1. Informacja ogólna jak rozumieć RODO w UIK

Czym jest RODO?

RODO to skrót od nazwy aktu rangi europejskiej pod pełną nazwą: 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, tzw. rozporządzenie ogólne UE czyli RODO.

Kim jest ADO?

ADO to skrót od nazwy „właściciela danych osobowych", czyli tego kto decyduje o środkach i celach przetwarzania danych osobowych tj. Administratora Danych Osobowych. ADO nie jest poszczególny człowiek, czy też członek zarządu. ADO to podmiot prawny, który posiada NIP i KRS, ten który zawiera wszelkiego rodzaju umowy i zaciąga zobowiązania, niemniej zgodnie z zasadami reprezentacji w jego imieniu działają konkretne organy jak np. zarząd. **W naszym przypadku ADO jest Uniwersytet Ignatianum w Krakowie kierowany przez zarząd tj. Rektora.**

Kim jest IOD?

IOD to skrót nazwy Inspektor Ochrony Danych. Jest to prawa ręka ADO w nadzorowaniu prawidłowości wykorzystywania danych osobowych w przedsiębiorstwie. Podlega wyłącznie najwyższemu kierownictwu. Nie można mu wydawać poleceń. IOD zostaje powołany przez ADO a następnie zgłoszony do Urzędu Ochrony Danych Osobowych i w ten sposób zostaje punktem kontaktowym pomiędzy UODO a ADO. W naszym przypadku jest to r.pr. dr. Paweł Biały.

2. Dane osobowe

2.1. Informacje, które posiadają status danych osobowych

Definicja danych osobowych została uregulowana w sposób niezwykle szeroki. Każda informacja, która wiąże się z osobą fizyczną, zarówno w sposób bezpośredni jak i pośredni może zostać uznana za dane osobową. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić pośrednio lub bezpośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Jak zauważa NSA, danymi osobowymi są wszelkie informacje „niosące komunikat o danej osobie”[1]. Tak więc, osobą fizyczną jest każdy człowiek. W tym miejscu należy również wspomnieć, że osoby fizyczne prowadzące działalność gospodarczą podlegają pełnej ochronie danych osobowych, które traktowane są tak, jakby dotyczyły zwykłej osoby a nie przedsiębiorcy. **W przypadku UIK, będą to wszelkiego rodzaju dane pozyskiwane z takich źródeł jak: pracownicy i współpracownicy, kontrahenci, podwykonawcy, przedstawiciele podmiotów współpracujących oraz przede wszystkim osoby korzystające z działań UIK tj. studenci i kandydaci na studia**.

2.2. Podstawa prawna przetwarzania danych osobowych

Legalne przetwarzanie danych osobowych, a zatem wykonywanie jakichkolwiek działań i operacji na lub w związku z danymi osobowymi, możliwe jest gdy:

a) osoba, której dane dotyczą, wyrazi na to zgodę (w jednym lub większej liczbie celów), chyba że chodzi o usunięcie dotyczących jej danych,
b) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
c) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
d) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
e) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą,
f) jest to niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (prawo krajowe lub prawo UE),

---

[1] Wyrok NSA z dnia 19.05. 2011 roku, sygn. akt i OSK 1079/10, www.nas.org.

g) jest to niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,

h) jest to niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,

Zgoda, o której mowa w punkcie a), może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania. Za prawnie usprawiedliwiony cel, o którym mowa w punkcie e) uważa się w szczególności marketing bezpośredni **produktów** lub usług administratora danych oraz dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

Należy podkreślić, że wszędzie tam, gdzie dochodzi do przetwarzania danych osobowych należy zawsze oprzeć się o jedną z przesłanek legalizujących proces przetwarzania danych osobowych. w przypadku, gdy jest to **zgoda** powinna być wyrażona w sposób jasny, wyraźny, jednoznaczny i bezwarunkowy. Chociaż przepisy prawa nie wymagają wyrażenia zgody w formie pisemnej (zgodnie z RODO może to być okazanie woli w formie wyraźnego działania potwierdzającego lub przyzwalającego na wykorzystywanie danych osobowych) rekomenduje się posługiwanie się tą formą, w szczególności mając na uwadze, iż to na administratorze danych spoczywa obowiązek udowodnienia, iż przetwarzał dane zgodnie z prawem – czyli, że zrealizował zasadę rozliczalności (art. 5 ust. 2 RODO).

3. Administrator Danych Osobowych (dalej jako: „ADO”)

3.1. Status administratora danych osobowych

Zgodnie z art. 4 pkt. 7 RODO, administratorem jest podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
Zgodnie z orzeczeniem Sądu Najwyższego z 2000 r. administrujący danymi to nie tylko administrator, ale także kadry na szczeblach pośrednich, czyli Zarząd oraz wszyscy, którzy odpowiadają za bezpieczeństwo danych osobowych lub mają w zakresie obowiązków administrowanie zbiorem danych osobowych. Przy czym do postawienia zarzutu wystarczy zlekceważenie obowiązku zabezpieczenia.

3.2. Obowiązki administratora danych

Do obowiązków administratora danych osobowych tj. wszystkich osób mających dostęp do danych osobowych, należy przede wszystkim:

a) przetwarzanie (wykorzystywanie) danych osobowych zgodnie z prawem, rzetelnie i przejrzyście, tak aby osoba, której dane dotyczą, nie miała wątpliwości w ww. zakresie,
b) zbieranie i wykorzystywanie danych osobowych w konkretnym celu, jasno i przejrzyście zakomunikowanym (zasada ograniczonego celu),
c) zbieranie i wykorzystywanie danych osobowych tylko w zakresie niezbędnym, adekwatnym do celu, który ma być zrealizowany (zasada minimalizacji, dawniej adekwatności),
d) prawidłowe wykorzystywanie danych osobowych pod kątem ich poprawności i prawdziwości, co pociąga za sobą obowiązek ich zmiany czy sprostowania,
e) przechowywanie w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane są przetwarzane (zasada ograniczonego przechowywania),
f) przetwarzanie (wykorzystywanie) w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (zasada integralności i poufności).
g) wdrożenie odpowiednich środków technicznych i organizacyjnych, aby wykazać przestrzeganie RODO. administrator powinien przyjąć wewnętrzne polityki i wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych. Takie środki mogą polegać m.in. na minimalizacji przetwarzania danych osobowych, jak najszybszej pseudonimizacji danych osobowych, przejrzystości co do funkcji i przetwarzania danych osobowych, umożliwieniu osobie, której dane dotyczą, monitorowania przetwarzania danych, umożliwieniu administratorowi tworzenia i doskonalenia

zabezpieczeń. Jeżeli opracowywane, projektowane, wybierane i użytkowane są aplikacje, usługi i produkty, które opierają się na przetwarzaniu danych osobowych albo przetwarzają dane osobowe w celu realizacji swojego zadania, należy zachęcać wytwórców tych produktów, usług i aplikacji, by podczas opracowywania i projektowania takich produktów, usług i aplikacji wzięli pod uwagę prawo do ochrony danych osobowych i z należytym uwzględnieniem stanu wiedzy technicznej zapewnili administratorom i podmiotom przetwarzającym możliwość wywiązania się ze spoczywających na nich obowiązków ochrony danych (zasada privacy by design i privacy by default).

Administrator jest odpowiedzialny za przestrzeganie ww. zasad i musi być w stanie wykazać ich przestrzeganie (zasada rozliczalności) co może być zrealizowane w konkretnych działaniach takich jak np.:

h) spełnienie obowiązku informacyjnego,
i) sporządzenie odpowiedniej dokumentacji, („Polityka bezpieczeństwa", „Instrukcja zarządzania systemem informatycznym w którym przetwarzane są dane osobowe", „umowa powierzenia", „rejestr czynności przetwarzania", „klauzula zgody", etc.),
j) należyte zabezpieczenie systemu przed ingerencją osób trzecich oraz podmiotów nieuprawnionych,
k) należyte zabezpieczenie danych osobowych,
l) prowadzenie ewidencji osób uprawnionych do przetwarzania danych osobowych,
m) przygotowanie odpowiednich upoważnień dla osób, które będą przetwarzać dane osobowe,
n) dokumentowanie naruszeń ochrony danych osobowych,
o) raport z naruszenia ochron danych osobowych
p) procedura postępowania w przypadku wystąpienia naruszenia ochrony danych osobowych,
q) prowadzenie kontroli nad całością procesu przetwarzania danych osobowych,
r) wyznaczenie Inspektora Ochrony Danych, następcę prawnego Administratora Bezpieczeństwa Informacji.

Mając na uwadze przepisy RODO, wyodrębnia się dwa podstawowe obowiązki[2] administratora danych osobowych: obowiązek informacyjny oraz obowiązek zabezpieczenia danych osobowych.

3.2.1. Obowiązek informacyjny

Obowiązki informacyjne należy podzielić w zależności od tego czy ADO zbiera dane osobowe od osoby, której dotyczą, czy też ADO zbiera dane osobowe niepochodzące od tej osoby. Mimo, iż powołany przepis nie określa momentu, w którym administrator ma obowiązek dopełnić obowiązku

[2] Por. art. 24 in. oraz art. 36 uodo.

(posługuje się bowiem pojęciem „podczas pozyskiwania"), przyjmuje się jednak, że powinno to nastąpić już na etapie zbierania danych osobowych.

W art. 13 ust. 4 RODO wskazano natomiast sytuacje, w przypadku których administrator jest zwolniony z tego obowiązku. Obowiązek został wyłączony w szczególności, jeżeli osoba, której dane dotyczą, posiada już informacje, o których mowa w art. 13 RODO.

RODO nie reguluje jednoznacznie sposobu, w jaki obowiązek informacyjny powinien być spełniony. Obowiązek ten można spełnić na piśmie, ustnie (gdy tego żąda osoba, której dane dotyczą) lub w innym sposób – w tym elektronicznie. Brak jest więc przeszkód prawnych, by obowiązek ten został spełniony za pomocą telefonu, Internetu, czy dokumentów pisemnych. Jednakże ze względu na utrudnienia dowodowe, w razie ewentualnego sporu, zaleca się utrwalenie dokonania obowiązku na nośniku lub zamieszczenie klauzuli informacyjnej na formularzu do zbierania danych.

Podkreślamy, że ADO musi spełnić obowiązek informacyjny w przejrzystej, łatwo dostępnej formie, językiem jasnym i prostym, niezależnie od tego czy osoba, której dane osobowe przetwarza chciałaby lub nie chciałaby zostać w tym zakresie poinformowana.

W zakresie obowiązku informacyjnego, ADO zobowiązany jest do poinformowania osoby fizycznej, od której dane osobowe zbiera, o:

a) adresie swojej siedziby i pełnej nazwie wraz z danymi kontaktowymi,
b) danych kontaktowych IOD np. e-mail, telefon, formularz kontaktowy itp.,
c) celu zbierania danych osobowych wraz z podstawą prawną (względnie uzasadniony interes ADO),
d) znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych osobowych,
e) zamiarze przekazania danych osobowych do państwa trzeciego (spoza UE),
f) okres lub kryteria jego ustalenia, w którym będą przechowywane dane osobowe,
g) prawie dostępu do treści swoich danych oraz uprawnieniu do ich sprostowania, usunięcia, ograniczenia przetwarzania, prawie wniesienia sprzeciwu, prawie do przenoszenia danych osobowych,
h) w niektórych przypadkach, prawie cofnięcia zgody,
i) prawie wniesienia skargi do organu nadzorczego,
j) dobrowolności albo obowiązku podania danych osobowych, ustawowym, umownym, warunku zawarcia umowy,
k) zautomatyzowanym podejmowaniu decyzji w tym profilowaniu,
l) przetwarzaniu w celu innym niż zostały zebrane, udzielając wszystkich ww. informacji, gdy zamierza wykorzystywać dane osobowe w innym celu niż ten, w którym je zebrał.

Gdy dane zostały pozyskane nie bezpośrednio od podmiotu danych, dodatkowo należy wskazać źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych (tzw. wtórny obowiązek informacyjny).
Spełnienie obowiązku informacyjnego jest o tyle istotne, że dzięki niemu osoba, której dane dotyczą ma świadomość, że jej dane są wykorzystywane. Zapewnienie jej tego prawa wymaga przynajmniej, aby mogła ona po uzyskaniu informacji o zebraniu jej danych od innego podmiotu sprzeciwić się dalszemu przetwarzaniu.

3.2.1.1. Ryzyko wynikające z niezgodności informacji

Brak dopełnienia obowiązku informacyjnego może skutkować odpowiedzialnością odszkodowawczą oraz nałożeniem finansowych kar administracyjnych, nakładanych na podstawie art. 82 RODO w trybie art. 83 RODO, w wysokości do 20 mln EUR lub 4 % obrotu rocznego światowego za ostatni rok obrotowy, przy czym zastosowanie ma kara wyższa.

3.2.2. Obowiązek zabezpieczenia danych

Realizacja tego obowiązku jest szczególnie wnikliwie badana w razie ewentualnych kontroli przeprowadzanych przez kontrolerów Urzędu Ochrony Danych Osobowych.
ADO zobowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem RODO, zmianą, utratą, uszkodzeniem oraz zniszczeniem. Istotą rzeczonej regulacji jest fakt, że znajduje ona zastosowanie zarówno do danych osobowych przetwarzanych w systemie informatycznym, jak również w sposób tradycyjny tj. manualny.

3.2.2.1. Polityka Ochrony Danych zgodna z RODO– podstawowe informacje

Polityka Bezpieczeństwa winna obejmować:

a) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych,
b) dodatkowe postanowienia zgodne z RODO, wprowadzane w każdy zindywidualizowanym przypadku odrębnie.

3.2.2.2. Instrukcja Zarządzania Systemem Informatycznym – podstawowe informacje

Instrukcja Zarządzania Systemem Informatycznym, choć nie jest dokumentem obowiązkowym, ale o ile ADO będzie chciał ją opracować, dotyczy przetwarzania danych osobowych w środowisku IT i w związku z tym powinna z kolei zawierać:

a) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazania osoby odpowiedzialnej za te czynności,
b) metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem,
c) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczonych dla użytkowników systemu,
d) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
e) opis sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych,
f) opis sposobu zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania,
g) sposób realizacji wymogów bezpieczeństwa oraz rejestracji określonych operacji na danych,
h) procedury wykonania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych,
i) dodatkowe postanowienia zgodne z RODO, wprowadzane w każdy zindywidualizowanym przypadku odrębnie.

3.2.2.3. Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych oraz inne dokumenty RODO

Obowiązek posiadania tego dokumentu wynika wprost z przepisów RODO. w praktyce posiadanie tego dokumentu jest niezbędne dla zapewnienia prawidłowego funkcjonowania jednostki organizacyjnej. Wejście w życie RODO nakłada na administratorów danych liczne obowiązki, w tym obowiązek analizy ryzyka, czy oceny skutków dla ochrony danych. Zmiany te mają na celu zapewnienie ochrony danych osobowych na jeszcze wyższym poziomie. Administrator danych przed wdrożeniem odpowiednich procedur bezpieczeństwa zobowiązany będzie do oceny ryzyk związanych z procesem przetwarzania danych a następnie dopasowanie mechanizmów bezpieczeństwa do możliwego do wystąpienia ryzyka.

3.2.2.4. Ewidencja osób upoważnionych do przetwarzania danych osobowych oraz upoważnienia do przetwarzania danych osobowych dla poszczególnych pracowników

Jest to szczególnie ważne bowiem nie każdy pracownik może mieć dostęp do wszystkich danych osobowych. Upoważnienia określają jaki pracownik w jakim zakresie i na ja długo może mieć dostęp do danych osobowych, które przetwarza ADO.

3.2.2.5. Umowy powierzenia przetwarzania danych osobowych

Bardzo często ADO współpracuje z podmiotami zewnętrznymi w ramach np. outsourcingu usług. Współpraca ta pociąga za sobą konieczność przekazania ww. danych osobowych na odpowiedniej podstawie prawnej. Jest nią umowa powierzenia przetwarzania danych osobowych zawarta pomiędzy ADO a każdym z tych podmiotów, w zakresie spełniającym wymagania przepisane treścią art. 28 w zw. z art. 32 RODO. **W przypadku UIK będzie to przede wszystkim taki obszar jak zewnętrzni podwykonawcy i kontrahenci**.

3.2.2.6. Incydent naruszenia ochrony danych osobowych

Naruszenie ochrony danych osobowych na gruncie RODO jest rozumiane jako dwie podstawowe sytuacje: (a) naruszenie prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, albo (b) nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych i inaczej przetwarzanych. Naruszenie, o którym mowa, może jednak być przypadkowe (niezamierzone) lub bezprawne (naruszające przepisy) i może polegać na działaniu lub zaniechaniu konkretnego podmiotu. Art. 4 pkt. 12 w zw. z art. 33 RODO.

3.2.3. Rejestr czynności przetwarzania a zgłoszenie zbiorów danych do rejestracji

RODO odchodzi od konieczności zgłaszania zbiorów danych osobowych do UODO. Niemniej sama definicja zbiorów danych osobowych jest zachowana w RODO, w niezmienionej treści. ADO jest zwolniony od konieczności zgłaszania zbiorów danych do UODO, ale jednocześnie powinien je prowadzić dla łatwiejszego opracowania pozostałej dokumentacji RODO jak np. rejestru czynności przetwarzania czy też upoważnień do przetwarzania danych osobowych.

3.2.4. Upoważnienia do przetwarzania danych osobowych

Zgodnie z art. 32 w zw. z art. 5 pkt. f) RODO ADO musi zapewnić ochronę przetwarzanych danych osobowych przed niedozwolonym dostępem do nich. Praktyczną pomocą w zrealizowaniu tej zasady integralności i poufności jest wykorzystanie dobrze znanego upoważnienia do przetwarzania danych osobowych. w związku z tym, do przetwarzania należy upoważnić pracownika, który ma dostęp do danych osobowych niezależnie od tego jaka jest podstawa prawna jego zatrudnienia. Upoważnienie do przetwarzania danych osobowych może zatem być obligatoryjnym dokumentem, który wydawany jest przez ADO wszystkim osobom, które zaangażowane są w przetwarzanie danych osobowych jednostce organizacyjnej. Upoważnienia powinny być wówczas ewidencjonowane. Ewidencja upoważnień stanowić będzie wtedy zindywidualizowany element procesu ochrony danych osobowych w świetle RODO.

3.2.5. Szacowanie – analiza ryzyka

RODO zawiera w art. 32 ust. 1 RODO przykładowe środki techniczne i organizacyjne, jednak to do administratora lub podmiotu przetwarzającego zależy wybór jakie środki zostaną zastosowane. Administrator lub podmiot przetwarzający powinien dobierać środki adekwatnie potrzeb, wynikających z szacowania ryzyka.

Przykładowe środki to:

a) pseudominizacja (przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej – art. 4 pkt 5 RODO) i szyfrowanie danych osobowych,
b) zdolność do ciągłego zapewniania poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

3.2.6. Ocena skutków dla ochrony danych osobowych

Przeprowadzanie oceny skutków dla ochrony danych jest jednym z elementów zarządzania ryzykiem związanym z przetwarzaniem danych.

Ocenę skutków należy podzielić na dwa etapy. W pierwszym etapie administrator dokonuje oceny, czy dany rodzaj przetwarzania (w szczególności z użyciem nowych technologii) ze względu na swój zakres kontekst lub cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (art. 35 ust. 1 RODO). Jeżeli odpowiedź jest twierdząca, to administrator powinien przystąpić do drugiego etapu oceny skutków. Dokonując oceny skutków, administrator jest zobowiązany do podjęcia konsultacji z inspektorem ochrony danych, jeżeli został powołany.

Zakres czynności, które powinny się znaleźć w ocenie skutków został określony w art. 35 ust. 7 RODO:

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,
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.

Artykuł 35 ust. 3 RODO zawiera przykładowe wyliczenie sytuacji, w których przeprowadzenie skutków dla ochrony danych jest obowiązkowe 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;
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; lub
c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Ponadto na podstawie art. 35 ust. 1, art. 35 ust. 3 lit. a-c), motywów 71, 75 oraz 91 preambuły RODO, Grupa Robocza art. 29 wskazała kryteria, które należy brać pod uwagę przy ocenie ryzyka dla naruszenia praw lub wolności osób fizycznych:

a) ocena lub punktacja, w tym profilowanie i przewidywanie, w szczególności dotyczące takich aspektów podmiotu danych jak świadczenie pracy, sytuacja ekonomiczna, zdrowie, osobiste preferencje, zainteresowania, wiarygodność, zachowanie, lokalizacja czy poruszanie się,

b) zautomatyzowane podejmowanie decyzji wywołujące skutki prawne lub wpływające na podmiot danych w podobny sposób,
c) systematyczne monitorowanie mające na celu obserwowanie, monitorowanie lub kontrolowanie podmiotu danych, w tym systematyczne monitorowanie miejsc dostępnie publicznych,
d) przetwarzanie tzw. danych wrażliwych lub przetwarzanie danych o charakterze wysoce osobistym,
e) dane przetwarzane na dużą skalę,
f) przetwarzanie danych osobowych podlegające łączeniu lub dopasowywaniu,
g) dane dotyczące osób wymagających szczególnej opieki, których dane dotyczą,
h) wykorzystanie do przetwarzania danych innowacyjnych rozwiązań technicznych lub organizacyjnych,
i) jeżeli przetwarzanie danych samo w sobie utrudnia podmiotom danych wykonywanie przysługujących im praw lub korzystanie z usługi lub z umowy.

Im więcej kryteriów zostanie spełnionych, tym większe jest prawdopodobieństwo, że przetwarzanie danych przez administratora może powodować wysokie ryzyko naruszenia praw lub wolności podmiotu danych. W większości przypadków administrator powinien uznać, że przetwarzanie spełniające dwa kryteria będzie wymagało przeprowadzenia oceny skutków dla ochrony danych. Natomiast jeżeli administrator danych uważa, że przetwarzanie danych nie narusza praw i wolności, mimo że zostały spełnione określone kryteria, to powinien tę okoliczność dokładnie udokumentować i załączyć stanowisko inspektora ochrony danych, jeżeli został on powołany.
Należy również dodać, że zgodnie z art. 35 ust. 4 RODO organ nadzorczy ustanawia i podaje do publicznej wiadomości wykaz operacji przetwarzania danych podlegających wymogowi oceny skutków dla ochrony danych.