Warszawa, dnia 4 października 2019 r.

Poz. 5

Z A R Z Ą D Z E N I E

M I N I S T R A F I N A N S Ó W, I N W E S T Y C J I I R O Z W O J U [1)]

z dnia 3 października 2019 r.

w sprawie Polityki ochrony danych osobowych w Ministerstwie Inwestycji i Rozwoju

Na podstawie art. 34 ust. 1 ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz. U. z 2019 r. poz. 1171) zarządza się, co następuje.

§ 1. W Ministerstwie Inwestycji i Rozwoju wprowadza się Politykę ochrony danych osobowych stanowiącą załącznik do zarządzenia.

§ 2. Zarządzenie wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

MINISTER FINANSÓW, INWESTYCJI I ROZWOJU

[1)] Minister Finansów, Inwestycji i Rozwoju kieruje działami administracji rządowej - budownictwo, planowanie i zagospodarowanie przestrzenne oraz mieszkalnictwo i rozwój regionalny na podstawie § 1 ust. 2 pkt 1 i 5 rozporządzenia Prezesa Rady Ministrów z dnia 26 września 2019 r. w sprawie szczegółowego zakresu działania Ministra Finansów, Inwestycji i Rozwoju (Dz. U. poz. 1841).

Załącznik do zarządzenia
Ministra Finansów, Inwestycji i Rozwoju
z dnia 3 października 2019 r.

Rozdział 1

Postanowienia ogólne

§ 1. 1. Polityka Ochrony Danych Osobowych, zwana dalej „Polityką”, określa zasady przetwarzania danych osobowych, dla których Minister Finansów, Inwestycji i Rozwoju, zwany dalej „Ministrem”, jest administratorem, zarówno w Ministerstwie Inwestycji i Rozwoju, zwanym dalej „Ministerstwem”, jak i poza jego siedzibą.

2. Politykę stosuje się do danych osobowych przetwarzanych:

1) w sposób całkowicie lub częściowo zautomatyzowany, w szczególności w systemie Elektronicznego Zarządzania Dokumentacją, innych systemach teleinformatycznych, poczcie elektronicznej, dyskach komputerów, dyskach sieciowych, pendrivach, telefonach oraz drukarkach;
2) w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych Ministerstwa, stanowiących zbiory danych w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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, z późn. zm.), zwanego dalej „RODO".

3. Politykę stosuje się także do przetwarzanych w Ministerstwie danych osobowych, których administratorem nie jest Minister, chyba że zawarte przez Ministra porozumienia z administratorami danych stanowią inaczej.

4. Polityki nie stosuje się do danych osobowych zawartych w dokumentach papierowych, jeżeli nie stanowią one części zbioru danych osobowych lub nie mają wejść w skład takiego zbioru. Do ochrony takich dokumentów stosuje się ogólne zasady bezpieczeństwa informacji.

5. Ze względu na specyfikę przetwarzania danych osobowych w Programach Operacyjnych oraz w Centralnym Systemie Teleinformatycznym wspierającym realizację Programów Operacyjnych dopuszcza się uregulowanie zasad przetwarzania danych osobowych w powyższych obszarach w odrębnych regulacjach wewnętrznych.

6. Regulacje, o których mowa w ust. 5, mają charakter przepisów szczególnych wobec Polityki oraz wydanych na jej podstawie wytycznych, zaleceń, wzorów dokumentów oraz standardowych środków organizacyjnych i technicznych przetwarzania danych osobowych.

7. Zasady oraz zakres obowiązków i odpowiedzialności użytkowników systemów teleinformatycznych w zakresie ochrony danych osobowych określają odrębne przepisy.

8. Kierujący BPB może dopuścić stosowanie w Ministerstwie szczegółowych instrukcji zarządzania systemami informatycznymi przetwarzającymi dane osobowe dla wyodrębnionych systemów informatycznych, o ile będą one zgodne z Polityką. Użytkownicy tych systemów mają obowiązek zapoznania się z taką instrukcją.

§ 2. Celem Polityki jest zapewnienie szczególnej ochrony interesów osób, których dane osobowe przetwarzane są w Ministerstwie lub dla których Minister jest administratorem, a w szczególności zapewnienie, aby dane te były:

1) przetwarzane zgodnie z prawem;
2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane przetwarzaniu niezgodnie z tymi celami;
3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

§ 3. 1. Przetwarzanie danych osobowych w Ministerstwie odbywa się zgodnie z:

1) RODO;
2) ustawą o ochronie danych osobowych, z dnia 10 maja 2018 (Dz.U. z 2019 r. poz. 1781), zwaną dalej „UODO”.

2. Przetwarzając dane osobowe w Ministerstwie uwzględnia się rekomendacje, stanowiska i wytyczne:

1) Prezesa Urzędu Ochrony Danych Osobowych (także organu poprzedzającego);
2) Europejskiej Rady Ochrony Danych;
3) Grupy Roboczej ds. Ochrony Danych Osobowych w Ministerstwie Cyfryzacji.

§ 4. 1. Użyte w Polityce określenia i skróty oznaczają:

1) analiza DPIA – ocenę skutków planowanych operacji przetwarzania dla ochrony danych osobowych, której dokonuje administrator, jeżeli dany rodzaj przetwarzania, w szczególności z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych; przeprowadzenie takiej analizy wymagane jest w przypadkach określonych w art. 35 ust. 3 RODO oraz danych rodzajów przetwarzania, które zostały wskazane w wykazie podanym do publicznej wiadomości przez krajowy organ nadzorczy, zgodnie z art. 35 ust. 4 RODO;

2) analiza ryzyka naruszenia praw lub wolności osób fizycznych – analizę możliwości nieosiągnięcia celów ochrony danych osobowych (lub braku możliwości zapewnienia ochrony danych osobowych na akceptowalnym poziomie);
3) BA – komórkę właściwą do spraw ochrony fizycznej;
4) BPB – komórkę właściwą do spraw koordynacji ochrony danych osobowych;
5) BZL – komórkę właściwą do spraw szkoleń;
6) Członek Kierownictwa Ministerstwa – Ministra, Sekretarzy i Podsekretarzy Stanu w Ministerstwie oraz Dyrektora Generalnego Ministerstwa;
7) DI – komórkę właściwą do spraw informatyki;
8) kierujący komórką organizacyjną – dyrektora departamentu, biura, a także szefa Gabinetu Politycznego Ministra lub osoby ich zastępujące;
9) Koordynator ds. Ochrony Danych Osobowych – osoba wyznaczona przez kierującego komórką organizacyjną w celu wsparcia realizacji zadań z zakresu ochrony danych osobowych w tej komórce;
10) komórka organizacyjna – departament, biuro lub Gabinet Polityczny Ministra;
11) komunikat PUODO – wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych wydany przez Prezesa Urzędu Ochrony Danych Osobowych na podstawie art. 35 ust. 4 RODO;
12) IOD – Inspektor Ochrony Danych;
13) Pełnomocnik ds. Ochrony Danych Osobowych – osoba wyznaczona przez administratora do wykonywania określonych w Polityce zadań z zakresu ochrony danych osobowych w obszarze wskazanym przez administratora;
14) pracownik – osobę zatrudnioną w Ministerstwie na podstawie stosunku pracy;
15) privacy by default (zasada prywatności w ustawieniach domyślnych) – uwzględnienie ochrony danych w ustawieniach domyślnych; zakłada ochronę prywatności, jako domyślne ustawienie każdego programu (systemu), a zmiana takiego ustawienia powinna następować jedynie na wyraźne żądanie gestora programu;
16) privacy by design (zasada prywatności w fazie projektowania) – uwzględnienie ochrony danych w fazie projektowania; „wbudowanie” zasad ochrony prywatności w każdy projekt zakładający przetwarzanie danych osobowych w taki sposób, aby od samego początku jego istnienia ochrona prywatności stanowiła jego część składową;
17) Regulaminy – dokumenty określające zasady oraz zakresy obowiązków i odpowiedzialności użytkowników systemów teleinformatycznych w zakresie ochrony danych osobowych przyjęte do stosowania na podstawie wewnętrznych regulacji lub umów zawartych przez Ministerstwo;

18) ryzyko akceptowalne (naruszenia praw i wolności osób fizycznych) – poziom ryzyka, który jest akceptowany w procesie formalnego szacowania ryzyka - bezwarunkowo lub warunkowo, przy czym w tym drugim przypadku należy podejmować próby dalszego ograniczenia ryzyka; poziom ryzyka akceptowalnego określa szczegółowo odrębna metodyka;
19) ryzyko nieakceptowalne (naruszenia praw i wolności osób fizycznych) - poziom ryzyka, który nie może zostać zaakceptowany bez podjęcia skutecznych działań ograniczających ryzyko do poziomu akceptowalnego, a w przypadku braku możliwości ograniczenia tego ryzyka należy zrezygnować z tych operacji przetwarzania, które są głównym źródłem wysokiego ryzyka; proces szczegółowo określa odrębna metodyka;
20) użytkownik – pracownika, stażystę, wolontariusza, praktykanta lub inną osobę wykonującą pracę bądź świadcząca usługi na rzecz Ministra lub Ministerstwa, albo powołaną przez Członka Kierownictwa Ministerstwa do wykonywania określonych czynności (np. członkowie zespołów, komisji);
21) wysoki poziom ryzyka [naruszenia praw i wolności osób fizycznych] – poziom ryzyka wymagający formalnie przeprowadzenia oceny DPIA i ograniczenia ryzyka do poziomu akceptowalnego, a w przypadku braku takiej możliwości – konsultacji z UODO; jakościowa miara poziomu ryzyka obejmuje następujące wartości: brak ryzyka (ryzyko niskie), ryzyko (średnie), poważne (wyższe) ryzyko oraz wysokie ryzyko; skalę ryzyka określa szczegółowo odrębna metodyka;
22) wyższy poziom ryzyka (poważne ryzyko) – poziom ryzyka poważnego, w którym następuje warunkowa akceptacja ryzyka z jednoczesnym podjęciem działań w celu ograniczenia ryzyka.

2. Pojęcia niezdefiniowane w Polityce mają znaczenie nadane im w Polityce Bezpieczeństwa Informacji w Ministerstwie oraz RODO.

Rozdział 2

Zasady przetwarzania danych osobowych

§ 5. 1. Przed rozpoczęciem przetwarzania danych osobowych kierujący komórką organizacyjną wykonuje analizę planowanej czynności przetwarzania obejmującą określenie:

1) celu i podstawy prawnej przetwarzania danych osobowych;
2) rodzajów przetwarzanych danych osobowych oraz kategorii osób, których dane dotyczą;
3) okresu przetwarzania danych osobowych;
4) sposobu pozyskania i przechowywania danych osobowych oraz rodzajów podmiotów, którym dane te będą udostępnianie;
5) sposobu realizacji obowiązku informacyjnego, o którym mowa w art. 13 i 14 RODO,

- z uwzględnieniem zasad privacy by design i privacy by default oraz zasad określonych w art. 5 RODO, a następnie we współpracy z kierującymi BPB, DI oraz BA dokonuje analizy ryzyka naruszenia praw lub wolności osób fizycznych, zgodnie z metodyką sporządzania analizy ryzyka naruszenia praw lub wolności osób fizycznych i analizy DPIA.

2. W przypadku, gdy w wyniku dokonania analizy ryzyka nie zostanie zidentyfikowany wysoki lub wyższy poziom ryzyka, kierujący właściwą komórką organizacyjną wdraża standardowe środki organizacyjne i techniczne przetwarzania danych osobowych, z zastrzeżeniem § 1 ust. 5 i 6, a następnie rozpoczyna przetwarzanie danych osobowych, począwszy od ich zebrania lub innej czynności rozpoczynającej przetwarzanie.

3. W przypadku, gdy w wyniku przeprowadzenia analizy ryzyka zidentyfikowany zostanie wysoki lub wyższy poziom ryzyka, kierujący komórką organizacyjną, we współpracy z kierującym BPB, DI i BA oraz IOD:

1) określa i wdraża dodatkowe środki organizacyjne i techniczne;
2) wykonuje inne czynności zmierzające do obniżenia poziomu ryzyka lub
3) przedstawia właściwemu Członkowi Kierownictwa Ministerstwa wniosek o akceptację poziomu ryzyka wraz z uzasadnieniem.

4. W przypadku, gdy w wyniku przeprowadzenia analizy ryzyka zidentyfikowany zostanie wysoki lub wyższy poziom ryzyka, a także w przypadkach, o których mowa w art. 35 RODO i Komunikacie PUODO, kierujący komórką organizacyjną, we współpracy z kierującym BPB, DI i BA oraz IOD, dokonuje analizy DPIA.

5. Analizę ryzyka naruszenia praw lub wolności osób fizycznych oraz analizę DPIA ponawia się nie rzadziej niż raz w roku oraz w przypadku wprowadzenia istotnych zmian w czynności przetwarzania danych osobowych, w szczególności dotyczących:

1) rozszerzenia zakresu przetwarzanych danych;
2) zmiany celu przetwarzania;
3) zmiany podstawy prawnej przetwarzania danych;
4) zmiany środków organizacyjno-technicznych;
5) zmiany otoczenia prawnego.

Przepisy ust. 3 i 4 stosuje się odpowiednio.

6. Kierujący komórką organizacyjną dokumentuje wykonanie czynności, o których mowa w ust. 1-5.

§ 6. 1. Dane osobowe przetwarzane w Ministerstwie mogą być przekazywane innym podmiotom w formie upublicznienia (udostępnienia) albo w formie powierzenia przetwarzania, zależnie od

stosunku prawnego łączącego administratora z tym podmiotem. W niektórych przypadkach stosunek prawny łączący Ministra i inny podmiot może być również stosunkiem współadministrowania.

2. Powierzenie przetwarzania danych osobowych, określenie zadań i obowiązków współadministratorów, a także przekazanie danych osobowych do państw trzecich (poza Europejski Obszar Gospodarczy) wymaga zawarcia umowy w formie pisemnej, elektronicznej lub dokumentowej. Projekty umów powierzenia przetwarzania danych osobowych sporządza się z uwzględnieniem wzorów określonych przez kierującego BPB lub zaopiniowanych przez BPB.

3. Projekty umów powierzenia przetwarzania danych osobowych kierujący komórką organizacyjną może przekazać do zaopiniowania przez BPB. W przypadku, w którym wprowadzono istotne modyfikacje względem wzoru określonego przez kierującego BPB, w szczególności dokonano zmiany elementów umowy, które we wzorze nie zostały przewidziane do modyfikacji, uzyskanie opinii BPB jest obowiązkowe.

4. Projekt umowy w sprawie współadministrowania danymi osobowymi oraz projekt umowy na podstawie których nastąpi przekazanie danych osobowych do państw trzecich podlega zaopiniowaniu przez BPB.

5. Oryginały umów powierzenia przetwarzania danych osobowych, umów w sprawie współadministrowania oraz umów na podstawie których nastąpi przekazanie danych osobowych do państw trzecich przechowuje komórka organizacyjna zawierająca umowę.

6. Komórki organizacyjne prowadzą rejestry zawartych umów powierzenia przetwarzania danych oraz porozumień w sprawie współadministrowania. Wzór rejestru stanowi załącznik nr 1 do Polityki.

7. Komórki organizacyjne udostępniają BPB oraz IOD aktualny rejestr umów powierzenia przetwarzania oraz porozumień w sprawie współadministrowania – w sposób wskazany przez kierującego BPB.

8. W przypadku, gdy w ramach zawartej umowy powierzenia przetwarzania danych osobowych zawierane są dalsze umowy powierzenia, kierujący komórką organizacyjną dokonuje oceny zgodności dalszych umów powierzenia przetwarzania z umową powierzenia przetwarzania oraz RODO.

§ 7. 1. BPB prowadzi rejestr czynności przetwarzania oraz rejestr kategorii czynności przetwarzania, oraz odpowiada za kompletność i spójność zawartych w nich informacji. Wzory rejestrów stanowią odpowiednio załącznik nr 2 i załącznik nr 3 do Polityki. Rejestry udostępniane są w intranecie.

2. Zmiany w rejestrach zatwierdza kierujący BPB, po uzyskaniu opinii IOD, oraz kierujących właściwymi komórkami organizacyjnymi Ministerstwa.

3. Kierujący BPB we współpracy z kierującymi komórkami organizacyjnymi dokonuje przeglądu rejestrów wymienionych w ust. 1, nie rzadziej niż raz w roku oraz w przypadku wprowadzenia istotnych zmian organizacyjnych w Ministerstwie.

§ 8. 1. Pracownicy, stażyści, wolontariusze i praktykanci ujęci w ewidencji uprawnień do systemu Elektronicznego Zarządzania Dokumentacją upoważnieni są do przetwarzania danych osobowych przetwarzanych w Ministerstwie w zakresie, w jakim jest to niezbędne do wykonywania przez nich obowiązków wynikających z:

1) przepisów prawa powszechnie obowiązującego;
2) regulacji wewnętrznych obowiązujących w Ministerstwie;
3) wiążących Ministra i Ministerstwo umów;
4) umów zawartych z użytkownikami, w szczególności umów o pracę i opisów stanowisk pracy;
5) poleceń wydawanych użytkownikom przez kierujących komórkami organizacyjnymi.

2. W przypadku użytkowników innych, niż wskazani w ust. 1 oraz jeżeli przepisy prawa powszechnie obowiązującego dopuszczają możliwość przetwarzania danych osobowych wyłącznie przez osoby posiadające imienne upoważnienie, upoważnienia do przetwarzania danych osobowych w ramach określonych czynności przetwarzania wydają:

1) kierujący BPB, pełnomocnik ds. ochrony danych osobowych w BPB lub jego zastępca – w odniesieniu do czynności przetwarzania, dla których nie został ustanowiony pełnomocnik ds. ochrony danych osobowych w komórce organizacyjnej;
2) pełnomocnik ds. ochrony danych osobowych w komórce organizacyjnej lub jego zastępca – w odniesieniu do czynności przetwarzania, dla których został ustanowiony.

3. W przypadku, gdy analiza ryzyka wykaże poważne ryzyko naruszenia praw i wolności osób fizycznych, w celu ograniczenia tego ryzyka, kierujący komórką organizacyjną w uzgodnieniu z kierującym BPB może ograniczyć krąg użytkowników posiadających dostęp do danych osobowych do użytkowników posiadających imienne upoważnienie do przetwarzania danych. Kierujący BPB opracowuje i udostępnia w intranecie wykaz danych osobowych, których przetwarzanie wymaga posiadania imiennego upoważnienia.

4. Wydanie imiennego upoważnienia następuje poprzez:

1) podpisanie dokumentu upoważniającego do przetwarzania danych osobowych, sporządzonego zgodnie ze wzorem stanowiącym odpowiednio załączniki nr 4a - 4e do Polityki lub
2) zatwierdzenie, w tym za pomocą podpisu elektronicznego, wniosku o wydanie upoważnienia, stanowiącego załącznik nr 5 do Polityki.

5. Kierujący BPB oraz pełnomocnicy ds. ochrony danych osobowych prowadzą rejestry wydanych imiennych upoważnień, których wzór stanowi załącznik nr 6 do Polityki. Jeżeli

dedykowany system informatyczny, w tym Centralny System Teleinformatyczny wspierający realizację Programów Operacyjnych, umożliwia rejestrowanie wydanych upoważnień imiennych, prowadzenie rejestru upoważnień według wzoru określonego w załączniku nr 6 do Polityki nie jest obligatoryjne.

6. Imienne upoważnienia do przetwarzania danych osobowych tracą moc z dniem ustania stosunku prawnego, na podstawie którego użytkownik wykonuje czynności w komórce organizacyjnej Ministerstwa lub zmiany zakresu obowiązków powodującej zaprzestanie przetwarzania danych osobowych w ramach wskazanej w upoważnieniu kategorii czynności przetwarzania.

7. Kierujący komórką organizacyjną niezwłocznie informuje BPB o okolicznościach, o których mowa w ust. 6.

Rozdział 3

Zakres i zasady ochrony danych osobowych

§ 9. Dokumentacja opisująca sposób przetwarzania danych osobowych oraz sposoby ich zabezpieczenia, w tym w systemach informatycznych służących do przetwarzania danych osobowych przez Ministerstwo, stanowią informacje wrażliwe.

§ 10. W doborze i stosowaniu środków ochrony przetwarzanych danych osobowych szczególną uwagę należy zwracać na należyte ich zabezpieczenie przed udostępnieniem osobom nieuprawnionym, kradzieżą, uszkodzeniem, nieuprawnioną modyfikacją, utratą lub zniszczeniem.

§ 11. Użytkownicy są w szczególności zobowiązani do:

1) przetwarzania danych osobowych zgodnie z RODO i UODO, regulacjami wewnętrznymi, w tym Polityką, wytycznymi kierującego BPB oraz zgodnie z celem, dla którego te dane zostały zebrane;
2) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczania, również po ustaniu zatrudnienia lub innego zobowiązania wynikającego z zawartych umów;
3) przetwarzania danych osobowych w odpowiednio zabezpieczonych pomieszczeniach służbowych lub wyznaczonych ich częściach;
4) bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania informacji w systemie teleinformatycznym, określonych w regulaminach;
5) zabezpieczania zbiorów danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych;
6) niszczenia wszystkich, niepodlegających archiwizacji, niepotrzebnych dokumentów zawierających dane osobowe, w sposób uniemożliwiający ich odczytanie lub odtworzenie;

7) nieudzielania innym podmiotom informacji o przetwarzanych danych osobowych, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione;
8) udziału w szkoleniach obowiązkowych, określonych przez kierującego BZL;
9) współpracy z IOD przy realizacji jego zadań.

§ 12. 1. Za naruszenie obowiązków w zakresie ochrony danych osobowych, pracownicy podlegają odpowiedzialności na podstawie przepisów określonych w UODO, odpowiedzialności dyscyplinarnej wynikającej z przepisów ustawy z dnia 21 listopada 2008 r. o służbie cywilnej (Dz. U. z 2018 r. poz. 1559 oraz z 2019 r. poz. 730) lub porządkowej wynikającej z przepisów prawa pracy.

2. Użytkownicy niebędący pracownikami, za naruszenie obowiązków, o których mowa w ust. 1, podlegają odpowiedzialności przewidzianej w UODO oraz umowach lub aktach powołania.

§ 13. Zasady zgłaszania naruszeń ochrony danych osobowych i postępowania z nimi, w tym oceny spełnienia przesłanek, o których mowa w art. 33 i 34 RODO, regulują odrębne przepisy.

Rozdział 4

Realizacja zadań związanych z ochroną danych osobowych

§ 14. 1. Członkowie Kierownictwa Ministerstwa sprawują, zgodnie z ustalonym podziałem pracy w kierownictwie, nadzór nad przetwarzaniem danych osobowych w podległych komórkach organizacyjnych.

2. Członek Kierownictwa Ministerstwa, z zastrzeżeniem § 13 oraz ust. 4, jest uprawniony do wykonywania wszystkich czynności administratora, w zakresie w jakim jest to niezbędne do wykonywania jego zadań - zgodnie z ustalonym podziałem pracy w kierownictwie, w tym do udzielenia upoważnień/pełnomocnictw pełnomocnikom ds. ochrony danych osobowych, o których mowa w § 19 i 20.

3. Członek Kierownictwa Ministerstwa może, w uzasadnionym przypadku, wyznaczyć pracownika podległej mu komórki organizacyjnej do pełnienia funkcji pełnomocnika ds. ochrony danych osobowych lub jego zastępcy. Wyznaczenie pełnomocnika oraz jego zastępcy następuje zgodnie z zarządzeniem w sprawie wydawania upoważnień i pełnomocnictw.

4. Dyrektor Generalny Ministerstwa, w imieniu Ministra wykonuje czynności administratora wobec IOD, w szczególności:
1) właściwe i niezwłoczne włączanie IOD we wszystkie sprawy dotyczące ochrony danych osobowych w Ministerstwie , o którym mowa w art. 38 ust. 1 RODO;

2) wspieranie IOD w wypełnianiu jego zadań, zapewnianie mu zasobów niezbędnych do wykonywania jego zadań oraz utrzymania wiedzy fachowej oraz zapewnienie dostępu do danych osobowych i operacji przetwarzania, o którym mowa w art. 38 ust. 2 RODO;
3) wyznaczanie IOD zadań i obowiązków niewynikających z RODO w zakresie niepowodującym konfliktu interesów, o którym mowa w art. 38 ust. 6 RODO;
4) występowanie do IOD o konsultację oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, o której mowa w art. 35 ust. 2 RODO.

§ 15. 1. Do zadań kierujących komórkami organizacyjnymi należy, w zakresie właściwości tych komórek, wykonywanie czynności administratora nie zastrzeżonych do właściwości innych podmiotów, w szczególności:

1) zbieranie, przechowywanie, udostępnianie i usuwanie danych osobowych;
2) zawieranie umów i porozumień dotyczących przetwarzania danych osobowych, w tym umów powierzenia przetwarzania danych osobowych oraz udzielanie dalszych pełnomocnictw do ich zawierania;
3) prowadzenie rejestru umów powierzenia przetwarzania danych osobowych;
4) przeprowadzanie analizy projektowanych czynności przetwarzania danych osobowych w zakresie określonym w § 5, w tym przeprowadzanie analizy ryzyka naruszenia praw lub wolności osób fizycznych oraz DPIA;
5) realizacja obowiązku informacyjnego, o którym mowa w art. 13 i 14 RODO;
6) rozpatrywanie wniosków, o których mowa w art. 15 - 22 RODO w terminie określonym w art. 12 ust. 3 i 4 RODO oraz niezwłoczna realizacja praw osób, których dane dotyczą;
7) zgłaszanie konieczność wprowadzenia zmian w rejestrach prowadzonych przez BPB;
8) współpraca z BPB i IOD przy realizacji ich zadań;
9) informowanie IOD o pracach dotyczących planowania/projektowania/przygotowania przedsięwzięć zarówno o charakterze programowym, legislacyjnym jak i projektowym, jeżeli ich realizacja będzie związana z przetwarzaniem danych osobowych oraz umożliwienie IOD włączenia się w te prace;
10) zapewnienie prawidłowego przetwarzania danych osobowych, z zastrzeżeniem zadań przypisanych DI, BA i BPB.

2. Do zadań kierujących komórkami organizacyjnymi pełniącymi funkcję Instytucji Zarządzających Programami Operacyjnymi oraz kierującego komórką organizacyjną odpowiedzialną za koordynację realizacji Programów Operacyjnych należy realizacja zadań administratora, o których mowa w § 15 ust. 1, a ponadto, opracowanie projektów wewnętrznych aktów normatywnych, wytycznych, zaleceń, wzorów dokumentów oraz standardowych środków organizacyjnych i

technicznych przetwarzania danych osobowych regulujących zasady przetwarzania danych osobowych w Programach Operacyjnych albo w Centralnym Systemie Teleinformatycznym wspierającym realizację Programów Operacyjnych - w zakresie właściwości tych komórek, o ile jest to uzasadnione specyfiką przetwarzania danych osobowych w powyższych obszarach.

3. Z zastrzeżeniem ust. 4, kierujący komórkami organizacyjnymi mogą wyznaczać koordynatorów ds. ochrony danych osobowych i ich zastępców w celu realizacji niektórych lub wszystkich zadań, o których mowa w Polityce. Zakres uprawnień i obowiązków koordynatorów ds. ochrony danych osobowych i ich zastępców określa akt powołania. O wyznaczeniu koordynatora oraz jego zastępcy oraz o zakresie ich działania kierujący komórką organizacyjną informuje niezwłocznie w EZD kierującego BPB oraz IOD.

4. Udzielenie dalszego pełnomocnictwa do zawierania umów i porozumień dotyczących przetwarzania danych osobowych, w tym umów powierzenia przetwarzania danych osobowych następuje zgodnie z zarządzeniem w sprawie wydawania upoważnień i pełnomocnictw.

§ 16. 1. Do zadań kierującego BPB należy realizacja czynności administratora, o których mowa w § 15 ust. 1, a ponadto:

1) wydawanie upoważnień do przetwarzania danych osobowych;
2) prowadzenie rejestru wydanych upoważnień;
3) opiniowanie projektów umów powierzenia przetwarzania danych osobowych;
4) koordynacja procesu przetwarzania danych osobowych w Ministerstwie, w szczególności opracowywanie i udostępnianie w intranecie wzorów dokumentów, standardowych środków organizacyjnych i technicznych przetwarzania danych osobowych oraz metodyki sporządzania analizy ryzyka naruszenia praw lub wolności osób fizycznych i analizy DPIA, a także formułowanie zaleceń i wytycznych - z własnej inicjatywy, na polecenie Dyrektora Generalnego albo IOD;
5) koordynacja realizacji zadań przez pełnomocników ds. ochrony danych osobowych;
6) współpraca z kierującymi komórkami organizacyjnymi przy realizacji czynności, o których mowa w § 5 ust. 1, 3 i 4;

2. Przed udostępnieniem wzorów, wytycznych, zaleceń i metodyk kierujący BPB występuje o opinie kierujących właściwymi komórkami organizacyjnymi oraz IOD.

3. Projekt standardowych środków organizacyjnych i technicznych przetwarzania danych osobowych podlega uzgodnieniu z kierującymi komórkami organizacyjnymi.

4. Stosowanie wytycznych, metodyki oraz standardowych środków organizacyjnych i technicznych przetwarzania danych osobowych jest obowiązkowe. Stosowanie wzorów i zaleceń kierującego BPB jest fakultatywne.

§ 17. Do zadań kierującego BA należy realizacja czynności administratora o których mowa w § 15 ust. 1, a ponadto:

1) zapewnienie w Ministerstwie warunków umożliwiających wdrożenie standardowych środków organizacyjnych i technicznych przetwarzania danych osobowych w formie papierowej;
2) współpraca przy opracowywaniu i wdrażaniu dodatkowych środków organizacyjnych i technicznych przetwarzania danych osobowych w formie papierowej, w przypadku o którym mowa w § 5 ust. 3 i 4.

§ 18. Do zadań kierującego DI należy realizacja czynności administratora o których mowa w §15 ust. 1, a ponadto:

1) zapewnienie w Ministerstwie warunków umożliwiających wdrożenie standardowych środków organizacyjnych i technicznych przetwarzania danych osobowych w systemach teleinformatycznych;
2) współpraca przy opracowywaniu i wdrażaniu dodatkowych środków organizacyjnych i technicznych przetwarzania danych osobowych w systemach teleinformatycznych, w przypadku o którym mowa w § 5 ust. 3 i 4;
3) opracowanie oraz opiniowanie projektów wewnętrznych aktów normatywnych Ministerstwa w zakresie przetwarzania danych osobowych w systemach teleinformatycznych.

§ 19. Do zadań pełnomocnika ds. ochrony danych osobowych w BPB oraz jego zastępców należy:

1) wydawanie upoważnień do przetwarzania danych osobowych oraz udzielanie dalszych pełnomocnictw do wydawania upoważnień;
2) prowadzenie rejestru wydanych upoważnień zgodnie z § 8 ust. 5;
3) opiniowanie projektów umów i porozumień dotyczących przetwarzania danych osobowych, w tym umów powierzenia przetwarzania danych osobowych;
4) współpraca z IOD przy realizacji jego zadań;

- w odniesieniu do kategorii czynności przetwarzania wskazanych w upoważnieniu/pełnomocnictwie wydanym przez właściwego członka Kierownictwa.

§ 20. Do zadań pełnomocnika ds. ochrony danych osobowych w komórce organizacyjnej oraz jego zastępców należy:

1) wydawanie upoważnień do przetwarzania danych osobowych oraz udzielanie dalszych pełnomocnictw do wydawania upoważnień;
2) prowadzenie rejestru wydanych upoważnień zgodnie z § 8 ust. 5;

3) współpraca z kierującym BPB w zakresie koordynacji procesu przetwarzania danych osobowych;
4) współpraca z IOD przy realizacji jego zadań;
5) przeprowadzanie, jeżeli zaistnieje taka konieczność, czynności kontrolnych przestrzegania zasad przetwarzania danych osobowych we właściwych komórkach organizacyjnych oraz czynności kontrolnych w podmiotach, którym zostało powierzone przetwarzanie danych osobowych;

- w odniesieniu do kategorii czynności przetwarzania wskazanych w upoważnieniu/pełnomocnictwie wydanym przez właściwego członka Kierownictwa.

§ 21. 1. W celu zapewnienia przestrzegania przepisów o ochronie danych osobowych w Ministerstwie funkcjonuje IOD powołany przez administratora.

2. IOD wykonuje zadania, o których mowa w art. 39 RODO, tj. w szczególności:
1) opiniuje projekty aktów normatywnych, aktów wewnętrznych, umów i innych dokumentów związanych z ochroną danych osobowych;
2) prowadzi szkolenia, warsztaty oraz udziela porad i konsultacji pracownikom i członkom kierownictwa Ministerstwa w zakresie ochrony danych osobowych;
3) monitoruje przestrzeganie przepisów z zakresu ochrony danych osobowych;
4) zapewnia obsługę adresu email: IOD@miir.gov.pl, w tym koordynuje udzielanie odpowiedzi na zapytania wysyłane na ten adres;
5) koordynuje procedurę rozpatrywania wniosków, o których mowa w art. 15 - 22 RODO skierowanych do Ministerstwa za pośrednictwem adresu e-mail: iod@miir.gov.pl oraz w przypadku, gdy wniosek dotyczy więcej niż jednej komórki organizacyjnej.

3. W trakcie realizacji swoich zadań IOD posiada, w niezbędnym zakresie, dostęp do wszystkich danych osobowych przetwarzanych w Ministerstwie.

4. IOD nie podejmuje działań, które prowadziłyby do przejęcia przez niego obowiązków, odpowiedzialności lub uprawnień administratora.

5. Administrator może powołać zastępcę IOD. Zastępca IOD w czasie nieobecności IOD wykonuje jego zadania.

Rozdział 5

Monitoring przestrzegania przepisów z zakresu ochrony danych osobowych

§ 22. 1. Monitoring przestrzegania przepisów z zakresu ochrony danych osobowych w Ministerstwie obejmuje:

1) sprawdzenia zgodności przetwarzania danych osobowych z prawem powszechnie obowiązującym oraz aktami wewnętrznymi obowiązującymi w Ministerstwie (dalej: „sprawdzenia”);
2) audyty i kontrole realizowane na zasadach określonych w odrębnych przepisach;
3) czynności kontrolne realizowane przez pełnomocników ds. ochrony danych osobowych;
4) sprawowanie nadzoru nad czynnościami przetwarzania danych osobowych;
5) bieżące zgłaszanie użytkownikom i kierującym komórkami organizacyjnymi uwag i propozycji dotyczących ochrony danych osobowych.

2. Sprawdzenia przeprowadza IOD. W uzasadnionych przypadkach sprawdzenia może dokonać zespół pod kierownictwem IOD, którego skład zatwierdza Dyrektor Generalny Ministerstwa.

3. Dokonując sprawdzeń IOD bierze pod uwagę kryteria legalności, skuteczności, efektywności oraz ryzyka.

4. IOD dokumentuje czynności przeprowadzone podczas sprawdzenia, w szczególności poprzez:
1) sporządzanie notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;
2) sporządzanie kopii otrzymanego dokumentu oraz obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;
3) utrwalanie danych z systemu informatycznego służącego do przetwarzania danych lub zabezpieczenia danych osobowych na informatycznym nośniku danych lub dokonaniu wydruku tych danych;
4) sporządzanie kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.

5. IOD zawiadamia kierującego komórką organizacyjną objętą sprawdzeniem o zakresie planowanych czynności w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności.

6. Z przeprowadzonych sprawdzeń sporządzane są sprawozdania w postaci papierowej lub elektronicznej. Sprawozdania, o których mowa w zdaniu poprzednim, przedkładane są Dyrektorowi Generalnemu Ministerstwa do wiadomości, akceptacji lub zatwierdzenia, niezwłocznie po zakończeniu sprawdzenia.

Rozdział 6

Szkolenia

§ 23. 1. Administrator zapewnia szkolenia dla użytkowników w zakresie obowiązujących przepisów, procedur oraz podstawowych zagrożeń związanych z przetwarzaniem danych osobowych.

2. Kierujący BZL w uzgodnieniu z kierującymi BPB, DI, BA oraz IOD określa zakres szkoleń obowiązkowych i fakultatywnych oraz wdraża mechanizmy mające na celu egzekwowanie udziału użytkowników w szkoleniach obowiązkowych.

3. Szkolenia prowadzi IOD, pracownik BPB lub inny podmiot posiadający wiedzę z zakresu ochrony danych osobowych.

Rozdział 7

Przepisy przejściowe

§ 24. 1. Przepisy, o których mowa w § 5, stosuje się odpowiednio do już realizowanych czynności przetwarzania. Analizy, o której mowa w § 5 ust. 1 dokonuje się w terminie 6 miesięcy od dnia wpisania czynności do rejestru czynności przetwarzania lub od dnia wejścia w życie Polityki, w zależności od tego, który z tych terminów jest późniejszy.

2. Właściwość kierującego komórką organizacyjną w odniesieniu do już realizowanych czynności przetwarzania ustala się na podstawie rejestru czynności przetwarzania. W przypadku braku przyporządkowania czynności przetwarzania danej komórce organizacyjnej, właściwym do realizacji zadań, o których mowa w ust. 1, jest kierujący BPB lub kierujący komórką organizacyjną wskazany przez Dyrektora Generalnego Ministerstwa.

§ 25. Do czasu opracowania metodyki, o której mowa w § 5 ust. 1, właściwym do dokonania analizy ryzyka praw lub wolności osób fizycznych oraz wykonywania zadań, o których mowa w § 5 ust. 3 i 4, jest kierujący BPB we współpracy z kierującymi DI i BA oraz kierującymi właściwymi komórkami organizacyjnymi, albo, jeżeli zgłoszą taką potrzebę, kierujący komórką organizacyjną pełniącą funkcję Instytucji Zarządzającej Programem Operacyjnym lub kierujący komórką organizacyjną odpowiedzialną za koordynację realizacji programów operacyjnych - w zakresie danych osobowych przetwarzanych w programach operacyjnych lub w Centralnym Systemie Teleinformatycznym wspierającym realizację Programów Operacyjnych.

§ 26. 1. W uzasadnionych przypadkach dopuszcza się wydawanie upoważnień odnoszących się do zbiorów danych osobowych. W takim przypadku kierujący BPB prowadzi rejestr zbiorów danych osobowych, zawierający co najmniej nazwę zbioru danych, rodzaje danych osobowych przetwarzanych w ramach zbioru oraz kategorie osób, których dane te dotyczą.

2. Upoważnienia/pełnomocnictwa do wykonywania czynności w imieniu administratora udzielone Członkom Kierownictwa Ministerstwa, kierującym komórkami organizacyjnymi oraz pełnomocnikom do spraw ochrony danych osobowych tracą moc w dniu wejścia w życie Polityki.

§ 27. 1. Upoważnienia do przetwarzania danych osobowych udzielone pracownikom, stażystom, wolontariuszom i praktykantom zachowują ważność przez okres 3 miesięcy od dnia wejścia w życie Polityki, w zakresie danych osobowych, których przetwarzanie wymaga imiennego upoważnienia zgodnie z przepisami prawa. W pozostałym zakresie upoważnienia tracą moc w dniu wejścia w życie Polityki.

2. Upoważnienia do przetwarzania danych osobowych wydane innym osobom, niż wymienione w ust. 1, zachowują ważność do czasu nastąpienia zdarzeń, które zgodnie z treścią tych upoważnień powodują ich wygaśnięcie.

Rozdział 8

Postanowienia końcowe

§ 28. 1. Każdy użytkownik, przed rozpoczęciem przetwarzania danych osobowych, obowiązany jest zapoznać się z przepisami, procedurami i zasadami dotyczącymi ochrony danych osobowych, w tym w szczególności z RODO i UODO, a także z obowiązującą w Ministerstwie Polityką, i innymi regulacjami wewnętrznymi dotyczącymi ochrony danych osobowych. Wykaz tych regulacji kierujący BPB publikuje w Intranecie.

2. Użytkownicy, w terminie 14 dni od dnia wejścia w życie Polityki lub nawiązania stosunku prawnego zobowiązującego ich do stosowania Polityki, potwierdzają zapoznanie się z Polityką na piśmie lub w innej formie, która w sposób jednoznaczny zapewni potwierdzenie tego faktu w zakresie spełnienia zasady rozliczalności. Kierujący BPB może określić i doprecyzować formy zapoznania się z Polityką.

Załącznik nr 1 do Polityki

Rejestr umów powierzenia przetwarzania danych osobowych oraz porozumień w sprawie współadministrowania w … (nazwa KO).

Sekcja	L.p.	Nazwa czynności przetwarzania/zbiór danych osobowych	Nazwa podmiotu, z którym zawarto umowę/porozumienie, adres jego siedziby lub miejsce zamieszkania	Data zawarcia umowy/ porozumienia	Data wygaśnięcia umowy/ porozumienia	Data uzyskania opinii BPB/IOD dot. projektu umowy/ porozumienia [1]	Uwagi
Powierzenie przetwarzania							
Współadministrowanie							

[1] Jeżeli umowa była opiniowana przez BPB/IOD

Załącznik nr 2 do Polityki

Rejestr czynności przetwarzania danych osobowych[2]

LP.	Nazwa czynności przetwarzania	Wiodąca Jednostka organizacyjna (departament, itp.)	Cel przetwarzania	Kategorie osób	Kategorie danych	Podstawa prawna	Źródło danych	Planowany termin usunięcia kategorii danych *(jeżeli jest to możliwe)*	Nazwa współadministratora i dane kontaktowe *(jeśli dotyczy)*	Nazwa podmiotu przetwarzajacego i dane kontakowe *(jeśli dotyczy)*	Kategorie odbiorców *(innych niż podmiot przetwarzajacy)*	Nazwa systemu lub oprogramowania	Ogólny opis technicznych i organizacyjnych srodków bezpieczeństwa zgodnie z art. 32 ust. 1 ***(jeżeli jest to możliwe)***	DPIA (jeśli tak, lokalizacja raportu)	Transfer do kraju trzeciego lub org. międzynarodowej	
															Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń
			Art. 30 ust. 1 pkt b	Art. 30 ust. 1 pkt c	Art. 30 ust. 1 pkt c			Art. 30 ust. 1 pkt f	Art. 30 ust. 1 pkt a	Art. 30 ust. 1 pkt d	Art. 30 ust. 1 pkt d		Art. 30 ust. 1 pkt g		Art. 30 ust. 1 pkt e	Art. 30 ust. 1 pkt e

[2] - artykuły wskazane w tabeli odnoszą się do Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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, z późn. zm.)

Załącznik nr 3 do Polityki

Rejestr kategorii czynności przetwarzania danych osobowych[3]

LP.	Kategorie przetwarzań	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	Administrator				Czas trwania przetwarzania	Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi	Podprzetwarzający (podwykonawca) - jeśli dotyczy	
			Nazwa i dane kontaktowe administratora	Nazwa i dane kontaktowe współadministratora (jeśli dotyczy)	Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono)	Inspektor ochrony danych administratora (jeśli powołano)				Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy)	Kategorie podpowierzonych przetwarzań
	Art. 30 ust. 2 lit. b	Art. 30 ust. 2 lit. d, art. 32 ust. 1	Art. 30 ust. 2 lit. a					Art. 30 ust. 2 lit. c	Art. 30 ust. 2 lit. c		

[3] - artykuły wskazane w tabeli odnoszą się do Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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, z późn. zm.)

MINISTER

FINANSÓW, INWESTYCJI I ROZWOJU

Załącznik nr 4a do Polityki

Warszawa, dnia…….

UPOWAŻNIENIE

Na podstawie § 8 ust. 2 pkt 1 zarządzenia Ministra Finansów, Inwestycji i Rozwoju w sprawie Polityki Ochrony Danych Osobowych oraz art. 29 RODO* upoważniam:

Panią/Pana: ……
(imię i nazwisko)

do przetwarzania danych osobowych w zakresie:

- (nazwa czynności przetwarzania lub nazwa zbioru danych)

- ……..

- ……..

w ramach zakresu zadań realizowanych w ……..……
(nazwa departamentu, biura lub innego podmiotu)

na stanowisku pracy, na którym dane osobowe są przetwarzane/**wynikających z ……

Niniejsze upoważnienie wygasa z dniem…../ z chwilą ustania zatrudnienia Pani / Pana w Departamencie/Biurze w Ministerstwie Inwestycji i Rozwoju/ zmiany zakresu obowiązków powodującej zaprzestanie przetwarzania danych osobowych w ww. zbiorze/-ach danych/* zaprzestania wykonywania zadań w ramach ……

(pieczątka i podpis osoby upoważnionej do wydania upoważnienia)

Oświadczam, że zapoznałem się z przepisami dotyczącymi ochrony danych osobowych, w tym z RODO*, Polityką Bezpieczeństwa Informacji, Polityką Ochrony Danych Osobowych, *Regulaminem bezpieczeństwa informacji przetwarzanych w aplikacji głównej centralnego systemu teleinformatycznego**** 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 się, zarówno w okresie realizacji ww. zadań, jak też po ich zakończeniu.

Oświadczam, że odbyłem obowiązkowe szkolenie z zakresu ochrony danych osobowych/**zapoznałem się z przekazanymi mi informacjami dotyczącymi zasad przetwarzania danych osobowych.

……
(czytelny podpis osoby upoważnionej)

Upoważnienie otrzymałem/otrzymałam

……
(miejscowość, data, czytelny podpis)

* RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 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, z późn. zm.)

** niepotrzebne skreślić

*** należy wskazać właściwy regulamin

Załącznik nr 4b do Polityki

.....
Nagłówek zgodny z wzorem papieru firmowego

Warszawa, dnia…….

UPOWAŻNIENIE

Na podstawie § 8 ust. 2 pkt 1 w zw. z § 16/17/18** zarządzenia Ministra Finansów, Inwestycji i Rozwoju w sprawie Polityki Ochrony Danych Osobowych oraz art. 29 RODO* upoważniam:

Panią/Pana: ……
(imię i nazwisko)

do przetwarzania danych osobowych w zakresie:

- (nazwa czynności przetwarzania lub nazwa zbioru danych)

- ……..

- ……..

w ramach zakresu zadań realizowanych w ……..……
(nazwa departamentu, biura lub innego podmiotu)

na stanowisku pracy, na którym dane osobowe są przetwarzane/**wynikających z …….

Niniejsze upoważnienie zobowiązuje Panią / Pana do:

1) zapoznania się z przepisami dotyczącymi ochrony danych osobowych, w tym z RODO*, Polityką Bezpieczeństwa Informacji, Polityką Ochrony Danych Osobowych, *Regulaminem bezpieczeństwa informacji przetwarzanych w aplikacji głównej centralnego systemu teleinformatycznego**** i przestrzegania zasad przetwarzania danych osobowych określonych w tych dokumentach;
2) zachowania w tajemnicy przetwarzanych danych osobowych, z którymi Pani / Pan się zapozna oraz sposobów ich zabezpieczania, zarówno w okresie realizacji ww. zadań, jak też po ich zakończeniu.

Niniejsze upoważnienie wygasa z chwilą ……

Z upoważnienia Administratora

……
(czytelny podpis)

Upoważnienie otrzymałam / otrzymałem

……
(miejscowość, data, czytelny podpis)

* RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 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, z późn. zm.)

** niepotrzebne skreślić

*** W uzasadnionych przypadkach należy wskazać inny, właściwy regulamin

Załącznik nr 4c do Polityki

Użytkownik – Instytucja Zarządzająca

.....
Nagłówek zgodny z wzorem papieru firmowego

UPOWAŻNIENIE

Działając na podstawie pełnomocnictwa udzielonego mi przez Ministra Finansów, Inwestycji i Rozwoju, na podstawie art. 29 RODO*, upoważniam Panią/Pana

[Imię i Nazwisko]

do przetwarzania danych osobowych oraz wydawania/odwoływania upoważnień do przetwarzania danych osobowych osobom wskazanym przez beneficjentów we wnioskach o nadanie uprawnień w zakresie zbioru:

Centralny system teleinformatyczny wspierający realizację programów operacyjnych

Pana/i identyfikator użytkownika w systemie: [login]

Niniejsze upoważnienie zobowiązuje Panią / Pana do:

- *zapoznania się z przepisami dotyczącymi ochrony danych osobowych, w tym z RODO, Polityką Ochrony Danych Osobowych w Ministerstwie Inwestycji i Rozwoju oraz Regulaminem bezpieczeństwa informacji przetwarzanych w aplikacji SL2014-PT centralnego systemu teleinformatycznego i przestrzegania zasad przetwarzania danych osobowych określonych w tych dokumentach;*
- *zachowania w tajemnicy przetwarzanych danych osobowych, z którymi Pani / Pan się zapozna oraz sposobów ich zabezpieczania, zarówno w okresie świadczenia pracy, jak też po zakończeniu świadczenia pracy w [Instytucja].*

Niniejsze upoważnienie wygasa z chwilą wycofania dostępu do centralnego systemu teleinformatycznego – aplikacja SL2014-PT.

z upoważnienia Administratora

[imię i nazwisko osoby zakładającej konto użytkownika]

Warszawa, [data]

* *- RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 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, z późn. zm.)*

Załącznik nr 4d do Polityki

Użytkownik – Instytucja Pośrednicząca:

.....
Nagłówek zgodny z wzorem papieru firmowego

UPOWAŻNIENIE

Działając na podstawie pełnomocnictwa udzielonego mi przez Ministra Finansów, Inwestycji i Rozwoju, na podstawie art. 29 RODO*, upoważniam Panią/Pana

[Imię i Nazwisko]

do przetwarzania danych osobowych w zakresie zbioru:

Centralny system teleinformatyczny wspierający realizację programów operacyjnych

Pana/i identyfikator użytkownika w systemie: [login]

Niniejsze upoważnienie zobowiązuje Panią / Pana do:

- *zapoznania się z przepisami dotyczącymi ochrony danych osobowych, w tym RODO*, Polityką Ochrony Danych Osobowych w Ministerstwie Inwestycji i Rozwoju oraz Regulaminem bezpieczeństwa informacji przetwarzanych w aplikacji SL2014-PT centralnego systemu teleinformatycznego i przestrzegania zasad przetwarzania danych osobowych określonych w tych dokumentach;*
- *zachowania w tajemnicy przetwarzanych danych osobowych, z którymi Pani / Pan się zapozna oraz sposobów ich zabezpieczania, zarówno w okresie świadczenia pracy, jak też po zakończeniu świadczenia pracy w [Instytucja].*

Niniejsze upoważnienie wygasa z chwilą wycofania dostępu do centralnego systemu teleinformatycznego – aplikacja SL2014-PT.

z upoważnienia Administratora

[imię i nazwisko osoby zakładającej konto użytkownika]

Warszawa, [data]

* *- RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 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, z późn. zm.)*

Załącznik nr 4e do Polityki

Użytkownik – Beneficjent *(osoba fizyczna wskazana przez beneficjenta we wniosku o nadanie uprawnień)*

.....
Nagłówek zgodny z wzorem papieru firmowego

UPOWAŻNIENIE

Działając na podstawie pełnomocnictwa udzielonego mi przez Ministra Finansów, Inwestycji i Rozwoju, na podstawie art. 29 RODO, upoważniam Panią/Pana*

[Imię i Nazwisko]

do przetwarzania danych osobowych w zakresie zbioru:

Centralny system teleinformatyczny wspierający realizację programów operacyjnych

w ramach projektów realizowanych przez *[Nazwa beneficjenta].*

Pana/i identyfikator użytkownika w systemie: (login w aplikacji): [login]

Niniejsze upoważnienie zobowiązuje Panią / Pana do:

- *zapoznania się z przepisami dotyczącymi ochrony danych osobowych, w tym z RODO, Polityką Ochrony Danych Osobowych w Ministerstwie Inwestycji i Rozwoju oraz Regulaminem bezpieczeństwa informacji przetwarzanych w aplikacji SL2014-PT centralnego systemu teleinformatycznego i przestrzegania zasad przetwarzania danych osobowych określonych w tych dokumentach;*
- *zachowania w tajemnicy przetwarzanych danych osobowych, z którymi Pani / Pan się zapozna oraz sposobów ich zabezpieczania, zarówno w okresie świadczenia pracy, jak też po zakończeniu świadczenia pracy dla [Nazwa beneficjenta].*

Niniejsze upoważnienie wygasa z chwilą wycofania dostępu do SL2014-PT.z upoważnienia Administratora

[imię i nazwisko osoby zakładającej konto użytkownika]

Warszawa, [data]

* *- RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 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, z późn. zm.)*

Załącznik nr 5 do Polityki

Warszawa, dnia…….

Wniosek o wydanie upoważnienia

Wnoszę o wydanie upoważnienia do przetwarzania danych osobowych dla użytkownika: ……
(imię i nazwisko)

do przetwarzania danych osobowych w zakresie:

- (nazwa czynności przetwarzania lub nazwa zbioru danych)

- ……..

- ……..

w ramach zakresu zadań realizowanych w ……,
(nazwa departamentu, biura lub innego podmiotu)

na podstawie ……
(rodzaj umowy lub innego stosunku prawnego uzasadniającego wydanie upoważnienia)

……
(imię i nazwisko kierującego komórką organizacyjną lub koordynatora ds. ochrony danych osobowych w komórce)

W związku ze złożeniem wniosku o wydanie upoważnienia do przetwarzania danych osobowych oświadczam, że:

1) zapoznałem/łam się z przepisami dotyczącymi ochrony danych osobowych, w tym z RODO*, Polityką Bezpieczeństwa Informacji, Polityką Ochrony Danych Osobowych, *Regulaminem bezpieczeństwa informacji przetwarzanych w aplikacji głównej centralnego systemu teleinformatycznego**** i przestrzegania zasad przetwarzania danych osobowych określonych w tych dokumentach;
2) odbyłem/łam obowiązkowe szkolenia wskazane przez kierującego BPB
3) zachowam w tajemnicy informacje o przetwarzanych danych osobowych oraz sposobach ich zabezpieczania, zarówno w okresie realizacji ww. zadań, jak też po ich zakończeniu.

……
(imię i nazwisko osoby, której wydane ma być upoważnienie)

Pouczenie:

Upoważnienie wydane w imieniu Ministra traci moc z dniem ustania stosunku prawnego wskazanego we wniosku na podstawie którego użytkownik wykonuje czynności w Departamencie/Biurze w Ministerstwie Inwestycji i Rozwoju lub zmiany zakresu obowiązków powodującej zaprzestanie przetwarzania danych osobowych w ramach ww. czynności przetwarzania.

* RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 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, z późn. zm.)

** niepotrzebne skreślić

*** należy wskazać właściwy regulamin

Załącznik nr 6 do Polityki

Rejestr upoważnień do przetwarzania danych osobowych

Nazwa komórki organizacyjnej prowadzącej rejestr					
LP.	**Imię i Nazwisko upoważnionego/ nazwa grupy upoważnionych**	**Nazwa komórki organizacyjnej lub innego podmiotu**	**Data wydania upoważnienia**	**Data wygaśnięcia upoważnienia**	**Nazwa czynności przetwarzania/zbioru danych opsobowych**