności i niezbędności przetwarzania, z uwzględnieniem następujących aspektów:
      - ☐ konkretne, wyraźne i prawnie uzasadnione cele (art. 5 ust. 1 lit. b));
      - ☐ zgodność przetwarzania z prawem (art. 6);
      - ☐ dane adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (art. 5 ust. 1 lit. c));
      - ☐ ograniczony czas przechowywania (art. 5 ust. 1 lit. e));
    - ☐ środki przyczyniające się do zachowania praw osób, których dane dotyczą:
      - ☐ poinformowanie osoby, której dane dotyczą (art. 12, 13 i 14);
      - ☐ prawo dostępu i prawo do przenoszenia danych (art. 15 i 20);
      - ☐ prawo do sprostowania i do usunięcia danych (art. 16, 17 i 19);
      - ☐ prawo do sprzeciwu i prawo do ograniczenia przetwarzania (art. 18, 19 i 21);
      - ☐ relacje z podmiotem przetwarzającym (art. 28);
      - ☐ zabezpieczenia przy międzynarodowym przekazywaniu danych (rozdział V);
      - ☐ uprzednie konsultacje (art. 36);
- ☐ przeprowadzono działania w zakresie zarządzania ryzykiem naruszenia praw i wolności osób, których dane dotyczą (art. 35 ust. 7 lit. c)):
  - ☐ uwzględniono źródło, charakter, specyfikę i powagę ryzyka (por. motyw 84), czy konkretniej, w przypadku każdego rodzaju ryzyka (bezprawnego dostępu, niepożądanej zmiany i zniknięcia danych), z punktu widzenia osób, których dane dotyczą:
    - ☐ uwzględniono źródła ryzyka (motyw 90);
    - ☐ zidentyfikowano możliwe skutki dla praw i wolności osób, których dane dotyczą, w przypadku zdarzeń takich jak bezprawny dostęp, niepożądane zmiany i zniknięcie danych;
    - ☐ zidentyfikowano zagrożenia, które mogłyby doprowadzić do bezprawnego dostępu, niepożądanych zmian i zniknięcia danych;
    - ☐ oszacowano prawdopodobieństwo i powagę (motyw 90);
  - ☐ określono środki, których podjęcie jest planowane w celu zaradzenia ryzyku (art. 35 ust. 7 lit. d) i motyw 90);
- ☐ zaangażowano zainteresowane strony:
  - ☐ skonsultowano się z inspektorem ochrony danych w celu uzyskania zalecenia (art. 35 ust. 2);

- ☐ w stosownych przypadkach zasięgnięto opinii osób, których dane dotyczą, lub ich przedstawicieli (art. 35 ust. 9).