



Unia Europejska
Europejski Fundusz Społeczny



Przewodnik po danych osobowych w projektach PO WER dla Wnioskodawców i Beneficjentów

Wersja 1.0

Ministerstwo Inwestycji i Rozwoju

Warszawa 2018 r.

I.	Wstęp	3
II.	Informacje o RODO.....	3
1.	Co to jest RODO?	3
2.	Od kiedy stosuje się RODO?	3
3.	Czy wnioskodawcy i beneficjenci podlegają RODO?	4
4.	Czy jest polska ustawa o ochronie danych osobowych?	4
5.	Co to jest Urząd Ochrony Danych Osobowych i kto nim zarządza?	4
6.	Co to są dane osobowe?	4
7.	Co to jest przetwarzane?.....	5
8.	Co to są kategorie danych osobowych i kiedy można je przetwarzać?.....	6
9.	Kto to jest administrator?	7
10.	Kto to jest inspektor ochrony danych?.....	8
11.	Kto może przetwarzać dane osobowe?.....	9
12.	Kto może przetwarzać dane osobowe w danej organizacji u podmiotu przetwarzającego?	10
13.	Co to jest zbiór danych?	11
14.	Co to jest cel przetwarzania danych?	12
15.	Jaki zakres danych osobowych można zbierać?	12
16.	Co to jest obowiązek informacyjny?	13
17.	Jak długo można przetwarzać dane osobowe?	16
18.	Co to jest rejestr czynności przetwarzania danych osobowych i czy muszą go prowadzić?	17
19.	W jaki sposób należy powierzyć przetwarzanie danych osobowych?	18
20.	Czy należy wystąpić do Instytucji Pośredniczącej z informacją o zamiarze powierzenia przetwarzania danych?.....	20
21.	Co oznacza obowiązek zgłaszania naruszeń ochrony danych?	20
22.	Co oznacza podejście przetwarzania oparte na ryzyku i w jaki sposób należy zabezpieczyć przetwarzanie danych osobowych?	21
23.	Czy za nieprzestrzeganie RODO może zostać nałożona kara?	22

I. Wstęp

Ochrona danych osobowych jest jednym z istotnych zagadnień podczas realizacji projektów w ramach Programu Operacyjnego Wiedza Edukacja Rozwój (PO WER). Należy dbać o to, aby przestrzegać przepisów ochrony przetwarzania danych osobowych na każdym etapie aplikowania o środki pochodzące z PO WER i realizacji projektu.

Dlatego Instytucja Zarządzająca PO WER (IZ), która pełni rolę administratora, w procesie przetwarzania danych osobowych w projektach, przygotowała „Przewodnik po danych osobowych w projektach PO WER dla Wnioskodawców i Beneficjentów”.

W kolejnych rozdziałach znajdują się szczegółowe informacje wymagane *Rozporządzeniem 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 (RODO)*, a także praktyczne przykłady zastosowania konkretnych rozwiązań.

II. Informacje o RODO

1. Co to jest RODO?

RODO to skrót od Rozporządzenia o Ochronie danych Osobowych - *Rozporządzeniem 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)*. Jest to akt przyjęty przez Unię Europejską (UE) i dotyczy zasad ochrony przetwarzania danych osobowych. Przepisy zawarte, w tym dokumencie obowiązują wszystkie kraje UE i są dla nich takie same.

Tekst tego aktu można znaleźć w Dzienniku Urzędowym Unii Europejskiej L z 4 maja 2016 r. nr. 119, str. 1 lub po wejściu na stronę:

<http://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32016R0679&from=EN> .

Dokument dostępny jest również na stronie Urzędu Ochrony Danych Osobowych (UODO) pod adresem: <https://uodo.gov.pl/pl/132> .

RODO zastępuje *ustawę z 29 sierpnia 1997 r. o ochronie danych osobowych* (Dz. U. 2016 r. poz. 922, z późn. zm.). Oznacza to, że RODO w większości przypadków zawiera wszystkie przepisy, które mają zastosowanie do ochrony danych osobowych.

2. Od kiedy stosuje się RODO?

RODO obowiązkowo stosuje się od 25 maja 2018r.

3. Czy wnioskodawcy i beneficjenci podlegają RODO?

Wszyscy Wnioskodawcy i Beneficjenci podlegają RODO, bowiem przetwarzają oni dane osobowe.

4. Czy jest polska ustawa o ochronie danych osobowych?

Tak, oprócz RODO dostępna jest również nowa polska ustawa – *ustawa z 10 maja 2018 r. o ochronie danych osobowych* (Dz. U. 2018 r. poz. 1000) (UODO). Akt ten dostępny jest pod adresem: <https://uodo.gov.pl/pl/131>.

RODO pozwala na uregulowanie niektórych zasad dotyczących ochrony danych osobowych w przepisach krajowych. Dlatego Minister Cyfryzacji wydał polską ustawę o ochronie danych osobowych, w której reguluje między innymi:

- zasady wyznaczania inspektora ochrony danych (IOD),
- zasady powoływania Prezesa Urzędu Ochrony Danych Osobowych (PUODO),
- zasady przeprowadzania kontroli przestrzegania przepisów o ochronie danych osobowych,
- zasady nakładania kar przez PUODO na podmioty zobowiązane do przestrzegania przepisów RODO.

5. Co to jest Urząd Ochrony Danych Osobowych i kto nim zarządza?

Urząd Ochrony Danych Osobowych (UODO) jest instytucją publiczną, która jest organem nadzorującym poprawne i zgodne z przepisami przetwarzanie danych osobowych. Na czele UODO stoi Prezes Urzędu Ochrony Danych Osobowych (PUODO). UODO zastąpił dotychczas wykonującego tę rolę Generalnego Inspektora Ochrony Danych Osobowych (GIODO), a także realizuje inne obowiązki nałożone przez RODO.

6. Co to są dane osobowe?

Dane osobowe to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Szczegółowa definicja dostępna jest w art. 4 RODO.

- Osoba zidentyfikowana to taka osoba, której tożsamość znamy i jesteśmy w stanie zidentyfikować z pośród innych osób.
- Osoba możliwa do zidentyfikowania to taka osoba, której tożsamości nie znamy, ale jesteśmy w stanie ją zidentyfikować na podstawie informacji, które o tej osobie posiadamy. Na przykład jeżeli posiadamy imię, nazwisko i adres zamieszkania danej osoby fizycznej, to na podstawie tych danych jesteśmy w stanie ją zidentyfikować. Jeżeli posiadalibyśmy wyłącznie imię tej osoby lub nawet tylko nazwisko, to na podstawie tej jednej danej nie jesteśmy w stanie zidentyfikować tej osoby. Takie samo nazwisko może mieć wiele osób i nie wiemy, na którą z tych osób to nazwisko wskazuje. Ale jeżeli oprócz nazwiska będziemy mieli np. numer projektu, to jeżeli w projekcie będzie tylko jedna osoba o tym nazwisku to tą

osobę będziemy mogli zidentyfikować. W niektórych sytuacjach wystarczy posiadać wyłącznie jedną informację na temat danej osoby, żeby była to dana osobowa. Taką informacją jest PESEL i może nią być adres e-mail. Jeżeli adres e-mail przyjmie konstrukcję jan.kowalski@xxxxx.pl, to domena (w przykładzie są to znaki xxxxx), jeżeli jest to na przykład nazwa firmy, będzie wskazywała na konkretną osobę i umożliwi jej zidentyfikowanie.

Oznacza to, że daną osobową jest zestaw informacji o osobie fizycznej, przy pomocy którego możemy tą osobę zidentyfikować z pośród innych osób. Jak pokazują wyżej przytoczone przykłady dla każdego przypadku ten zestaw informacji może być różny i każdy przypadek należy rozpatrywać indywidualnie.

Danych osobowych nie posiadają osoby prawne, ale ich pracownicy mogą już takie dane posiadać i jako osoby fizyczne mogą zostać zidentyfikowani. Na przykład:

- informacja, którą jest nazwa spółki „ABDCE sp. z o. o.” – nie jest daną osobową,
- informacja, którą jest nazwa spółki i jej reprezentant, „ABCDE sp. z o. o. reprezentowana przez Jana Kowalskiego” – może stanowić dane osobowe, ponieważ posiadając informacje o nazwie spółki oraz imię i nazwisko osoby, która ją reprezentuje jesteśmy w stanie zidentyfikować tą osobę.

Powyższe oznacza, że w każdym projekcie, który jest realizowany w PO WER będą występowały dane osobowe. Danymi osobowymi będą nie tylko dane uczestników, którzy otrzymują wsparcie, ale również dane innych osób, od których zebraliśmy dane, takie jak na przykład:

- dane osobowe zebrane od partnerów,
- dane osobowe zebrane od personelu projektu,
- dane osobowe uczestników spotkań informacyjnych organizowanych przez Beneficjenta,
- dane osobowe podmiotów biorących udział w realizacji projektu.

7. Co to jest przetwarzane?

Pod pojęciem przetwarzanie rozumie się operację, którą wykonuje się na danych osobowych, taką jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczenie, usuwanie lub niszczenie. Operacja może zostać wykonana w

sposób zautomatyzowany, na przykład przez system informatyczny, lub niezautomatyzowany, na przykład gdy dane przetwarzane są papierowo.

Pełna definicja przetwarzania dostępna jest w art. 4 RODO.

Oznacza to, że jeżeli posiadamy dane osobowe i wykonujemy z nimi jakiegokolwiek operacje to dane te przetwarzamy.

Zakres danych osobowych, które są przetwarzane w PO WER stanowi załącznik do umowy o dofinansowanie projektu.

8. Co to są kategorie danych osobowych i kiedy można je przetwarzać?

Dane osobowe dzielą się na dwie kategorie:

- a. dane osobowe zwykłe,
- b. dane osobowe szczególnej kategorii – tzw. dane wrażliwe.

Zwykłe dane osobowe są to wszystkie dane, które nie są danymi osobowymi szczególnej kategorii. Przykładem danych należących do tej kategorii są: imię, nazwisko, adres zamieszkania (miejscowość, ulica, numer budynku, nr lokalu), wiek, data urodzenia, PESEL, wykształcenie.

Dane osobowe szczególnej kategorii są to dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby fizycznej.

Żeby móc legalnie przetwarzać dane osobowe musi zachodzić zgodność przetwarzania z prawem. Aby móc przetwarzać dane muszą być spełnione określone warunki, na które wskazuje RODO. Dane osobowe przetwarzane są jeżeli na przykład:

- osoba, której dane są przetwarzane wyraziła na to zgodę – to oznacza, że osoba zgodziła się, żeby jej dane były przetwarzane,
- są niezbędne do wykonywania obowiązku prawnego ciążącego na administratorze – to oznacza, że przepisy prawa wskazują na potrzebę zbierania danych osobowych,
- przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą – oznacza to, że osoba sama publicznie udostępniła swoje dane,

Szczegółowe przesłani definiuje RODO w art. 6 i 9.

W projektach współfinansowanych z PO WER przetwarzane są zarówno dane osobowe zwykłe oraz dane osobowe szczególnych kategorii. Dane osobowe zwykłe przetwarzane są na podstawie warunku z art. 6 ust. 1 lit. c, to jest: przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. Oznacza, to że przepisy prawa wskazują na potrzebę zbierania danych osobowych. Dane osobowe szczególnych kategorii w PO WER przetwarzane są na podstawie art. 9 ust. 2 lit. g. Ustęp ten wskazuje, że przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii i prawa państwa członkowskiego. Wyżej wymienionym warunki są spełnione przez następujące przepisy szczegółowe:

- art. 54 ust. 2, art. 59 ust. 1, art. 65, art. 74. ust 1 i 3, art. 115, art. 122, art. 125 ust. 2 lit. d, ust. 4 lit. a oraz ust. 5 i 6 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013 z dnia 17 grudnia 2013 r. ustanawiającego wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności, Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich oraz Europejskiego Funduszu Morskiego i Rybackiego oraz ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności i Europejskiego Funduszu Morskiego i Rybackiego oraz uchylającego rozporządzenie Rady (WE) nr 1083/2006 (Dz. Urz. UE L 347 z 20.12.2013, str. 320, z późn. zm.) oraz pkt 3 A ppkt iv załącznika XIII Kryteria desygnacji Instytucji Zarządzającej i Instytucji Certyfikującej do tego rozporządzenia,

- art. 5 oraz art. 19 ust. 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1304/2013 z dnia 17 grudnia 2013 r. w sprawie Europejskiego Funduszu Społecznego i uchylającego rozporządzenie Rady (WE) nr 1081/2006 (Dz. Urz. UE L 347 z 20.12.2013, str. 470) oraz załącznika I i II do tego rozporządzenia,

- art. 9 ust. 2, art 22 - 24 i 26 ustawy z dnia 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014–2020.

W PO WER nie przetwarzamy danych osobowych na podstawie zgody.

9. Kto to jest administrator?

Administrator to taki podmiot, który decyduje o celach i sposobach przetwarzania danych osobowych. Przez cel rozumie się „po co” dane osobowe są przetwarzane. Przez sposób rozumie się jak dane osobowe będą przetwarzane.

Szczegółowa definicja dostępna jest w art. 4 RODO.

Administratorem dla danych osobowych przetwarzanych w projektach realizowanych w ramach PO WER jest minister do spraw rozwoju regionalnego. Zakres danych, który jest przetwarzany stanowi załącznik do umowy o dofinansowanie projektu.

10. Kto to jest inspektor ochrony danych?

Inspektor ochrony danych (IOD) to dawnej Administrator Bezpieczeństwa Informacji (ABI). Do jego głównych zadań należą między innymi:

- informowanie pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich i doradzanie im w jaki sposób należy przetwarzać dane osobowe, aby przetwarzanie było zgodne z RODO i UODO,
- monitorowanie przestrzegania w organizacji RODO, UODO oraz polityk (wymagań) administratora,
- zwiększanie świadomości w zakresie przetwarzania danych osobowych zgodnie z prawem, w tym prowadzenie szkoleń personelu uczestniczącego w operacjach przetwarzania,
- współpraca z organem nadzorczym, którym jest PUODO, w tym pełnienie funkcji punktu kontaktowego dla tego organu.

Szczegółowo zakres zadań IOD określa art. 39 RODO.

Wyznaczenie IOD jest obowiązkowe między innymi gdy:

- główna działalność podmiotu, który przetwarza dane polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cel wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę,
- główna działalność podmiotu, który przetwarza dane polega na przetwarzaniu na dużą skalę szczegółowych kategorii danych osobowych lub danych osobowych skazujących.

Szczegółowo zasady powoływania IOD zostały określone w art. 37 RODO.

Główną działalnością podmiotu będzie działalność kluczowa z punktu widzenia osiągnięcia celów administratora. Nie każdy podmiot, którego główną działalnością jest przetwarzanie danych, musi powołać IOD. Tylko taki podmiot, którego działalność polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cel wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę. Z powyższego wynika, że każdy przypadek należy rozpatrywać indywidualnie. Nie jest możliwe wskazanie konkretnej wartości, czy rozmiaru zbioru danych, czy liczby osób, których dane dotyczą, którą powodowałyby dużą skalę.

W PO WER można skontaktować się z IOD wysyłając korespondencję elektroniczną na adres IOD@miir.gov.pl. Beneficjenci, którzy realizują projekty i mają powołanych inspektorów danych osobowych powinni również podawać kontakt do swojego inspektora lub innej osoby, która u Beneficjenta odpowiada za zgodność przetwarzania danych osobowych z RODO. Praktyka taka spowoduje łatwiejszy dostęp do informacji i zasad panujących u Beneficjenta, w zakresie ochrony przetwarzania danych osobowych, w związku z realizacją projektu.

11. Kto może przetwarzać dane osobowe?

Administrator decyduje o celach i sposobach przetwarzania danych osobowych. Może on w zakresie przetwarzania danych korzystać z usług innego podmiotu, który nazywany jest podmiotem przetwarzającym. Podmiot przetwarzający nie decyduje o celach i środkach przetwarzania danych. Jeżeli przetwarzanie danych osobowych ma być dokonane w imieniu administratora przez inny podmiot, musi dojść do powierzenia danych w drodze umowy (tak zwanej umowy powierzenia) lub innego instrumentu prawnego.

Szczegółowo kwestie powierzenia danych omawia art. 28 RODO.

W PO WER administrator powierzył przetwarzanie danych osobowych Instytucji Pośredniczącej (IP), która jest podmiotem przetwarzającym, na podstawie *Porozumienia w sprawie powierzenia przetwarzania danych osobowych w związku z realizacją Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2010 (Porozumienie)*. Jednocześnie administrator umocował w tym Porozumieniu IP do dalszego powierzenia przetwarzania danych osobowych Beneficjentowi. Zapisy, które regulują kwestie powierzenia przetwarzania danych pomiędzy IP a Beneficjentem dostępne są w *Umowie o dofinansowanie projektu* i w myśl art. 28 RODO powierzają przetwarzanie danych osobowych oraz regulują obowiązki stron. W drodze umowy sporządzonej na piśmie Beneficjent może powierzyć przetwarzanie danych osobowych innemu podmiotowi pod warunkiem, że podmiot ten będzie zaangażowany w realizację projektu. Podmiot, któremu Beneficjent powierzył przetwarzanie danych osobowych nie może powierzyć już danych innemu podmiotowi, z którym współpracuje. W takim wypadku może to zrobić Beneficjent.

Zapisy w *Umowie o dofinansowanie projektu*, które zawierają odwołania do RODO będą występowały w ramach nowych projektów, dla których umowa ta została zawarta po 24 maja 2018 r. W pozostałych projektach będą występowały zapisy, które odnoszą się do poprzedniej ustawy o ochronie danych osobowych. Nie mniej jednak, z uwagi na fakt, że RODO należy stosować wprost, dla zapisów które odnoszą się do poprzedniej ustawy o ochronie danych osobowych należy stosować ich odpowiedniki z RODO. Należy również przestrzegać innych regulacji, które wcześniej nie występowały w poprzedniej ustawie o

ochronie danych osobowych, a teraz są wymagane przez RODO, na przykład wdrożenie odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa oparte na zidentyfikowanym ryzyku.

12. Kto może przetwarzać dane osobowe w danej organizacji u podmiotu przetwarzającego?

W organizacji dane osobowe przetwarzane są przez osoby fizyczne, które są pracownikami danej organizacji lub współpracownikami. Osoby te muszą posiadać upoważnienia do przetwarzania danych osobowych. RODO nie definiuje w jakiej formie ma zostać wydane upoważnienie. Każdy podmiot przetwarzający może przyjąć inny sposób upoważnienia do przetwarzania danych osobowych.

W PO WER wzór upoważnienia do przetwarzania danych osobowych jest jednym z załączników do Umowy o dofinansowanie projektu. Dla każdego projektu, który jest realizowany przez Beneficjenta upoważnienie powinno zostać wydane indywidualnie. Należy jednocześnie pamiętać, że Beneficjent może zastosować swój wzór upoważnienia do przetwarzania danych. Beneficjent może również wybrać inną formę upoważnienia do przetwarzania danych osobowych, która obowiązuje w procedurach danej organizacji. Ze względu na zmianę podstawy prawnej, na podstawie której upoważniane są osoby fizyczne do przetwarzania danych osobowych oraz mając na uwadze stosowanie przepisów RODO wprost, administrator, jako dobrą praktykę, zaleca wydanie nowych upoważnień do przetwarzania danych. Jednocześnie w nowych upoważnieniach, które są wydawane należy stosować podstawy prawne zgodne z RODO. Przykładowa treść upoważnienia do przetwarzania danych osobowych znajduje się poniżej.

UPOWAŻNIENIE Nr _____ DO PRZETWARZANIA DANYCH OSOBOWYCH

Z dniem [_____] r., na podstawie art. 29 w związku z art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE. L 119 z 4 maja 2016, str. 1) (RODO), upoważniam [_____] do przetwarzania danych osobowych w zbiorze Program Operacyjny Wiedza Edukacja Rozwój/Zbiór danych osobowych z ZUS*.

Upoważnienie wygasa z chwilą ustania Pana/Pani* stosunku prawnego łączącego Pana/Panią* z [_____].

Czytelny podpis osoby upoważnionej do wydawania i odwoływania upoważnień.

Upoważnienie otrzymałem/am

(miejsowość, data, podpis)

Oświadczam, że zapoznałem/am się z przepisami powszechnie obowiązującymi dotyczącymi ochrony danych osobowych, w tym z RODO, a także z obowiązującym w _____ opisem technicznych i organizacyjnych środków zapewniających ochronę i bezpieczeństwo przetwarzania danych osobowych i zobowiązuję się do przestrzegania zasad przetwarzania danych osobowych określonych w tych dokumentach.

Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych, z którymi zapoznałem/am się oraz sposobów ich zabezpieczenia, zarówno w okresie trwania umowy jak również po ustaniu stosunku prawnego łączącego mnie z [_____].

Czytelny podpis osoby składającej oświadczenie

*niepotrzebne skreślić

Uwaga:

Przetwarzanie danych osobowych w zbiorze *Zbiór danych osobowych z ZUS* dotyczy sytuacji, w której *umowa o dofinansowanie projektu* została zawarta z Beneficjentem przez Ministerstwo Rodziny, Pracy i Polityki Społecznej lub Wojewódzki Urząd Pracy, w ramach Działania 1.2 lub 1.3.

13. Co to jest zbiór danych?

Zbiór danych zgodnie z definicją RODO oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów.

W PO WER wyróżniamy zbiór danych pod nazwą *Program Operacyjny Wiedza Edukacja Rozwój*. Dane osobowe przetwarzane w tym zbiorze, to w szczególności dane zebrane w wersji papierowej, które nie zostały jeszcze wprowadzone do SL2014. Są to również dane, które mogą być przetwarzane za pośrednictwem Systemu Obsługi Wniosków

Aplikacyjnych.

Zastosowanie ma również zbiór *Centralny system teleinformatyczny wspierający realizację programów operacyjnych*. Zbiór ten ma zastosowanie w sytuacji kiedy zalogowani jesteśmy do systemu SL2014 i przetwarzamy dane wprowadzone do tego systemu.

W niektórych przypadkach wykorzystywany jest również zbiór pod nazwą *Dane osobowe z ZUS*. Zbiór ten znajduje zastosowanie w niektórych projektach Ministerstwa Rodziny, Pracy i Polityki Społecznej oraz Wojewódzkich Urzędach Pracy i służy zweryfikowaniu kwalifikowalności udziału osób w projektach PO WER.

14. Co to jest cel przetwarzania danych?

Cel przetwarzania danych osobowych to informacja o tym po co przetwarzamy dane osobowe. Cel jest określony wyłącznie przez administratora. Dane osobowe można przetwarzać wyłącznie w celu, dla którego dane zostały zebrane.

W PO WER administrator danych zdefiniował cel przetwarzania danych w następujący sposób:

- aplikowanie o środki unijne i realizacja projektów, w szczególności potwierdzanie kwalifikowalności wydatków, udzielanie wsparcia uczestnikom projektów, ewaluacji, monitoringu, kontroli, audytu, sprawozdawczości oraz działań informacyjno-promocyjnych, w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020,
- zapewnienie realizacji obowiązku informacyjnego dotyczącego przekazywania do publicznej wiadomości informacji o podmiotach uzyskujących wsparcie z Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020

Oznacza to, że wyłącznie w tym celu dopuszcza się przetwarzanie danych osobowych. Dane osobowe przetwarzane w PO WER nie mogą być przetwarzane w innym celu.

15. Jaki zakres danych osobowych można zbierać?

RODO w art. 5 ust. lit c) wprowadza zasadę minimalizacji danych. Oznacza to, że można zbierać tylko dane, które są niezbędne do zrealizowania celu.

W PO WER administrator określił zakres danych, jaki może być przetwarzany w projektach realizowanych w programie. Zakres ten stanowi załącznik do *Umowy o dofinansowanie projektu*. Przetwarzanie danych powinno zatem zostać ograniczone do danych, które wynikają z zawartej *Umowy o dofinansowanie projektu*. Dla danych, które wykraczają

poza powierzony zakres danych minister właściwy do spraw rozwoju regionalnego nie jest ich administratorem.

16. Co to jest obowiązek informacyjny?

RODO wymaga, aby podczas pozyskiwania danych osobowych od osoby fizycznej przekazać jej szereg informacji:

- kto jest administratorem i jego dane kontaktowe,
- dane kontaktowe IOD,
- cel oraz podstawę prawną przetwarzania danych osobowych,
- nazwy odbiorców danych osobowych lub kategorie odbiorców, jeżeli są już znane. Odbiorcy to również podmioty, którym administrator w drodze umowy powierzył przetwarzanie danych, na przykład Instytucja Pośrednicząca PO WER, Beneficjent,
- gdy ma to zastosowanie informacje o przekazywaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej,
- okres, przez który dane osobowe będą przetwarzane, a gdy nie jest to możliwe, kryteria ustalenia tego okresu,
- o prawie do żądania dostępu do danych osobowych dotyczących osoby, której dane dotyczą,
- o prawie do wniesienia skargi do organu nadzorczego, to jest PUODO,
- o tym czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych.

Wyżej wymienionych danych nie trzeba podawać jeżeli osoba, której dane dotyczą dysponuje już tymi informacjami.

RODO nie definiuje formy, w jakiej należy podawać informacje w przypadku zbierania danych od osoby, której dane dotyczą. Jednak obowiązek ten musi zostać zrealizowany skutecznie. Dobrą praktyką jest przedłożenie osobie fizycznej klauzuli zawierającej wszystkie wyżej wymienione informacje. Można również do takiej osoby wysłać korespondencję elektroniczną, która będzie zawierała wspomniane informacje lub dołączyć klauzulę do kierowanej w wersji papierowej korespondencji.

Szczegółowo kwestie i zakres obowiązku informacyjnego reguluje art. 13 RODO.

Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą dodatkowo osobę fizyczną należy poinformować o źródle pochodzenia danych.

Szczegółowe regulacje dotyczące pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą dostępne są w art. 14.

W PO WER obowiązek informacyjny w stosunku do uczestników projektu należy realizować przy użyciu *Oświadczenia uczestnika Projektu*, którego zwór stanowi załącznik do *Umowy o dofinansowanie projektu*. Podpisane przez uczestników oświadczenia stanowią dokumentację projektu i Beneficjent przechowuje je w swojej siedzibie. Należy jednocześnie zwrócić uwagę, że treść oświadczenia, która odpowiada informacjom wymaganym przez RODO należy stosować zarówno do projektów, dla których została zawarta *Umowa o dofinansowanie projektu* w dniu 25 maja 2018 r. i później, jak i w tych projektach, które są już realizowane na podstawie umowy zawartej przed 25 maja 2018 r. Dla projektów już realizowanych obowiązek informacyjny według nowych zasad należy realizować wobec uczestników projektów, którzy dopiero przystępują do projektów. Zmiana treści dotychczasowego oświadczenia nie wymaga aneksowania ww. umowy.

Należy również podkreślić, że zgodnie z art. 13 i 14 RODO obowiązek informowania osób realizowany jest w stosunku do wszystkich osób fizycznych. Oznacza, to że obowiązek ten należy realizować nie tylko w stosunku do uczestników projektów, ale wszystkich osób, których dane osobowe pojawiają się w projekcie, na przykład personelu projektu, partnerów, innych podmiotów które świadczą w projekcie usługi na zlecenie Beneficjenta.

W stosunku do osób fizycznych, innych niż uczestnicy projektów, *Umowa o dofinansowanie projektu* nie wskazuje w jakiej formie obowiązek powinien zostać zrealizowany. Należy jednak zadbać, aby obowiązek ten bez żadnych wątpliwości został zrealizowany skutecznie.

KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO”, [nazwa i adres podmiotu udzielającego informację] informuje, że:

1. Administratorem Pani/Pana danych osobowych jest minister właściwy do spraw rozwoju regionalnego, pełniący funkcję Instytucji Zarządzającej dla Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020, z siedzibą w Warszawie przy ul. Wspólnej 2/4, 00-926 Warszawa. Z Administratorem danych można się skontaktować poprzez adres e-mailowy: kancelaria@miir.gov.pl lub pisemnie przekazując

korespondencję na adres siedziby Administratora.

2. Administrator wyznaczył inspektora ochrony danych, z którym może się Pani/Pan skontaktować poprzez e-mail: iod@miir.gov.pl lub pisemnie przekazując korespondencję na adres siedziby Administratora. Z inspektorem ochrony danych można się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych.

Administrator powierzył przetwarzanie Pani/Pana danych osobowych, na podstawie zawartej umowy o dofinansowanie projektu, [nazwa podmiotu, któremu powierzono przetwarzanie danych osobowych]. Może się Pani/Pan również skontaktować z inspektorem ochrony danych [nazwa podmiotu, któremu powierzono przetwarzanie danych osobowych], podmiotu który realizuje projekt nr [numer projektu] poprzez email: [adres e-mail].

3. Przetwarzanie Pani/Pana danych osobowych w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020 odbywa się na podstawie art. 6 ust. 1 pkt c oraz art. 9 ust. 2 lit. g RODO:

–rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 1303/2013 z dnia 17.12.2013 r. ustanawiającego wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności, Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich oraz Europejskiego Funduszu Morskiego i Rybackiego oraz ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności i Europejskiego Funduszu Morskiego i Rybackiego oraz uchylającego rozporządzenie Rady (WE) nr 1083/2006 (Dz.U.UE.L.2013.347.320, z późn. zm.);

–rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 1304/2013 z dnia 17 grudnia 2013 r. w sprawie Europejskiego Funduszu Społecznego i uchylającego rozporządzenie Rady (WE) nr 1081/2006 (Dz.U.UE.L.2013.347.470) oraz załącznika I i II do tego rozporządzenia;

–rozporządzenia Wykonawczego Komisji (UE) nr 1011/2014 z dnia 22 września 2014 r. ustanawiającego szczegółowe przepisy wykonawcze do Rozporządzenia Parlamentu europejskiego i Rady (UE) nr 1303/2013 w odniesieniu do wzorów służących do przekazywania Komisji określonych informacji oraz szczegółowe przepisy dotyczące wymiany informacji między beneficjentami a instytucjami zarządzającymi, certyfikującymi, audytowymi i pośredniczącymi(Dz. Urz. UE L 286 z 30.09.2014);

–ustawy z dnia 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014-2020.

4. Pani/ Pana dane osobowe będą przetwarzane wyłącznie w celu realizacji projektu, w szczególności potwierdzenia kwalifikowalności wydatków, udzielenia wsparcia, monitoringu, ewaluacji, kontroli, audytu i sprawozdawczości oraz działań informacyjno-promocyjnych w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020.

5. Podanie danych jest wymogiem niezbędnym do realizacji ww. celu, o którym mowa w

pkt. 4. Konsekwencje niepodania danych osobowych wynikają z przepisów prawa, w tym uniemożliwiają udział w projekcie realizowanym w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020.

6. Pani/ Pana dane osobowe zostały powierzone Instytucji Pośredniczącej [nazwa i adres właściwej Instytucji Pośredniczącej], beneficjentowi realizującemu projekt [nazwa i adres podmiotu, któremu powierzono dane] oraz podmiotom, które na zlecenie beneficjenta uczestniczą w realizacji projektu [nazwa i adres ww. podmiotów]. Pani/ Pana dane osobowe mogą zostać również powierzone specjalistycznym firmom, realizującym na zlecenie Instytucji Zarządzającej, Instytucji Pośredniczącej oraz beneficjenta ewaluację, kontrole i audyt w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020.
7. Pani/ Pana dane osobowe mogą zostać udostępnione organom upoważnionym zgodnie z obowiązującym prawem.
8. Dane będą przechowywane przez okres niezbędny do realizacji celu, o którym mowa w pkt. 4, do momentu wygaśnięcia obowiązku przechowywania danych wynikającego z przepisów prawa.
9. W związku z przetwarzaniem Pani/Pana danych osobowych przysługują Pani/Panu następujące uprawnienia: prawo dostępu do swoich danych osobowych, prawo żądania ich sprostowania, usunięcia lub ograniczenia ich przetwarzania.
10. W przypadku powzięcia informacji o niezgodnym z prawem przetwarzaniu danych, przysługuje Pani/ Panu również prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych, którym jest Prezes Urzędu Ochrony Danych Osobowych.
11. Pani/Pana dane nie będą podlegały zautomatyzowanemu podejmowaniu decyzji i nie będą profilowane.
12. Pani/ Pana dane osobowe nie będą przekazywane do państwa trzeciego.

.....
Podpis osoby, która zapoznała się z klauzulą informacyjną

17. Jak długo można przetwarzać dane osobowe?

Dane osobowe mogą być przetwarzane wyłącznie przez pewien okres, nie dłuższy jest to niezbędne do zrealizowania celu, dla którego dane te są przetwarzane. Okres ten może być dłuższy jeżeli dane osobowe będą przetwarzane na przykład do celów archiwalnych w interesie publicznym.

Katalog wszystkich przypadków opisujący ograniczenia przechowywania dostępny jest w art. 5 ust. 1 lit. e) RODO.

W PO WER dane osobowe przetwarzane będą do czasu rozliczenia Programu Operacyjnego Wiedza Edukacja Rozwój 2014 -2020 oraz zakończenia archiwizowania dokumentacji, który to okres wynika z ustawy o narodowym zasobie archiwalnym i archiwach.

18. Co to jest rejestr czynności przetwarzania danych osobowych i czy muszę go prowadzić?

Prowadzenie rejestru czynności przetwarzania danych osobowych jest jednym z wymogów RODO i stanowi jeden z elementów dokumentacji dotyczącej przetwarzania danych osobowych. Rejestr prowadzony jest odrębnie przez administratora i każdy podmiot, któremu zostało powierzone przetwarzanie danych osobowych.

Podmiot przetwarzający prowadzi rejestr czynności przetwarzania, w którym odnotowuje:

- nazwę oraz dane kontaktowe podmiotu przetwarzającego,
- kategorie przetwarzania dokonanych w imieniu administratora – jest to rodzaj usługi realizowanej przez podmiot przetwarzający na zlecenie administratora. Przykładowymi rodzajami takich usług mogą być na przykład: zbieranie danych od osób fizycznych w związku z realizacją projektu, przechowywanie danych, modyfikowanie danych, wykorzystywanie danych w celu raportowania z realizacji projektu, powierzanie danych innym podmiotom w imieniu administratora w związku z realizacją projektu,
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o którym mowa w art. 32 RODO – jest to ogólny opis technicznych i organizacyjnych środków bezpieczeństwa. Opis powinien wskazywać na najważniejsze założenia czy elementy przyjętych systemów lub koncepcji w zakresie bezpieczeństwa danych osobowych. Ogólny opis jest uzasadniony zwłaszcza w przypadkach, gdy koncepcje te obejmują wiele elementów i rozwiązań, które uszczegółowione są w dokumentacji, polityce bezpieczeństwa lub procedurach. W rejestrze należy zamieścić ogólną informację o rodzaju zastosowanych zabezpieczeń (na przykład: kontrola dostępu do systemów w oparciu o identyfikator i hasło, kontrolowany dostęp do budynku i pomieszczeń) i odesłanie do dokumentacji opisującej szczegóły zarządzania danego rodzaju zabezpieczeniami.

Rejestr prowadzony jest w formie pisemnej. RODO jednocześnie nie narzuca wymagań dotyczących postaci, w jakiej rejestr powinien być prowadzony, wskazując, że może to być postać zarówno papierowa, jak i elektroniczna.

Rejestru czynności przetwarzania danych nie muszą prowadzić podmioty zatrudniające mniej niż 250 osób pod warunkiem, że nie przetwarzają danych szczególnej kategorii (danych wrażliwych).

Dodatkowe informacje na temat rejestru czynności przetwarzania dostępne są w art. 30 RODO.

Wskazówki i wyjaśnienia dotyczące prowadzenia rejestrów czynności przetwarzania dostępne są również na stronach UODO pod adresem <https://uodo.gov.pl/pl/123/214>.

W projektach PO WER przetwarzane są dane szczególnych kategorii. Oznacza to, że stosując przepisy RODO Beneficjenci nie są zwolnieni z prowadzenia rejestru. Na prowadzenie przez Beneficjentów rejestru czynności przetwarzania wskazuje również zawarta *Umowa o dofinansowania projektu*.

Rejestr czynności przetwarzania u Beneficjenta powinien zawierać co najmniej następujące informacje:

- nazwę oraz dane kontaktowe podmiotu przetwarzającego – należy podać nazwę oraz adres podmiotu, któremu administrator powierzył przetwarzanie danych,
- kategorie przetwarzanych danych – można ją określić jako przetwarzanie danych osobowych w związku z realizacją projektów w ramach Programu Operacyjnego Wiedza Edukacja Rozwój,
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa – w punkcie należy wskazać m.in. jakie środki bezpieczeństwa są stosowane: na przykład: kontrola dostępu do systemów informatycznych z wykorzystaniem identyfikatora i hasła, dostęp do danych tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy na stacjach roboczych, na których są przetwarzane dane osobowe, system wykrywania włamań. Zamykane szafy w pomieszczeniach zamykanych na klucz, dostępnych tylko dla upoważnionych osób. Monitorowany dostęp do budynku. W punkcie powinno się znaleźć odwołanie do dokumentów, które szczegółowo określają politykę bezpieczeństwa w organizacji, na przykład do polityki bezpieczeństwa systemów teleinformatycznych.

19. W jaki sposób należy powierzyć przetwarzanie danych osobowych?

Jeżeli podmiot, który przetwarza dane osobowe na zlecenie administratora planuje umożliwić przetwarzanie danych osobowych innemu podmiotowi powinien z tym podmiotem zawrzeć umowę, tak zwaną umowę powierzenia, w której określone zostaną zasady przetwarzania danych osobowych.

Istotną różnicą w stosunku do przepisów, które obowiązywały przez 25 maja 2018 r. jest prawny obowiązek powierzenia przetwarzania danych osobowych tylko takim podmiotom, które zagwarantują odpowiednią ochronę danych osobowych.

Dodatkowo od podmiotu, któremu powierza się przetwarzanie danych osobowych przepisy RODO wymagają:

- zapewnienia, aby osoby przetwarzające dane osobowe były do tego umocowane (posiadały upoważnienia do przetwarzania danych osobowych),
- zapewnienia, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy,
- zapewnienia środków zabezpieczenia danych osobowych oraz pomagania administratorowi wywiązać się z tych obowiązków,
- zapewnienia, aby w przypadku korzystania z usług innego podmiotu zapewnić w drodze umowy powierzenia przetwarzanie danych zgodnie z RODO,
- zobowiązania, aby podmiot, któremu powierzono przetwarzanie danych osobowych pomagał administratorowi wywiązać się z obowiązku odpowiadania na pytania osoby, której dane dotyczą, w zakresie wykonywania jej praw, na które wskazuje RODO,
- zobowiązania podmiotu do udzielania odpowiedzi na pytania administratora,
- zobowiązania podmiotu do przeprowadzenia audytu poprawności przetwarzania danych osobowych z obowiązującymi przepisami w zakresie przetwarzania danych osobowych,
- zobowiązania podmiotu do usunięcia danych osobowych lub do ich zwrotu do administratora, w sytuacji kiedy został zrealizowany cel ich przetwarzania.

W PO WER zawarta z Beneficjentem *Umowa o dofinansowanie projektu* pozwala na powierzenie przetwarzania danych osobowych przez Beneficjenta innemu podmiotowi wykonującemu zadania związane z udzielaniem wsparcia i realizacją projektu, pod warunkiem spełnienia wymogów RODO oraz zapisów ww. umowy.

Beneficjent zobligowany jest do zawarcia z podmiotem, któremu powierza przetwarzanie danych osobowych umowę powierzenia. Zanim jednak umowa z podmiotem zostanie zawarta Beneficjent musi wystąpić do Instytucji Pośredniczącej, z którą zawartą ma *Umowę o dofinansowanie projektu* o zgodę na powierzenie przetwarzania danych. Jeżeli w okresie 7 dni roboczych od dnia wpłynięcia informacji o zamiarze powierzenia przetwarzania danych osobowych Instytucja Pośrednicząca nie wyrazi sprzeciwu Beneficjent może zawrzeć umowę powierzenia. Podmiot, któremu Beneficjent powierzył przetwarzanie danych osobowych nie jest umocowany do dalszego powierzenia danych innemu podmiotowi. W takim przypadku, jeżeli dalsze powierzenie danych jest

uzasadniono, umowę powierzenia, ze wskazanym przez podmiot podmiotem, może zawrzeć Beneficjent.

20. Czy należy wystąpić do Instytucji Pośredniczącej z informacją o zamiarze powierzenia przetwarzania danych?

Beneficjent, który przy realizacji projektu zamierza korzystać z usług innego podmiotu, musi zawrzeć z tym podmiotem umowę powierzenia przetwarzania danych osobowych. Aby to zrobić, zgodnie z zapisami *Umowy o dofinansowanie projektu*, Beneficjent powinien zwrócić się do Instytucji Pośredniczącej z informacją o planowanym powierzeniu danych innemu podmiotowi. W zgłoszeniu Beneficjent powinien podać nazwę podmiotu, któremu planuje powierzyć dane oraz adres jego siedziby. Jeżeli Instytucja Pośrednicząca, w terminie 7 dni od wpłynięcia informacji, nie wyrazi sprzeciwu Beneficjent będzie mógł zawrzeć umowę powierzenia.

W szczególnych przypadkach, na przykład jeżeli Beneficjent realizując zadania statutowe działa w oparciu o przepis prawa, nie dochodzi do powierzenia danych osobowych, a do ich udostępnienia. Taka sytuacja może mieć miejsce w przypadku projektów realizowanych przez Powiatowe Urzędy Pracy, które realizują swoje zadania na podstawie ustawy o promocji zatrudnienia i instytucjach rynku pracy oraz przepisów wykonawczych do tej ustawy. Oznacza to, że co do zasady nie powierzają one przetwarzania danych osobowych w trybie art. 28 RODO, lecz udostępniają je podmiotom, z którymi współpracują w celach odbycia stażu czy przygotowania zawodowego dorosłych. O ile zatem zakres danych osobowych przekazywany podmiotom współpracującym z Powiatowymi Urzędami Pracy nie wykracza poza właściwy dla danej formy wsparcia, określony w aktach prawnych, następuje udostępnienie danych a nie powierzenie ich przetwarzania. Natomiast w przypadku przekazywania ww. podmiotom szerszego zakresu danych osobowych niż wynikający z ustawy i rozporządzeń, zgodnego z zakresem zbioru *Program Operacyjny Wiedza Edukacja Rozwój*, na przykład w celu zlecenia firmie szkoleniowej zebrania od uczestników odbywającego się w ramach projektu powiatowego urzędu pracy dodatkowych danych osobowych, niezbędnych do wypełnienia w Centralnym systemie teleinformatycznym SL2014 modułu monitorowania uczestników, powierzenie danych do przetwarzania następuje w trybie art. 28 RODO, co skutkuje zgodnie z zapisami *umowy o dofinansowanie projektu* koniecznością uzyskania zgody IP i podpisania umowy powierzenia z podmiotem organizującym na przykład staż.

21. Co oznacza obowiązek zgłaszania naruszeń ochrony danych?

Obowiązek zgłoszenia naruszeń ochrony danych wynika z art. 33 RODO. W przypadku naruszenia ochrony danych osobowych administrator nie później niż w terminie 72 godzin po stwierdzeniu naruszenia zgłasza je do PUODO. W niektórych przypadkach, gdy może to

powodować wysokie prawdopodobieństwo naruszenia praw i wolności osoby, której dane dotyczą należy również o naruszeniu poinformować tę osobę.

W PO WER zgodnie z zapisami *Umowy o dofinansowanie projektu*, jeżeli Beneficjent stwierdzi naruszenie w przetwarzaniu danych osobowych, zobowiązany jest zgłosić je bez zbędnej zwłoki, nie później jednak niż w ciągu 24 godzin do Instytucji Pośredniczącej, z którą zawarł *Umowę o dofinansowanie projektu*. Zgłoszenie powinno:

- opisywać charakter naruszenia ochrony danych osobowych, w tym kategorie danych (na przykład dane uczestników) i przybliżoną liczbę osób, których dotyczy naruszenie,
- zawrzeć dane kontaktowe osoby u Beneficjenta, od której można uzyskać więcej informacji,
- zawierać opis możliwych konsekwencji naruszenia ochrony danych osobowych,
- zawierać opis proponowanych środków w celu zaradzenia naruszeniu ochrony danych osobowych, w tym opis środków w celu zminimalizowania jego ewentualnych negatywnych skutków,
- zawierać informacje umożliwiające administratorowi określenie, czy naruszenie skutkuje wysokim ryzykiem naruszenia praw lub wolności osób fizycznych.

22. Co oznacza podejście przetwarzania oparte na ryzyku i w jaki sposób należy zabezpieczyć przetwarzanie danych osobowych?

RODO w przeciwieństwie do poprzedniej ustawy o ochronie danych osobowych odchodzi od wskazywania konkretnych środków zabezpieczenia danych osobowych jakie powinny zostać wdrożone przez administratora danych osobowych i podmiot przetwarzający, któremu przetwarzanie danych osobowych zostało powierzone. Nie wskazuje również rodzaju dokumentów jakie należy posiadać. Wcześniej wymagane było posiadanie przez podmiot polityki bezpieczeństwa oraz w sytuacji, gdy dane były przetwarzane z wykorzystaniem systemu informatycznego również instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Zamiast tych rozwiązań RODO przewiduje przetwarzanie danych osobowych oparte na ryzyku. Oznacza to, że każdy podmiot powinien w sposób świadomy, samodzielnie określić jakie środki powinien wdrożyć, żeby zadbać o bezpieczeństwo przetwarzanych danych. Jest to o tyle istotne, że każdy podmiot przetwarzający ponosi odpowiedzialność w przypadku naruszenia bezpieczeństwa danych osobowych.

Podejście oparte na ryzyku wymaga ciągłego analizowania ryzyka i stałego dostosowywania środków technicznych i organizacyjnych do prawdopodobieństwa wystąpienia zagrożeń,

charakteru przetwarzanych danych osobowych oraz ich celu i środowiska, w którym są przetwarzane.

RODO reguluje podejście przetwarzania danych oparte na ryzyku w art. 32.

Na stronie internetowej UODO, pod adresem <https://uodo.gov.pl/pl/123/208>, dostępne są materiały jak rozumieć i stosować podejście oparte na ryzyku.

W pierwszej części, zatytułowanej *Jak rozumieć podejście oparte na ryzyku według RODO?*, eksperci UODO wyjaśniają istotę zasady podejścia opartego na ryzyku oraz wskazują, do czego zasada ta zobowiązuje podmioty stosujące przepisy RODO. Tłumaczą też, czym jest ryzyko naruszenia praw i wolności osób, których dane dotyczą. Podkreślają przy tym należy, że szacowanie ryzyka to proces ciągły, który powinien być przeprowadzany przy użyciu konkretnej metody, zapewniającej jednocześnie stosowanie jednolitych definicji i pojęć.

W drugiej części, zatytułowanej *Jak stosować podejście oparte na ryzyku?*, przedstawione zostały kolejne możliwe etapy działań podejmowanych w celu przeprowadzania ogólnej oceny ryzyka oraz szczegółowej oceny ryzyka, czyli tzw. oceny skutków dla ochrony danych.

23. Czy za nieprzestrzeganie RODO może zostać nałożona kara?

Za nieprzestrzeganie RODO może zostać nałożona kara pieniężna. Kara może zostać nałożona na administratora danych oraz podmiot przetwarzający, który dopuścił się przetwarzania danych osobowych niezgodnie z przepisami prawa powszechnie obowiązującego, to jest RODO i UODOA. Karę w drodze decyzji administracyjnej nakłada PUODO.

Warunki nakładania administracyjnych kar pieniężnych reguluje art. 83 RODO oraz rozdział 11 UODOO.