POLITYKA OCHRONY DANYCH OSOBOWYCH

MINISTERSTWA RODZINY
I POLITYKI SPOŁECZNEJ

Warszawa, 2021 r.

ROZDZIAŁ I

Podstawowe pojęcia

1) **Administrator** – Minister Rodziny i Polityki Społecznej, który decyduje o celach i sposobach przetwarzania danych osobowych;
2) **BA** – Biuro Administracyjne;
3) **BKA** – Biuro Kontroli i Audytu w Ministerstwie;
4) **dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
5) **dane osobowe szczególne** – dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej danej osoby;
6) **DI** – Departament Informatyki;
7) **Inspektor Ochrony Danych (IOD)** – pracownik Ministerstwa, który realizuje zadania określone w art. 39 RODO oraz inne zadania i obowiązki, jeżeli nie powodują konfliktu interesów;
8) **kierujący komórka organizacyjną** – dyrektor komórki organizacyjnej lub osoba pełniąca jego obowiązki;
9) **komórka organizacyjna** – departament lub biuro;
10) **Minister** – Minister Rodziny i Polityki Społecznej;
11) **Ministerstwo** – Ministerstwo Rodziny i Polityki Społecznej;
12) **odbiorca** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, którym ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państwa członkowskiego, nie są uznawane za odbiorców;
13) **ograniczenie przetwarzania** – oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
14) **organizacja międzynarodowa** – organizacja i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy;
15) **państwo trzecie** – państwo niebędące członkiem Unii Europejskiej oraz nienależące do Europejskiego Obszaru Gospodarczego (EOG);
16) **podmiot przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
17) **PUODO**- Prezes Urzędu Ochrony Danych Osobowych, organ nadzorczy;
18) **Polityka** – Polityka ochrony danych osobowych;
19) **RODO** – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);

20) **strona trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które z upoważnienia administratora lub podmiotu przetwarzającego mogą przetwarzać dane osobowe;

21) **UODO** – Urząd Ochrony Danych Osobowych, obsługujący organ nadzorczy PUODO;

22) **ustawa o ochronie danych osobowych** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781);

23) **użytkownik** – Minister, sekretarz i podsekretarz stanu, Dyrektor Generalny, szef gabinetu politycznego, kierujący komórką organizacyjną Ministerstwa, pracownik Ministerstwa, stażysta, praktykant lub wolontariusz;

24) **współadministrator –** jeden z co najmniej dwóch administratorów wspólnie ustalających cele i sposoby przetwarzania, o którym mowa w art. 26 RODO;

25) **zgoda** – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

ROZDZIAŁ II

Postanowienia ogólne

§ 1.

1. Polityka określa zasady przetwarzania danych osobowych, dla których Minister jest administratorem.
2. Politykę stosuje się do danych osobowych przetwarzanych:
   1) w systemie Elektronicznego Obiegu Dokumentów eDok, innych systemach teleinformatycznych, poczcie elektronicznej, dyskach komputerów, dyskach sieciowych, pendrive'ach, telefonach oraz drukarkach i urządzeniach centralnych;
   2) w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych Ministerstwa, stanowiących zbiory danych w rozumieniu 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.

§ 2.

Polityka ma na celu zapewnienie ochrony praw i wolności 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) przetwarzane przez osoby upoważnione;
5) chronione przed niedozwolonym lub niezgodnym z prawem przetwarzaniem;
6) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

§ 3.

Polityka ma zastosowanie do przetwarzania danych osobowych w Ministerstwie, w szczególności w związku z realizacją:

1) zadań wynikających z przepisów prawa krajowego oraz Unii Europejskiej i określonych szczegółowo w Regulaminie organizacyjnym Ministerstwa;
2) obowiązków pracodawcy w rozumieniu Kodeksu pracy;
3) umów o organizację staży, praktyk, wolontariatu;
4) innych zadań niezbędnych do zapewnienia funkcjonowania Ministerstwa.

ROZDZIAŁ III

Ogólne zasady przetwarzania danych osobowych

§ 4.

1. Przetwarzanie danych osobowych oznacza każdą operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, w tym:

1) zbieranie;
2) utrwalanie;
3) organizowanie;
4) porządkowanie;
5) przechowywanie;
6) adaptowanie lub modyfikowanie;
7) pobieranie;
8) przeglądanie;
9) wykorzystywanie;
10) ujawnianie przez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie;
11) dopasowywanie lub łączenie;
12) ograniczanie;
13) usuwanie lub niszczenie.

2. Zbieranie danych osobowych to każde wejście w posiadanie danych osobowych z zamiarem ich dalszego przetwarzania, niezależnie od tego, kto to inicjuje (administrator czy osoba, której dane dotyczą).
3. Utrwalanie to wszelkie formy i postaci zarejestrowania (zapisania) informacji na materialnym nośniku – informacja utrwalona, co do zasady, powinna się nadawać do dalszego przetwarzania zgodnie z celem, w jakim ją zebrano.
4. Organizowanie danych to operacje polegające na nadaniu określonej struktury zbiorowi lub zestawowi, w jakich dane są przetwarzane, lub zmianie jego dotychczasowej struktury.
5. Porządkowanie to operacja, która ma poprawić funkcjonalność użytkowania danych, w szczególności przez wprowadzenie jakichkolwiek innych niż dotychczasowe kryteriów wyszukiwania dostępu do określonych kategorii informacji.
6. Przechowanie (archiwizowanie) jest związane z uprzednim utrwaleniem danych osobowych na nośniku materialnym z możliwością ich odtworzenia w późniejszym czasie.
7. Adaptowanie lub modyfikowanie danych osobowych to uzyskanie nowej wiedzy na temat osoby, której dane są przetwarzane. Adaptowanie danych osobowych jest zmianą wynikającą ze skorzystania przez osobę, której dane są przetwarzane, z przysługujących jej praw, w szczególności: ograniczenia przetwarzania,

usunięcia części danych. Modyfikowanie danych związane jest z ingerencją osoby, której dane dotyczą, tj. sprostowania danych.

8. Pobieranie danych osobowych to operacja związana z wykonywaniem kopii danych osobowych lub ich części, pozyskanych za pośrednictwem sieci telekomunikacyjnej lub innego kanału przekazywania informacji.
9. Przeglądanie danych to wyszukiwanie danych przez używanie odpowiednich haseł, które dzięki zastosowanemu mechanizmowi indeksującemu pozwalają na zapoznanie się z konkretnymi danymi.
10. Wykorzystywanie danych to działanie zmierzające do osiągnięcia konkretnego celu.
11. Ujawnianie przez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie to operacje, które prowadzą do zapoznania się z danymi przez odbiorców za zgodą administratora.
12. Dopasowywanie lub łączenie danych osobowych to aktywne działanie podjęte przez administratora w celu weryfikacji poprawności danych, uzyskanie dodatkowych informacji wynikających ze skali przetwarzania czy usprawnienie procesów przetwarzania.
13. Ograniczenie to każda forma zawężenia możliwości przetwarzania zarówno zakresu przetwarzanych informacji, jak i celów dla jakich są one wykorzystywane.
14. Usuwanie lub niszczenie to trwałe kasowanie danych.

§ 5.

Administrator przetwarza dane osobowe zgodnie z zasadami:

1) legalności – przetwarzanie danych powinno odbywać się zgodnie z prawem, na podstawie co najmniej jednej z przesłanek przetwarzania danych osobowych, o których mowa w art. 6 i art. 9 RODO;
2) rzetelności – dane powinny być przetwarzane z uwzględnieniem interesów i uzasadnionych oczekiwań osób, których dane dotyczą;
3) przejrzystości – osoba, której dane dotyczą powinna być poinformowana w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem o istotnych dla niej aspektach przetwarzania jej danych;
4) ograniczenia celu – dane powinny być przetwarzane w konkretnych, wyraźnych i prawnie uzasadnionych celach;
5) minimalizacji danych – administrator powinien przetwarzać tylko te dane, które są niezbędne do osiągnięcia celu przetwarzania;
6) prawidłowości danych – administrator powinien przetwarzać prawidłowe dane osobowe i uaktualniać je w razie potrzeby;
7) ograniczenia przechowywania – administrator powinien przechowywać dane osobowe w dokumentacji tworzącej akta spraw przez okres wynikający z Jednolitego Rzeczowego Wykazu Akt, uzgodnionego w trybie ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2020 r. poz. 164), z właściwym archiwum państwowym;
8) integralności i poufności – administrator do przetwarzania danych osobowych powinien dopuścić jedynie osoby upoważnione oraz zastosować takie środki techniczne i organizacyjne, by dane były chronione przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem;
9) ochrony danych osobowych w fazie projektowania – ochrona prywatności powinna być realizowana na etapie projektowanych działań skutkujących przetwarzaniem danych osobowych;
10) domyślnej ochrony danych osobowych – domyślne ustawienia przetwarzania danych osobowych powinny umożliwić przetwarzanie jedynie danych niezbędnych do osiągnięcia konkretnego celu przetwarzania. Jednocześnie ustawienia systemów przetwarzania danych nie powinny umożliwiać udostępnienia danych nieokreślonej liczbie osób fizycznych bez interwencji osoby, której dane dotyczą.

ROZDZIAŁ IV

Wydawanie upoważnień do przetwarzania danych osobowych

§ 6.

1. W Ministerstwie przetwarzanie danych osobowych odbywa się na podstawie imiennych upoważnień do przetwarzania danych osobowych, wydawanych użytkownikom.
2. Sposób wydawania upoważnień do przetwarzania danych osobowych jest określony w załączniku nr 2 do zarządzenia.
3. Wydanie imiennego upoważnienia następuje przez:
   1) podpisanie, w tym za pomocą podpisu elektronicznego, dokumentu upoważniającego do przetwarzania danych osobowych, sporządzonego zgodnie ze wzorem zawartym w załączniku nr 2 do zarządzenia lub
   2) zatwierdzenie, w tym za pomocą podpisu elektronicznego, wniosku o wydanie upoważnienia, zawartego w załączniku nr 2 do zarządzenia.
4. Dyrektor BKA oraz kierujący komórkami organizacyjnymi prowadzą rejestry wydanych imiennych upoważnień, których zakres jest określony w załączniku nr 2 do zarządzenia.
5. Użytkownik jest obowiązany do:
   1) zapoznania się z Polityką oraz obowiązującymi przepisami prawa dotyczącymi ochrony danych osobowych;
   2) potwierdzenia faktu zapoznania się z treścią i zakresem upoważnienia lub odpowiednio – zatwierdzonego wniosku, o których mowa w ust. 3 i oświadczenia o zachowaniu poufności za pośrednictwem elektronicznego obiegu dokumentów eDok. W przypadku braku dostępu do systemu eDok – za pośrednictwem poczty elektronicznej na adres sekretariatu BKA lub w postaci papierowej.

ROZDZIAŁ V

Rejestr czynności przetwarzania danych oraz rejestr kategorii czynności przetwarzania danych

§ 7.

1. W Ministerstwie prowadzi się rejestr czynności przetwarzania danych oraz rejestr kategorii czynności przetwarzania danych. Rejestry mogą być udostępniane w intranecie, o którym mowa w załączniku nr 1 do zarządzenia nr 1 Dyrektora Generalnego Ministerstwa Rodziny, Pracy i Polityki Społecznej z dnia 9 stycznia 2020 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w obszarze IT Ministerstwa Rodziny, Pracy i Polityki Społecznej (PBI).
2. Sposób tworzenia rejestru czynności przetwarzania danych oraz rejestru kategorii czynności przetwarzania danych jest określony w załączniku nr 3 do zarządzenia.
3. Zmiany w rejestrach zatwierdza i publikuje IOD.
4. IOD we współpracy z kierującymi komórkami organizacyjnymi dokonuje przeglądu rejestrów wymienionych w ust. 1 nie rzadziej niż dwa razy w roku oraz w przypadku wprowadzenia istotnych zmian organizacyjnych w Ministerstwie.

ROZDZIAŁ VI

Umowy lub porozumienia w sprawie powierzenia przetwarzania danych osobowych

§ 8.

1. Minister realizując swoje zadania skutkujące przetwarzaniem danych osobowych może być:
   1) podmiotem, który zleca przetwarzanie danych w swoim imieniu innemu podmiotowi;

2) podmiotem, który na zlecenie i w imieniu innego podmiotu przetwarza dane osobowe (podmiot przetwarzający).

2. Kierujący komórką organizacyjną, realizując zadania skutkujące powierzeniem przetwarzania danych osobowych innemu podmiotowi, odpowiada za wybór podmiotu przetwarzającego, który zapewni wystarczającą gwarancję wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie chroniło prawa osób, których dane dotyczą.

3. Kierujący komórką organizacyjną, który na zlecenie innego podmiotu i w jego imieniu przyjmuje przetwarzanie danych, odpowiada za realizację obowiązków wynikających z umowy powierzenia.

4. Kierujący komórkami organizacyjnymi prowadzą rejestry zawartych umów powierzenia przetwarzania danych. Komórka organizacyjna udostępnia IOD aktualny rejestr umów powierzenia przetwarzania oraz porozumień w sprawie współadministrowania – w sposób wskazany przez IOD.

5. 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.

6. Dane dotyczące umowy lub porozumienia w sprawie przetwarzania danych osobowych (data zawarcia, podmiot, zakres i cel) zawarte są w rejestrze cząstkowym prowadzonym przez komórkę organizacyjną i w rejestrze czynności prowadzonym w Ministerstwie.

7. Kategorie czynności, które zostały administratorowi powierzone do przetwarzania, zawarte są w rejestrze kategorii czynności prowadzonym w komórce organizacyjnej i w rejestrze kategorii czynności prowadzonym w Ministerstwie.

8. Szczegółowy sposób postępowania w zakresie wskazanym w ust. 1–5 jest określony w załączniku nr 4 do zarządzenia.

ROZDZIAŁ VII

Prawa osób, których dane są przetwarzane w Ministerstwie niewymagające złożenia wniosku oraz sposób ich realizacji

§ 9.

1. Każda osoba, której dane osobowe są przetwarzane w Ministerstwie, ma prawo do informacji o fakcie i zakresie przetwarzania tych danych. Ministerstwo realizuje to prawo wykonując obowiązek informacyjny.

2. Zakres danych przekazywanych w ramach realizacji obowiązku informacyjnego, wskazanego w ust. 1, zależy od sposobu pozyskania danych osobowych.

§ 10.

1. W przypadku zbierania danych od osoby, której dane dotyczą, Administrator w momencie pozyskiwania danych, w celu dalszego ich przetwarzania, przekazuje w szczególności następujące informacje:

   1) tożsamość administratora danych;

   2) cele przetwarzania danych;

   3) prawa przysługujące osobie, której dane są przetwarzane.

2. Wzór minimalnego zakresu danych ujętych w klauzuli informacyjnej w przypadku zbierania danych od osoby, której dane dotyczą, określa załącznik nr 5 do zarządzenia.

§ 11.

1. W przypadku zbierania danych w sposób inny niż od osoby, której dane dotyczą, Administrator przekazuje w szczególności następujące informacje:

   1) tożsamość administratora danych;

2) cele przetwarzania danych;

3) prawa przysługujące osobie, której dane są przetwarzane;

4) źródło pozyskania danych.

2. Informacje, o których mowa w ust. 1, Administrator podaje w terminie, o którym mowa w art. 14 ust. 3 RODO.

3. Wzór minimalnego zakresu danych ujętych w klauzuli informacyjnej w przypadku zbierania danych w sposób inny niż od osoby, której dane dotyczą, określa załącznik nr 6 do zarządzenia.

4. Postanowień ust. 1–3 nie stosuje się w sytuacjach określonych w art. 14 ust. 5 RODO.

§ 12.

1. Za realizację obowiązku informacyjnego, o którym mowa w § 10 i § 11, odpowiada kierujący komórką organizacyjną, w której dane osobowe będą przetwarzane.

2. Realizacja obowiązku informacyjnego następuje pisemnie, w postaci papierowej lub elektronicznej, przez zamieszczenie informacji na tablicy informacyjnej w miejscu ogólnodostępnym, a w szczególnych przypadkach przez odczytanie.

3. W przypadku właściwości kilku komórek organizacyjnych, obowiązek informacyjny realizuje komórka udzielająca zbiorczej odpowiedzi.

ROZDZIAŁ VIII
Prawa osób, których dane są przetwarzane w Ministerstwie, wymagające złożenia wniosku

§ 13.

1. Osobie, której dane są przetwarzane, przysługuje prawo:

1) dostępu do danych przetwarzanych w Ministerstwie oraz uzyskania potwierdzenia, czy Ministerstwo przetwarza jej dane;

2) sprostowania dotyczących jej danych osobowych;

3) do usunięcia danych (prawo do bycia zapomnianym);

4) do ograniczenia przetwarzania danych;

5) do sprzeciwu wobec przetwarzania danych osobowych.

2. Realizacja praw, o których mowa w ust. 1, odbywa się na podstawie pisemnego wniosku osoby, której dane dotyczą.

3. Sposób realizacji praw osoby, której dane dotyczą, wymagających złożenia wniosku jest określony w załączniku nr 7 do zarządzenia.

ROZDZIAŁ IX
Przetwarzanie danych osobowych na podstawie zgody osoby, której dane są przetwarzane w Ministerstwie

§ 14.

1. W szczególnych przypadkach przewidzianych prawem lub w sytuacjach, gdy przetwarzanie jest wymagane dla prawidłowej realizacji zadania, a nie mają zastosowania inne przesłanki określone w art. 6 i art. 9 RODO, przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą.

2. W celu realizacji zasady rozliczalności zgoda powinna być udokumentowana w formie pisemnej.

3. Jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy również innych kwestii, oświadczenie zgody musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii.

4. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

5. Ramowy wzór treści zgody jest określony w załączniku nr 8 do zarządzenia.

6. Kierujący komórką organizacyjną, w ramach której jest realizowane zadanie, z którym wiąże się wyrażenie zgody, prowadzi rejestr zgód, którego zakres jest określony w załączniku nr 8 do zarządzenia. Możliwy jest inny sposób gromadzenia danych o pozyskanych zgodach, o ile umożliwia on identyfikację osoby, która zgody udzieliła oraz czasu i celu, w jakim zgoda była udzielona.

ROZDZIAŁ X
Przekazanie danych osobowych do państw trzecich

§ 15.

1. Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych może odbywać się jedynie zgodnie z zasadami wskazanymi w rozdziale V RODO.

2. Kierujący komórką organizacyjną jest obowiązany zweryfikować istnienie podstawy prawnej uprawniającej do przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej przed dokonaniem przekazania.

3. Przekazanie danych osobowych odbywa się tylko w formie pisemnej.

4. Kierujący komórką organizacyjną, w ramach której następuje przekazanie, prowadzi rejestr zdarzeń, wskazując okoliczności i podstawę przekazania. Możliwy jest inny sposób gromadzenia danych o przekazanych danych osobowych, o ile umożliwia on identyfikację osoby, której dane zostały przekazane, państwa lub organizacji, do której dane zostały przekazane, oraz daty i podstawy przekazania.

5. Przepisów ust. 3–4 nie stosuje się, jeśli sposób przekazywania danych osobowych do państw trzecich jest odrębnie uregulowany w przepisach powszechnie obowiązującego prawa.

ROZDZIAŁ XI
Naruszenia ochrony danych osobowych

§ 16.

1. Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem:

   1) zniszczenia lub

   2) utracenia, lub

   3) zmodyfikowania, lub

   4) nieuprawnionego ujawnienia, lub

   5) nieuprawnionego dostępu.

2. Pracownicy Ministerstwa są obowiązani zgłaszać każde zdarzenie zagrażające bezpieczeństwu danych osobowych, a ustalenie, czy stanowi ono naruszenie ochrony danych osobowych, należy do IOD.

3. Sposób postępowania w przypadku naruszenia ochrony danych osobowych, w szczególności ich zgłaszanie i dokumentowanie, określa załącznik nr 9 do zarządzenia.

4. Zasady zgłaszania naruszeń ochrony danych osobowych do organu nadzorczego i postępowania z nimi regulują odrębne przepisy.

ROZDZIAŁ XII
Przeprowadzenie oceny skutków dla ochrony danych osobowych

§ 17.

1. Ocenę skutków dla ochrony danych osobowych planowanych procesów przetwarzania przeprowadza się, 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 i wolności osób fizycznych.
2. Ocena skutków dla ochrony danych osobowych przeprowadzana jest przez komórkę organizacyjną Ministerstwa, w której będzie odbywało się lub odbywa się przetwarzanie danych osobowych wymagające przeprowadzenia oceny skutków dla ochrony danych osobowych.
3. Komórka organizacyjna realizująca proces wskazany w ust. 1 jest obowiązana skonsultować z IOD w szczególności kwestie dotyczące:
   1) faktu, czy należy przeprowadzić ocenę skutków dla ochrony danych osobowych;
   2) metodologii przeprowadzenia oceny skutków dla ochrony danych osobowych;
   3) zabezpieczeń (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń naruszenia praw i wolności osób, których dane dotyczą;
   4) prawidłowości przeprowadzonej oceny skutków dla ochrony danych osobowych i zgodności jej wyników z RODO (czy należy kontynuować przetwarzanie, czy też nie, oraz jakie zabezpieczenia należy stosować).
4. Za przeprowadzenie oceny skutków dla ochrony danych osobowych odpowiedzialny jest kierujący komórką organizacyjną, w której właściwości pozostaje proces.

§ 18.

1. Ocena skutków dla ochrony danych osobowych zawiera co najmniej następujące elementy:
   1) opis planowanych operacji przetwarzania i celów przetwarzania, w tym gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez Ministerstwo;
   2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
   3) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
   4) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.
2. W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z procesu przetwarzania, kierujący komórką organizacyjną, który odpowiada za dany proces, dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych osobowych.
3. W sytuacji, o której mowa w ust. 2, kierujący komórką organizacyjną sporządza notatkę, która zawiera w szczególności elementy wskazane w ust. 1 po uwzględnieniu zmian. Kopia notatki przekazywana jest do IOD.
4. Nie przeprowadza się oceny skutków dla ochrony danych osobowych w przypadku, o którym mowa w art. 35 ust. 10 RODO.

§ 19.

1. Jeżeli przeprowadzona ocena skutków dla ochrony danych osobowych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator nie zastosował środków w celu zminimalizowania tego ryzyka, przed rozpoczęciem przetwarzania Administrator konsultuje się z organem nadzorczym.
2. Komórka organizacyjna, która przeprowadziła ocenę, konsultuje się z UODO za pośrednictwem IOD, przedstawiając następujące informacje:
   1) jeżeli ma to zastosowanie – odpowiednie obowiązki Administratora, współadministratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu;
   2) cele i sposoby zamierzonego przetwarzania;
   3) środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą;
   4) dane kontaktowe IOD;
   5) ocenę skutków dla ochrony danych;
   6) wszelkie inne informacje, których zażąda organ nadzorczy.

ROZDZIAŁ XIII
Inspektor Ochrony Danych (IOD)

§ 20.

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, w szczególności:
   1) opiniuje projekty aktów normatywnych, aktów wewnętrznych, umów i innych dokumentów związanych z ochroną danych osobowych;
   2) informuje Administratora i użytkowników o obowiązkach spoczywających na nich z mocy RODO oraz wynikających z innych przepisów w zakresie ochrony danych osobowych;
   3) doradza użytkownikom w zakresie obowiązków spoczywających na nich z mocy RODO oraz innych przepisów w zakresie ochrony danych osobowych; działanie to IOD realizuje przez przygotowywanie opinii, notatek służbowych, udział w ocenie skutków dla ochrony danych osobowych;
   4) prowadzi szkolenia, w tym wstępne, warsztaty oraz udziela porad i konsultacji użytkownikom w zakresie ochrony danych osobowych;
   5) monitoruje przestrzeganie przepisów z zakresu ochrony danych osobowych oraz regulacji wewnętrznych dotyczących ochrony danych osobowych wdrożonych w Ministerstwie; działanie to IOD realizuje w szczególności przez przeprowadzanie czynności monitoringowych, w ramach których zbiera informacje w celu identyfikacji czynności przetwarzania oraz przeprowadza analizę zgodności tego przetwarzania;
   6) zapewnia obsługę adresu e-mail: iodo@mrips.gov.pl, w tym koordynuje udzielanie odpowiedzi na zapytania wysyłane na ten adres;
   7) koordynuje procedurę rozpatrywania wniosków, o których mowa w art. 15–22 RODO skierowanych do Ministerstwa za pośrednictwem adresu e-mail: iodo@mrips.gov.pl oraz w przypadku, gdy wniosek dotyczy więcej niż jednej komórki organizacyjnej;
   8) udziela zaleceń co do oceny skutków dla ochrony danych osobowych oraz monitoruje wykonanie oceny skutków dla ochrony danych osobowych;
   9) współpracuje z UODO i pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, oraz w stosownych przypadkach prowadzi konsultacje w innych sprawach;

10) prowadzi rejestr czynności przetwarzania oraz rejestr kategorii czynności przetwarzania Ministerstwa dbając o kompletność i spójność zawartych w nich informacji.

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. IOD podlega bezpośrednio Ministrowi, któremu składa roczne sprawozdanie w zakresie podejmowanych działań, z zastrzeżeniem § 23 ust. 5.
6. Administrator może powołać zastępcę lub zastępców IOD. Zastępca IOD w czasie nieobecności IOD wykonuje jego zadania.

ROZDZIAŁ XIV
Środki techniczne i organizacyjne zapewniające bezpieczeństwo danych osobowych przetwarzanych w Ministerstwie

§ 21.

1. Środki techniczne i organizacyjne w systemach informatycznych stosowane w celu zapewnienia bezpieczeństwa danych osobowych przetwarzanych w Ministerstwie są określone w PBI. Za ich wdrożenie odpowiada Dyrektor DI.
2. Środki techniczne i organizacyjne dotyczące fizycznego dostępu do obszaru, w którym przetwarzane są dane osobowe, są określone w regulacjach wewnętrznych Ministerstwa. Za ich wdrożenie odpowiada Dyrektor BA.
3. Środki techniczne i organizacyjne, o których mowa w ust. 1 i 2, zostały dobrane na podstawie przeprowadzonej analizy ryzyka, w której uwzględniono następujące elementy:
   1) stan wiedzy technicznej;
   2) koszt wdrożenia środków technicznych i organizacyjnych;
   3) charakter przetwarzania, przez który należy rozumieć częstotliwość, czasowość, długoterminowość, masowość przetwarzania;
   4) zakres przetwarzania (katalog operacji na danych osobowych);
   5) kontekst przetwarzania, czyli kategorie przetwarzanych danych, kategorie osób, których dane dotyczą, okoliczności zbierania i dalszego przetwarzania, otoczenie i zagrożenia dla bezpieczeństwa i integralności danych;
   6) cele przetwarzania.
4. 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.

ROZDZIAŁ XV
Analiza ryzyka w obszarze ochrony danych osobowych

§ 22.

1. W Ministerstwie analiza ryzyka dla procesów, w ramach których przetwarzane są dane osobowe przeprowadzana jest zgodnie z wewnętrznymi regulacjami w tym zakresie.
2. Sposób przeprowadzania i dokumentowania wyników analizy ryzyka wskazanej w ust. 1 opisują odrębne regulacje obowiązujące w Ministerstwie.

3. Analiza ryzyka dla procesów, w ramach których przetwarzane są dane osobowe, jest przeprowadzana również w następujących przypadkach:

   1) naruszenia ochrony danych osobowych, o której mowa w rozdziale XI;

   2) przeprowadzania oceny skutków dla ochrony danych osobowych, o której mowa w rozdziale XII.

4. W sytuacji wskazanej w ust. 3 pkt 1 przeprowadzana jest ocena ryzyka prywatności tj. oceny prawdopodobieństwa naruszenia praw i wolności osób, których dane dotyczą i wiążących się z tym potencjalnych skutków. Ocena jest niezbędna do identyfikacji środków zaradczych i do wydania rekomendacji w celu zaradzenia naruszeniu.

5. W sytuacji wskazanej w ust. 3 pkt 2 analiza ryzyka przeprowadzana jest z uwzględnieniem:

   1) oceny ryzyka przetwarzania, tj. stopnia zagrożenia dla poufności, integralności i dostępności informacji, wyrażonego jako prawdopodobieństwo wystąpienia zagrożenia i szkodliwości jego skutków;

   2) oceny ryzyka prywatności, tj. prawdopodobieństwa naruszenia praw i wolności osób, których dane dotyczą i wiążących się z tym potencjalnych skutków.

ROZDZIAŁ XVI
Obowiązki użytkowników i odpowiedzialność za przetwarzanie danych osobowych

§ 23.

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 § 17, 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.

3. Członek Kierownictwa Ministerstwa, zgodnie z ustalonym podziałem pracy w kierownictwie, jest uprawniony do zawierania umów i porozumień dotyczących przetwarzania danych osobowych, w tym umów powierzenia przetwarzania danych osobowych, a także zawierania aneksów do tych umów i porozumień.

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

5. Dyrektor Generalny Ministerstwa, w imieniu Ministra wykonuje czynności administratora wobec IOD, w szczególności:

   1) właściwie i niezwłocznie włącza IOD we wszystkie sprawy dotyczące ochrony danych osobowych w Ministerstwie, zgodnie z art. 38 ust. 1 RODO;

   2) wspiera IOD w wypełnianiu jego zadań, zapewnia mu zasoby niezbędne do wykonywania jego zadań oraz utrzymania wiedzy fachowej oraz zapewnia dostęp do danych osobowych i operacji przetwarzania, zgodnie z art. 38 ust. 2 RODO;

   3) wyznacza IOD zadania i obowiązki niewynikające z RODO jedynie w zakresie niepowodującym konfliktu interesów, zgodnie z art. 38 ust. 6 RODO.

§ 24.

1. Do zadań kierujących komórkami organizacyjnymi należy, w zakresie właściwości tych komórek, wykonywanie czynności administratora niezastrzeżonych 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 na podstawie posiadanego upoważnienia lub pełnomocnictwa;

3) prowadzenie rejestru umów powierzenia przetwarzania danych osobowych;

4) przeprowadzanie analizy projektowanych czynności przetwarzania danych osobowych w zakresie określonym w rozdziale XII, w tym przeprowadzanie analizy ryzyka naruszenia praw lub wolności osób fizycznych oraz oceny skutków dla ochrony danych osobowych

5) realizacja obowiązku informacyjnego, o którym mowa w rozdziale VII;

6) rozpatrywanie wniosków, o których mowa w art. 15–22 RODO, niepozostających we właściwości IOD, w terminie określonym w art. 12 ust. 3 i 4 RODO oraz niezwłoczna realizacja praw osób, których dane dotyczą;

7) zgłaszanie konieczności wprowadzenia zmian w rejestrze czynności przetwarzania danych i rejestrze kategorii czynności przetwarzania;

8) współpraca z IOD przy realizacji jego zadań;

9) informowanie IOD o pracach dotyczących planowania/projektowania/przygotowania przedsięwzięć o charakterze programowym, legislacyjnym lub 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 BKA.

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 ust. 1, w zakresie właściwości tych komórek.

3. Kierujący komórką organizacyjną może wyznaczać koordynatora ds. ochrony danych osobowych w celu realizacji niektórych lub wszystkich zadań, o których mowa w § 28 Polityki. Zakres uprawnień i obowiązków koordynatora ds. ochrony danych osobowych określa opis stanowiska pracy. O wyznaczeniu koordynatora oraz o zakresie jego działania kierujący komórką organizacyjną informuje niezwłocznie IOD.

§ 25.

Do zadań Dyrektora BKA należy:

1) wydawanie upoważnień do przetwarzania danych osobowych dla użytkowników;

2) prowadzenie rejestru wydanych upoważnień.

§ 26.

Do zadań kierującego BA należy zapewnienie w Ministerstwie warunków umożliwiających wdrożenie standardowych środków organizacyjnych i technicznych przetwarzania danych osobowych w postaci papierowej dla procesów, których to dotyczy.

§ 27.

Do zadań kierującego DI należy:

1) zapewnienie w Ministerstwie warunków umożliwiających wdrożenie standardowych środków organizacyjnych i technicznych przetwarzania danych osobowych w systemach teleinformatycznych;

2) opracowanie oraz opiniowanie projektów wewnętrznych aktów normatywnych Ministerstwa w zakresie przetwarzania danych osobowych w systemach teleinformatycznych.

§ 28.

Do zadań koordynatora ds. ochrony danych osobowych w komórce organizacyjnej należy:

1) współpraca z IOD w zakresie przetwarzania danych osobowych w komórce organizacyjnej;

2) prowadzenie rejestru czynności i rejestru kategorii czynności przetwarzania danych;

3) prowadzenie rejestru wydanych upoważnień;

4) przeprowadzanie, jeżeli zaistnieje taka konieczność, czynności monitoringu przestrzegania zasad przetwarzania danych osobowych w komórce organizacyjnej 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.

§ 29.

1. Użytkownicy są w szczególności obowiązani do:

1) przetwarzania danych osobowych zgodnie z RODO i Polityką oraz innymi regulacjami wewnętrznymi 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) zabezpieczenia danych osobowych przed ich utratą, uszkodzeniem lub zniszczeniem, zmianą lub udostępnieniem osobom nieupoważnionym przez:

a) przestrzeganie procedur właściwego użytkowania systemów informatycznych, w których przetwarza się dane osobowe, w tym nieujawnianie innym użytkownikom swoich loginów i haseł,

b) zabezpieczenie dokumentów w postaci papierowej, zawierających dane osobowe oraz zabezpieczanie dostępu do danych osobowych przetwarzanych w systemie informatycznym na stanowisku pracy

– w pomieszczeniach służbowych lub wyznaczonych ich częściach a w przypadku pracy zdalnej stosowania analogicznych środków w miejscu jej wykonywania;

4) bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania danych w systemach teleinformatycznych, określonych w PBI;

5) niszczenia wszystkich niepodlegających archiwizacji, zbędnych dokumentów zawierających dane osobowe;

6) uczestniczenia w okresowych szkoleniach z obszaru ochrony danych osobowych;

7) współpracy z IOD przy realizacji jego zadań.

2. Za naruszenie obowiązków w zakresie ochrony danych osobowych pracownicy podlegają odpowiedzialności dyscyplinarnej, wynikającej z przepisów o służbie cywilnej, lub porządkowej, wynikającej z przepisów prawa pracy.

3. Użytkownicy niebędący pracownikami, za naruszenie obowiązków, o których mowa w ust. 1, podlegają odpowiedzialności przewidzianej w umowach lub w innych aktach i dokumentach, na podstawie których przetwarzają dane osobowe.

4. Każdy użytkownik, przed rozpoczęciem przetwarzania danych osobowych, jest obowiązany zapoznać się z przepisami i procedurami dotyczącymi ochrony danych osobowych, w tym w szczególności z RODO i ustawą o ochronie danych osobowych, a także z obowiązującą w Ministerstwie Polityką i innymi regulacjami wewnętrznymi dotyczącymi ochrony danych osobowych.

5. 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, składając oświadczenie według wzoru stanowiącego załącznik nr 10 do zarządzenia, tak aby w sposób jednoznaczny zapewnić potwierdzenie tego faktu w zakresie spełnienia zasady rozliczalności. Oświadczenie jest składane w postaci elektronicznej. Oświadczenia gromadzone są w BKA.

6. W przypadku długotrwałej nieobecności użytkownika okres 14 dni liczony jest od pierwszego dnia po ustaniu tej nieobecności.