DZIENNIK URZĘDOWY
MINISTRA FINANSÓW,
FUNDUSZY I POLITYKI REGIONALNEJ

Warszawa, dnia 31 grudnia 2020 r.

Poz. 37

ZARZĄDZENIE

MINISTRA FINANSÓW, FUNDUSZY I POLITYKI REGIONALNEJ

z dnia 29 grudnia 2020 r.

w sprawie wprowadzenia Polityki Ochrony Danych Osobowych

Na podstawie art. 24 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE. L 119 z 04.05.2016, str. 1, z późn. zm.[1)]) oraz art. 31 ust. 4 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125) zarządza się, co następuje:

§ 1. 1. Wprowadza się Politykę Ochrony Danych Osobowych, zwaną dalej „Polityką”, stanowiącą załącznik do zarządzenia, w:

1) Ministerstwie Finansów;
2) izbach administracji skarbowej;
3) urzędach skarbowych;
4) urzędach celno-skarbowych wraz z podległymi oddziałami celnymi;
5) Krajowej Informacji Skarbowej;
6) Krajowej Szkole Skarbowości;
7) Centrum Informatyki Resortu Finansów;
8) delegaturach jednostek organizacyjnych Krajowej Administracji Skarbowej utworzonych przez ministra właściwego do spraw finansów publicznych na podstawie art. 36 ust. 2 ustawy z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz. U. z 2020 r. poz. 505, 568, 695, 1087 i 1106).

---

1) Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE. L 127 z 23.05.2018, str. 2.

2. Politykę stosuje się do przetwarzania danych osobowych przez Ministra Finansów, Funduszy i Polityki Regionalnej jako samodzielnego administratora lub jako współadministratora w działach administracji rządowej: budżet, finanse publiczne i instytucje finansowe.

3. Politykę stosuje się również do przetwarzania danych osobowych przez Ministra Finansów, Funduszy i Polityki Regionalnej w działach administracji rządowej: budżet, finanse publiczne i instytucje finansowe jako podmiotu przetwarzającego w zakresie, w jakim umowa powierzenia przetwarzania danych osobowych go wiążąca, nie stanowi inaczej.

§ 2. Zarządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia[2)].

Minister Finansów, Funduszy i Polityki Regionalnej: T. Kościński

[2)] Niniejsze zarządzenie było poprzedzone Polityką Ochrony Danych Osobowych dla Ministerstwa Finansów, zatwierdzoną w dniu 25 maja 2018 r.

Załącznik do zarządzenia
Ministra Finansów, Funduszy i Polityki Regionalnej
z dnia 29 grudnia 2020 r. w sprawie wprowadzenia
Polityki Ochrony Danych Osobowych (poz. 37)

POLITYKA OCHRONY DANYCH OSOBOWYCH

SPIS TREŚCI

Rozdział 1

Postanowienia ogólne

§ 1. Użyte w Polityce pojęcia oznaczają:

1) Administrator – ministra właściwego do spraw budżetu państwa, finansów publicznych oraz instytucji finansowych;
2) ASI (administrator systemu teleinformatycznego) – pracownika, wyznaczonego zgodnie z PBT przez dyrektora komórki organizacyjnej w Ministerstwie właściwej do spraw informatyzacji, przez dyrektora CI RF albo przez Dyrektora IAS, jeżeli IAS wykonuje zadania centrum kompetencyjnego lub zadania scentralizowane, o ile zakres zadań obejmuje administrowanie systemem teleinformatycznym służącym do przetwarzania danych osobowych, odpowiedzialnego za administrowanie i monitorowanie systemu teleinformatycznego służącego do przetwarzania danych osobowych oraz zapewnienie jego bezpiecznej eksploatacji, zgodnie z zadaniami określonymi w PBT;
3) AZU (administrator zarządzający uprawnieniami) – pracownika, wyznaczonego zgodnie z PBT przez dyrektora komórki organizacyjnej w Ministerstwie pełniącej funkcję właściciela biznesowego systemu teleinformatycznego w porozumieniu z dyrektorem komórki organizacyjnej w Ministerstwie właściwej do spraw informatyzacji albo przez Dyrektora IAS, jeżeli IAS wykonuje zadania centrum kompetencyjnego lub zadania scentralizowane, o ile zakres zadań obejmuje zarządzanie uprawnieniami w systemie teleinformatycznym służącym do przetwarzania danych osobowych, wykonującego zadania w zakresie zarządzania uprawnieniami użytkowników w systemie teleinformatycznym służącym do przetwarzania danych osobowych;
4) CI RF – Centrum Informatyki Resortu Finansów;
5) 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;
6) DB – komórkę organizacyjną w Ministerstwie właściwą do spraw bezpieczeństwa i ochrony informacji;
7) IAS – Izbę Administracji Skarbowej;

8) IOD MF (Inspektor Ochrony Danych) – osobę wyznaczoną przez Administratora, zgodnie z art. 37 RODO i art. 46 ustawy policyjnej, realizującą zadania określone w art. 39 ust. 1 RODO i art. 47 ust. 1 ustawy policyjnej, a także - w przypadku nieobecności IOD MF – osobę wyznaczoną przez Administratora do zastępowania IOD MF;
9) Jednostka – jednostkę organizacyjną podległą ministrowi właściwemu do spraw budżetu, finansów publicznych oraz instytucji finansowych albo przez niego nadzorowaną, objętą Polityką;
10) organy KAS – organy wskazane w art. 11 ust. 1 ustawy o KAS;
11) koordynator do spraw ochrony danych osobowych – pracownika wyznaczonego przez odpowiednio dyrektora komórki organizacyjnej w Ministerstwie lub kierownika Jednostki. Koordynatorem do spraw ochrony danych osobowych w Jednostce może być osoba pełniąca funkcję inspektora ochrony danych w Jednostce lub osoba go zastępująca;
12) koordynator merytoryczny systemu teleinformatycznego – pracownika wyznaczonego przez dyrektora komórki organizacyjnej w Ministerstwie pełniącej funkcję właściciela biznesowego systemu teleinformatycznego;
13) Ministerstwo – Ministerstwo Finansów;
14) naruszenie ochrony danych osobowych – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
15) Polityka – Politykę Ochrony Danych Osobowych;
16) PBT – Politykę Bezpieczeństwa Teleinformatycznego;
17) pracownik – osobę fizyczną realizującą zadania na rzecz Ministerstwa lub na rzecz Jednostki na podstawie umowy o pracę, powołania, mianowania albo umowy cywilnoprawnej, osobę pełniącą w niej służbę, w tym funkcjonariusza Służby Celno-Skarbowej, oraz praktykanta, stażystę lub wolontariusza;
18) Regulamin organizacyjny Ministerstwa – regulamin ustalony zarządzeniem Ministra Finansów z dnia 17 kwietnia 2019 r. w sprawie ustalenia regulaminu organizacyjnego Ministerstwa Finansów (Dz. Urz. Min. Fin. z 2020 r. poz. 80, z późn. zm.);
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) (Dz. Urz. UE. L 119 z 04.05.2016, str. 1, z późn. zm.);
20) system teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie

danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2019 r. poz. 2460, z późn. zm.);

21) UODO – Urząd Ochrony Danych Osobowych;

22) UCS – urząd celno-skarbowy wraz z podległymi oddziałami celnymi;

23) US – urząd skarbowy;

24) ustawa o KAS – ustawę z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz. U. z 2020 r. poz. 505, z późn. zm.);

25) ustawa policyjna – ustawę z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125);

26) właściciel biznesowy danych – komórkę organizacyjną w Ministerstwie odpowiedzialną merytorycznie za przetwarzanie danych, w szczególności danych osobowych, w zakresie wynikającym z zadań określonych w Regulaminie organizacyjnym Ministerstwa. Właściciel biznesowy danych może być jednocześnie Właścicielem biznesowym systemu teleinformatycznego;

27) właściciel biznesowy systemu teleinformatycznego – komórkę organizacyjną w Ministerstwie odpowiedzialną za wykonywanie zadań właściciela biznesowego w odniesieniu do przypisanego systemu teleinformatycznego służącego do przetwarzania danych osobowych, w zakresie określonym w Regulaminie organizacyjnym Ministerstwa.

Cel Polityki

§ 2. 1. Polityka służy zapewnieniu ochrony danych osobowych przetwarzanych w Ministerstwie oraz Jednostkach, przez:

1) ustanowienie jednolitych reguł postępowania w zakresie przetwarzania danych osobowych;

2) wdrożenie środków organizacyjnych i technicznych, które zapewniają przetwarzanie danych osobowych zgodnie z prawem, w szczególności z RODO i ustawą policyjną, oraz możliwość wykazania tej zgodności.

2. Szczegółowymi celami Polityki są:

1) zapewnienie realizacji praw osób, których dane osobowe dotyczą, zgodnie z procedurą, o której mowa w § 43;

2) określenie obowiązków i odpowiedzialności osób zobowiązanych do realizacji zadań, określonych w Polityce;

3) zapewnienie przeprowadzania oceny skutków dla ochrony danych;

4) zarządzanie naruszeniami ochrony danych osobowych i ograniczanie ich skutków.

Zakres stosowania Polityki

§ 3. 1. Polityka określa sposób przetwarzania danych osobowych i zarządzania procesami związanymi z przetwarzaniem danych osobowych w celu zapewnienia odpowiedniej ochrony tych danych, dla których administratorem lub współadministratorem jest Minister Finansów, Funduszy i Polityki Regionalnej w działach administracji rządowej: budżet, finanse publiczne i instytucje finansowe.

2. Polityka określa również sposób przetwarzania danych osobowych i zarządzania procesami związanymi z przetwarzaniem danych osobowych w celu zapewnienia odpowiedniej ochrony tych danych, dla których Minister Finansów, Funduszy i Polityki Regionalnej w działach administracji rządowej: budżet, finanse publiczne i instytucje finansowe, jest podmiotem przetwarzającym, w zakresie, w jakim umowa powierzenia przetwarzania danych osobowych wiążąca Ministra Finansów, Funduszy i Polityki Regionalnej, nie stanowi inaczej.

3. Polityka określa obowiązki i odpowiedzialność osób zobowiązanych do realizacji zadań związanych z procesami, o których mowa w ust. 1 i 2.

4. Polityka ma zastosowanie do przetwarzania danych osobowych, o których mowa w ust. 1 i 2, niezależnie od:

1) sposobu przetwarzania (całkowicie zautomatyzowany, częściowo zautomatyzowany lub inny niż zautomatyzowany);
2) formy lub postaci przetwarzania (papierowa, elektroniczna lub inna);
3) kanałów przepływu danych osobowych;
4) narzędzi informatycznych służących do przetwarzania danych osobowych (systemów, aplikacji, programów);
5) celu przetwarzania;
6) źródła pochodzenia danych osobowych;
7) kategorii danych osobowych.

5. Politykę stosują wszystkie osoby, które na polecenie Administratora uczestniczą w przetwarzaniu danych osobowych.

Deklaracja Administratora

§ 4. 1. Administrator przykłada szczególną wagę do zapewnienia ochrony danych osobowych, ponieważ ma ona istotne znaczenie dla realizacji misji, wizji i celów Ministerstwa Finansów i Krajowej Administracji Skarbowej.

2. Administrator:

1) wdraża, utrzymuje i udoskonala ochronę danych osobowych, której celem jest zapewnienie realizacji praw i wolności osób, których te dane dotyczą;
2) systemowo identyfikuje ryzyka dla bezpieczeństwa danych osobowych oraz minimalizuje ryzyka, przez zastosowanie adekwatnych środków organizacyjnych i technicznych;
3) wspiera IOD MF w wypełnianiu przez niego zadań, zapewniając mu w niezbędnym zakresie zasoby do ich wykonania, dostęp do informacji mających wpływ na ochronę danych osobowych i dostęp do operacji przetwarzania, w szczególności przez niezwłoczne włączanie IOD MF we wszystkie sprawy dotyczące ochrony danych osobowych, a także przez zapewnienie zasobów niezbędnych do utrzymania jego wiedzy fachowej;
4) reaguje na naruszenia ochrony danych osobowych oraz wdraża środki zapobiegające ich wystąpieniu w przyszłości.

3. Administrator zapewnia:

1) merytoryczną podległość IOD MF bezpośrednio Administratorowi;

2) niezależność IOD MF w zakresie wykonywanych obowiązków, co oznacza, że nie może on otrzymywać instrukcji dotyczących wykonywania swoich zadań oraz nie może zostać ukarany za wypełnianie swoich zadań, ani z tego powodu odwołany;

3) powierzanie IOD MF tylko takich zadań i obowiązków, które nie pozostają w konflikcie interesów.

Organizacyjne środki ochrony danych osobowych

§ 5. 1. W celu zapewnienia zgodności przetwarzania danych osobowych z przepisami RODO i ustawy policyjnej Administrator wdraża środki organizacyjne obejmujące w szczególności:

1) organizację systemu ochrony danych osobowych, z określeniem ról, zadań i odpowiedzialności;
2) polityki szczegółowe obejmujące Politykę, a także PBT i polityki szczegółowe dotyczące ciągłości działania oraz bezpieczeństwa fizycznego, a także powiązane z nimi procedury i instrukcje;
3) okresowe przeglądy Polityki oraz dokumentów powiązanych, nie rzadziej niż raz na rok;
4) procedury wydawania upoważnień do przetwarzania danych osobowych, o których mowa w rozdziale 3;
5) zarządzanie naruszeniami ochrony danych osobowych, zgodnie z procedurą, o której mowa w § 37 ust. 2;
6) procedury zarządzania uprawnieniami w systemach teleinformatycznych służących do przetwarzania danych osobowych, zgodnie z PBT;
7) podnoszenie świadomości pracowników w zakresie ochrony danych osobowych;
8) procedury zapewniające realizację obowiązków informacyjnych, zgodnie z § 43;

9) procedury zapewniające realizację praw osób, których dane dotyczą, zgodnie z rozdziałem 12.

2. W razie konieczności, w oparciu o wyniki analizy ryzyka, stosuje się dodatkowo inne organizacyjne środki ochrony danych osobowych.

Techniczne środki ochrony danych osobowych

§ 6. 1. W celu zabezpieczenia danych osobowych przed udostępnieniem osobom nieupoważnionym, zabraniem przez osoby nieuprawnione, przetwarzaniem z naruszeniem prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, Administrator wdraża techniczne środki ochrony danych osobowych odpowiednie do zagrożeń oraz kategorii danych osobowych oraz niezbędne zabezpieczenia.

2. Szczegółowe wymagania w zakresie stosowania wskazanych środków ochrony oraz niezbędnych zabezpieczeń określone są w politykach szczegółowych, instrukcjach i procedurach dotyczących:

1) bezpieczeństwa teleinformatycznego;
2) ciągłości działania;
3) bezpieczeństwa fizycznego.

Rozdział 2

Role i odpowiedzialności

§ 7. Dyrektor komórki organizacyjnej w Ministerstwie w zakresie swojej właściwości:

1) sprawuje nadzór nad przetwarzaniem i ochroną danych osobowych w celu zapewnienia zgodności ich przetwarzania z przepisami prawa i Polityką;
2) zarządza ryzykiem związanym z przetwarzaniem danych osobowych, zgodnie z procedurą zarządzania ryzykiem, w tym dokonywania analizy ryzyka;
3) udziela i cofa pracownikom komórki organizacyjnej w Ministerstwie upoważnienia do przetwarzania danych osobowych, zgodnie z § 20;
4) prowadzi ewidencję wydanych zgodnie z § 20 upoważnień do przetwarzania danych osobowych oraz upoważnień udzielonych na podstawie § 19 ust. 2;
5) zawiera, modyfikuje i rozwiązuje w imieniu Administratora umowy powierzenia przetwarzania danych osobowych, zgodnie z § 38 ust. 1, i je realizuje;
6) zawiera umowy powierzenia przetwarzania danych osobowych, w imieniu ministra właściwego do spraw budżetu, finansów publicznych oraz instytucji finansowych działającego jako podmiot przetwarzający, zgodnie z § 38 ust. 2, i je realizuje;

7) weryfikuje podmioty przed zawarciem umowy powierzenia przetwarzania danych osobowych, o której mowa w pkt 5;
8) prowadzi, w uzasadnionych przypadkach, w uzgodnieniu z IOD MF, audyty i inspekcje związane z powierzeniem przetwarzania danych osobowych podmiotom zewnętrznym;
9) realizuje zadania właściciela biznesowego systemu teleinformatycznego, określone w § 27 ust. 1 pkt 7 regulaminu organizacyjnego Ministerstwa, w odniesieniu do systemu teleinformatycznego służącego do przetwarzania danych osobowych, oraz w zakresie:
   a) wyznaczania koordynatora merytorycznego dla systemu teleinformatycznego;
   b) akceptacji wniosków o przyznawanie, modyfikację i odebranie praw dostępu do danych osobowych w systemie teleinformatycznym;
   c) akceptowania środków ochrony danych osobowych wynikających z analizy ryzyka;
   d) wyznaczania AZU w przypadku realizowania przez właściciela biznesowego systemu teleinformatycznego zadań związanych z zarządzaniem uprawnieniami;
10) podejmuje decyzje w zakresie udostępniania danych osobowych;
11) zgłasza i aktualizuje czynności przetwarzania danych osobowych w rejestrze prowadzonym zgodnie z art. 30 ust. 1 RODO i art. 35 ust. 1 i 2 ustawy policyjnej;
12) zgłasza i aktualizuje kategorie czynności przetwarzania dokonywane przez ministra właściwego do spraw budżetu, finansów publicznych oraz instytucji finansowych jako podmiot przetwarzający, w rejestrze prowadzonym zgodnie z art. 30 ust. 2 RODO i art. 35 ust. 3 i 4 ustawy policyjnej;
13) dokonuje przeglądu i usuwa dane osobowe zgodnie z procedurą przeglądu i usuwania danych osobowych;
14) wypełnia obowiązki informacyjne zgodnie z art. 12–14 RODO lub art. 22 ustawy policyjnej;
15) realizuje prawa osób, których dane dotyczą, na podstawie art. 15-21 RODO lub art. 22–26 ustawy policyjnej, zgodnie z § 43;
16) zapewnia właściwe i niezwłoczne włączanie IOD MF we wszystkie sprawy dotyczące ochrony danych osobowych, zgodnie z Regulaminem organizacyjnym Ministerstwa – począwszy od etapu ich projektowania oraz analizowania ryzyka dla ochrony danych osobowych, przez ich realizację, wdrożenie, aż do usunięcia danych osobowych, w szczególności konsultuje z IOD MF:
   a) projekty aktów prawnych, regulacji wewnętrznych i innych dokumentów, w tym związanych z organizacją resortu, mających związek z przetwarzaniem lub ochroną danych osobowych,
   b) planowane lub podejmowane przedsięwzięcia, w tym realizowane projekty, programy i inne inicjatywy, związane z przetwarzaniem danych osobowych,
   c) projekty umów powierzenia przetwarzania danych osobowych,

d) projekty pism dotyczących ochrony danych osobowych kierowane do jednostek organizacyjnych podległych Ministrowi albo przez niego nadzorowanych, urzędów obsługujących organy administracji publicznej, jednostek organizacyjnych podległych organom administracji publicznej albo przez nich nadzorowanych oraz innych podmiotów spoza Ministerstwa, w szczególności pism kierowanych do UODO,

e) projektowanie i modyfikowanie systemów teleinformatycznych służących do przetwarzania danych osobowych,

f) środki ochrony praw i wolności osób, których dane osobowe dotyczą,

g) szkolenia, konferencje i inne spotkania, w szczególności spotkania z udziałem przedstawicieli UODO lub dotyczące ochrony danych osobowych;

h) rozwiązania organizacyjne pod kątem właściwego wdrażania systemu ochrony danych osobowych;

17) dokonuje, w porozumieniu z IOD MF, oceny skutków dla ochrony danych w odniesieniu do operacji przetwarzania, na podstawie art. 35 RODO lub art. 37 ustawy policyjnej;

18) prowadzi, w przypadkach, o których mowa w art. 36 RODO lub art. 38 ustawy policyjnej, w porozumieniu z IOD MF, konsultacje z organem nadzorczym przed rozpoczęciem przetwarzania danych osobowych;

19) zgłasza zdarzenie mogące stanowić naruszenie ochrony danych osobowych, zgodnie z procedurą zarządzania incydentami, i uczestniczenia w czynnościach wyjaśniających;

20) zawiadamia, w uzgodnieniu z IOD MF, osoby, których dane zostały dotknięte naruszeniem ochrony danych osobowych, zgodnie z procedurą, o której mowa w pkt 19;

21) przekazuje do DB dokumentację i niezbędne wyjaśnienia na potrzeby kontroli zewnętrznych dotyczących ochrony danych osobowych;

22) wyznacza koordynatora do spraw ochrony danych osobowych i umożliwia mu wykonywanie jego zadań, w szczególności przez bieżący dostęp do informacji o działaniach komórki organizacyjnej w Ministerstwie.

§ 8. Dyrektor DB:

1) opracowuje, aktualizuje i wdraża Politykę oraz procedury, instrukcje i inne dokumenty z zakresu ochrony danych osobowych, z zastrzeżeniem procedur, dla których zgodnie z Polityką właścicielem jest inna komórka organizacyjna w Ministerstwie;

2) przygotowuje i publikuje wzory dokumentów dotyczących ochrony danych osobowych, w tym klauzul informacyjnych, upoważnień do przetwarzania danych osobowych oraz umów powierzenia przetwarzania danych osobowych;

3) koordynuje zarządzanie ryzykiem związanym z przetwarzaniem danych osobowych w celu określenia adekwatnych technicznych i organizacyjnych środków ochrony danych osobowych;
4) prowadzi rejestr czynności przetwarzania danych osobowych, zgodnie z art. 30 ust. 1 RODO i art. 35 ust. 1 i 2 ustawy policyjnej;
5) prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych przez ministra właściwego do spraw budżetu, finansów publicznych oraz instytucji finansowych działającego jako podmiot przetwarzający, zgodnie z art. 30 ust. 2 RODO i art. 35 ust. 3 i 4 ustawy policyjnej;
6) bierze udział, na wniosek dyrektora komórki organizacyjnej w Ministerstwie, dyrektora IAS lub z własnej inicjatywy, w weryfikacji podmiotu przed zawarciem umowy powierzenia przetwarzania danych osobowych;
7) bierze udział, w uzasadnionych przypadkach, w audytach i inspekcjach związanych z powierzeniem przetwarzania danych osobowych podmiotom zewnętrznym;
8) przygotowuje dokumentację i niezbędne wyjaśnienia na potrzeby kontroli zewnętrznych dotyczących ochrony danych osobowych, we współpracy z IOD MF, na podstawie informacji przekazanych przez właściwą merytorycznie komórkę organizacyjną w Ministerstwie;
9) zarządza naruszeniami ochrony danych osobowych, w tym prowadzi rejestr naruszeń ochrony danych osobowych oraz zgłasza naruszenia ochrony danych osobowych do Prezesa UODO na podstawie odrębnego upoważnienia;
10) wykonuje w imieniu Administratora czynności należące do zakresu jego właściwości określonej w RODO, na podstawie odrębnego upoważnienia;
11) współpracuje, w porozumieniu z IOD MF, z koordynatorami do spraw ochrony danych osobowych w komórkach organizacyjnych w Ministerstwie i w IAS;
12) bierze udział i udziela wsparcia komórkom organizacyjnym w Ministerstwie w przeprowadzaniu oceny skutków dla ochrony danych.

§ 9. Dyrektor IAS w zakresie swojej właściwości, w odniesieniu do danych osobowych, o których mowa w § 3 ust. 1, przetwarzanych przez IAS oraz podległe US oraz UCS:

1) sprawuje nadzór nad przetwarzaniem i ochroną danych osobowych w celu zapewnienia zgodności ich przetwarzania z przepisami prawa i Polityką;
2) zarządza ryzykiem związanym z przetwarzaniem danych osobowych, zgodnie z procedurą zarządzania ryzykiem, w tym dokonuje analizy ryzyka;
3) udziela i cofa pracownikom IAS upoważnienia do przetwarzania danych osobowych, zgodnie z § 20;

4) prowadzi ewidencję wydanych zgodnie z § 20 upoważnień do przetwarzania danych osobowych, oraz upoważnień udzielonych na podstawie § 19 ust. 3;
5) zawiera, modyfikuje i rozwiązuje – po akceptacji IOD MF i właściciela biznesowego systemu teleinformatycznego – w imieniu Administratora umowy powierzenia przetwarzania danych osobowych, zgodnie z § 38 ust. 1, w zakresie realizacji zadań w ramach centrum kompetencyjnego lub wykonywania zadania scentralizowanego, i je realizuje;
6) weryfikuje podmiot przed zawarciem umowy powierzenia przetwarzania danych osobowych, o której mowa w pkt 5;
7) bierze udział, na wniosek właściciela biznesowego danych, w audytach i inspekcjach związanych z powierzeniem przetwarzania danych osobowych podmiotom zewnętrznym oraz prowadzi takie audyty i inspekcje, za wiedzą IOD MF i właściciela biznesowego systemu teleinformatycznego, dla umów powierzenia, o których mowa w pkt 5;
8) podejmuje decyzje w zakresie udostępniania danych osobowych;
9) dokonuje przeglądu i usuwa dane osobowe zgodnie z procedurą przeglądu i usuwania danych osobowych;
10) wypełnia obowiązki informacyjne zgodnie z art. 12–14 RODO lub art. 22 ustawy policyjnej, w porozumieniu z właścicielem biznesowym systemu teleinformatycznego służącego do przetwarzania danych osobowych;
11) realizuje prawa osób, których dane dotyczą, na podstawie art. 15–21 RODO lub art. 22–26 ustawy policyjnej oraz zgodnie z § 43, w porozumieniu z właścicielem biznesowym systemu teleinformatycznego służącego do przetwarzania danych osobowych;
12) zapewnia właściwe i niezwłoczne włączanie IOD MF we wszystkie sprawy dotyczące ochrony danych osobowych objętych Polityką – począwszy od etapu ich projektowania oraz analizowania ryzyka dla ochrony danych osobowych, przez ich realizację, wdrożenie, aż do usunięcia danych osobowych;
13) dokonuje, w porozumieniu z koordynatorem do spraw ochrony danych osobowych i po akceptacji IOD MF, oceny skutków dla ochrony danych w odniesieniu do operacji przetwarzania, na podstawie art. 35 RODO lub art. 37 ustawy policyjnej, w zakresie realizacji zadań w ramach centrum kompetencyjnego lub wykonywania zadania scentralizowanego;
14) prowadzi, w przypadku o którym mowa w art. 36 RODO lub art. 38 ustawy policyjnej, w porozumieniu z IOD MF i właścicielem biznesowym systemu teleinformatycznego, konsultacje z organem nadzorczym przed rozpoczęciem przetwarzania danych osobowych, w zakresie realizacji zadań w ramach centrum kompetencyjnego lub wykonywania zadania scentralizowanego;

15) zgłasza zdarzenia mogące stanowić naruszenie ochrony danych osobowych, zgodnie z procedurą zarządzania incydentami, i uczestniczy w czynnościach wyjaśniających;
16) zawiadamia, w uzgodnieniu z IOD MF i właścicielem biznesowym systemu teleinformatycznego, osoby, których dane zostały dotknięte naruszeniem ochrony danych osobowych, zgodnie z procedurą, o której mowa w pkt 15;
17) przekazuje IOD MF wszelkie istotne informacje dotyczące wykonywania zadań z zakresu ochrony i sposobu przetwarzania danych osobowych, o których mowa w § 3 ust.1, w celu realizacji przez IOD MF zadań, zgodnie z przepisami RODO i ustawy policyjnej;
18) przekazuje DB, dokumentację i niezbędne wyjaśnienia na potrzeby kontroli zewnętrznych dotyczących ochrony danych osobowych;
19) przekazuje DB i IOD MF informacje o planowanych kontrolach zewnętrznych dotyczących ochrony danych osobowych objętych Polityką, w szczególności kontrolach prowadzonych przez Prezesa UODO;
20) wyznacza koordynatora do spraw ochrony danych osobowych w IAS i umożliwia mu, w szczególności przez bieżący dostęp do informacji o działaniach IAS, wykonywanie jego zadań.

§ 10. Naczelnik US lub UCS w zakresie swojej właściwości, w odniesieniu do danych osobowych, o których mowa w § 3 ust.1:

1) sprawuje nadzór nad przetwarzaniem i ochroną danych osobowych w celu zapewnienia zgodności ich przetwarzania z przepisami prawa i Polityką;
2) zarządza ryzykiem związanym z przetwarzaniem danych osobowych, zgodnie z procedurą zarządzania ryzykiem, w tym dokonuje analizy ryzyka;
3) udziela i cofa upoważnienia do przetwarzania danych osobowych, zgodnie z § 20, pracownikom odpowiednio US lub UCS;
4) prowadzi ewidencję wydanych zgodnie z § 20 upoważnień do przetwarzania danych osobowych;
5) podejmuje decyzje w zakresie udostępniania danych osobowych;
6) dokonuje przeglądu i usuwa dane osobowe zgodnie z procedurą przeglądu i usuwania danych osobowych;
7) wypełnia obowiązki informacyjne zgodnie z art. 12–14 RODO lub art. 22 ustawy policyjnej, w przypadku otrzymania polecenia od IAS;
8) realizuje prawa osób, których dane dotyczą, na podstawie art. 15–21 RODO lub art. 22–26 ustawy policyjnej oraz zgodnie z § 43, zgodnie z wytycznymi Administratora;
9) zgłasza IAS zdarzenia mogące stanowić naruszenie ochrony danych osobowych, zgodnie z procedurą zarządzania incydentami, i uczestniczy w czynnościach wyjaśniających;

10) zawiadamia osoby, których dane zostały dotknięte naruszeniem ochrony danych osobowych, w przypadku otrzymania polecenia od IAS, zgodnie z procedurą, o której mowa w pkt 9;
11) przekazuje DB dokumentację i niezbędne wyjaśnienia na potrzeby kontroli zewnętrznych dotyczących ochrony danych osobowych;
12) przekazuje DB, IOD MF i IAS informacje o planowanych kontrolach zewnętrznych dotyczących ochrony danych osobowych objętych Polityką, w szczególności kontrolach prowadzonych przez Prezesa UODO;
13) wyznacza koordynatora do spraw ochrony danych osobowych odpowiednio w US lub UCS i umożliwia mu wykonywanie jego zadań, w szczególności przez bieżący dostęp do informacji o działaniach US lub UCS.

§ 11. Dyrektor Krajowej Informacji Skarbowej (KIS) oraz dyrektor Krajowej Szkoły Skarbowości (KSS) w zakresie swojej właściwości, w odniesieniu do danych osobowych, o których mowa w § 3 ust. 1:

1) sprawują nadzór nad przetwarzaniem i ochroną danych osobowych w celu zapewnienia zgodności ich przetwarzania z przepisami prawa i Polityką;
2) zarządzają ryzykiem związanym z przetwarzaniem danych osobowych, zgodnie z procedurą zarządzania ryzykiem, w tym dokonują analizy ryzyka;
3) udzielają i cofają upoważnienia do przetwarzania danych osobowych, zgodnie z § 20, pracownikom odpowiednio KIS lub KSS;
4) prowadzą ewidencje wydanych zgodnie z § 20 upoważnień do przetwarzania danych osobowych;
5) zawierają, modyfikują i rozwiązują w imieniu Administratora umowy powierzenia przetwarzania danych osobowych, zgodnie z § 38 ust. 1, i je realizują;
6) weryfikują podmiot przed zawarciem umowy powierzenia przetwarzania danych osobowych, o której mowa w pkt 5;
7) biorą udział, w uzasadnionych przypadkach, w audytach i inspekcjach związanych w powierzeniem przetwarzania danych osobowych podmiotom zewnętrznym;
8) podejmują decyzje w zakresie udostępniania danych osobowych;
9) dokonują przeglądów i usuwają dane osobowe zgodnie z procedurą przeglądu i usuwania danych osobowych;
10) wypełniają obowiązki informacyjne zgodnie z art. 12–14 RODO lub art. 22 ustawy policyjnej, w porozumieniu z właścicielem biznesowym systemu teleinformatycznego służącego do przetwarzania danych osobowych;

11) realizują prawa osób, których dane dotyczą, na podstawie art. 15–21 RODO lub art. 22–26 ustawy policyjnej oraz zgodnie z § 43, w porozumieniu z właścicielem biznesowym systemu teleinformatycznego służącego do przetwarzania danych osobowych;
12) zapewniają właściwe i niezwłoczne włączanie IOD MF we wszystkie sprawy dotyczące ochrony danych osobowych objętych Polityką – począwszy od etapu ich projektowania oraz analizowania ryzyka dla ochrony danych osobowych, przez ich realizację, wdrożenie, aż do usunięcia danych osobowych;
13) zgłaszają zdarzenia mogące stanowić naruszenie ochrony danych osobowych, zgodnie z procedurą zarządzania incydentami, i uczestniczą w czynnościach wyjaśniających;
14) zawiadamiają, w uzgodnieniu z IOD MF, osoby których dane zostały dotknięte naruszeniem ochrony danych osobowych, zgodnie z procedurą, o której mowa w pkt 13;
15) przekazują DB dokumentację i niezbędne wyjaśnienia na potrzeby kontroli zewnętrznych dotyczących ochrony danych osobowych;
16) przekazują DB i IOD MF informacje o planowanych kontrolach zewnętrznych dotyczących ochrony danych osobowych objętych Polityką, w szczególności kontrolach prowadzonych przez Prezesa UODO;
17) wyznaczają koordynatora do spraw ochrony danych osobowych odpowiednio w KIS lub w KSS i umożliwiają mu wykonywanie jego zadań, w szczególności przez bieżący dostęp do informacji o działaniach odpowiednio KIS lub KSS.

§ 12. Dyrektor CI RF, w odniesieniu do danych osobowych, o których mowa w § 3 ust. 1, przetwarzanych przez CI RF:

1) sprawuje nadzór nad przetwarzaniem i ochroną danych osobowych w celu zapewnienia zgodności ich przetwarzania z przepisami prawa i Polityką;
2) zarządza ryzykiem związanym z przetwarzaniem danych osobowych, zgodnie z procedurą zarządzania ryzykiem, w tym dokonywania analizy ryzyka;
3) udziela i cofa upoważnienia do przetwarzania danych osobowych, zgodnie z § 20, pracownikom CI RF;
4) prowadzi ewidencję wydanych zgodnie z § 20 upoważnień do przetwarzania danych osobowych;
5) bierze udział, na wniosek właściciela biznesowego systemu teleinformatycznego, dyrektora komórki organizacyjnej w Ministerstwie właściwej do spraw informatyzacji lub dyrektora IAS, w weryfikacji podmiotu przed zawarciem umowy powierzenia przetwarzania danych osobowych;
6) bierze udział, w uzasadnionych przypadkach, w audytach i inspekcjach związanych z powierzeniem przetwarzania danych osobowych podmiotom zewnętrznym;

7) dokonuje przeglądu i usuwa dane osobowe zgodnie z procedurą przeglądu i usuwania danych osobowych;
8) realizuje prawa osób, których dane dotyczą, na podstawie art. 15–21 RODO lub art. 22–26 ustawy policyjnej oraz zgodnie z § 43, na polecenie właściciela biznesowego systemu teleinformatycznego służącego do przetwarzania danych osobowych;
9) bierze udział w dokonywaniu, na wniosek komórki organizacyjnej w Ministerstwie, oceny skutków dla ochrony danych w odniesieniu do operacji przetwarzania, na podstawie art. 35 RODO lub art. 37 ustawy policyjnej;
10) zgłasza zdarzenia mogące stanowić naruszenie ochrony danych osobowych, zgodnie z procedurą zarządzania incydentami, i uczestniczy w czynnościach wyjaśniających;
11) przekazuje DB dokumentację i niezbędne wyjaśnienia na potrzeby kontroli zewnętrznych dotyczących ochrony danych osobowych;
12) przekazuje DB i IOD MF informacje o planowanych kontrolach zewnętrznych dotyczących ochrony danych osobowych objętych Polityką, w szczególności kontrolach prowadzonych przez Prezesa UODO;
13) wyznacza koordynatora do spraw ochrony danych osobowych w CI RF i umożliwia mu wykonywanie jego zadań, w szczególności przez bieżący dostęp do informacji o działaniach CI RF.

§ 13. Do zadań IOD MF należy:

1) informowanie Administratora oraz osób upoważnionych do przetwarzania danych osobowych o obowiązkach spoczywających na nich na mocy RODO, ustawy policyjnej oraz innych przepisów powszechnie obowiązujących o ochronie danych osobowych;
2) opiniowanie i doradzanie w sprawach dotyczących bezpośrednio lub pośrednio ochrony danych osobowych;
3) opiniowanie rozwiązań organizacyjnych pod kątem właściwego wdrażania systemu ochrony danych osobowych;
4) monitorowanie zgodności przetwarzania danych osobowych z RODO, ustawą policyjną, innymi przepisami powszechnie obowiązującymi dotyczącymi ochrony danych osobowych, a także z Polityką, w tym prowadzenie audytów i sprawdzeń;
5) udział, na wniosek komórki organizacyjnej w Ministerstwie, IAS lub z własnej inicjatywy, w weryfikacji podmiotu przed zawarciem umowy powierzenia przetwarzania danych osobowych;
6) udział, w uzasadnionych przypadkach, w audytach i kontrolach związanych z powierzeniem przetwarzania danych osobowych podmiotom zewnętrznym;

7) prowadzenie działań zwiększających świadomość w zakresie ochrony danych osobowych, w tym, we współpracy z komórką organizacyjną w Ministerstwie właściwą do spraw szkoleń, organizacja szkoleń i instruktaży dla osób upoważnionych do przetwarzania danych osobowych;
8) udzielanie zaleceń co do oceny skutków dla ochrony danych osobowych oraz monitorowanie wykonania tej oceny;
9) współpraca z Prezesem UODO, w tym pełnienie funkcji punktu kontaktowego dla Prezesa UODO w kwestiach związanych z przetwarzaniem danych osobowych, a także prowadzenie, zgodnie z art. 39 ust. 1 lit. e RODO oraz art. 47 ust. 1 pkt 7 ustawy policyjnej, konsultacji we wszelkich innych sprawach, w szczególności pełnienie funkcji punktu kontaktowego w związku z prowadzonymi przez Administratora uprzednimi konsultacjami w rozumieniu art. 36 RODO i art. 38 ustawy policyjnej oraz w stosownych przypadkach przedstawianie Prezesowi UODO stanu realizacji zaleceń przedstawionych w procesie uprzednich konsultacji w rozumieniu ustawy policyjnej oraz – za pośrednictwem Administratora – sprawozdania z przeprowadzonego sprawdzenia w rozumieniu ustawy policyjnej;
10) pełnienie funkcji punktu kontaktowego dla osób, których dane osobowe dotyczą;
11) uczestniczenie w kontrolach zewnętrznych dotyczących ochrony danych osobowych;
12) udział w postępowaniach wyjaśniających w zakresie podejrzenia naruszenia ochrony danych osobowych, prowadzonych zgodnie z procedurą zarządzania incydentami;
13) okresowe informowanie Administratora lub osoby przez niego wskazanej o przypadkach naruszenia ochrony danych osobowych;
14) opiniowanie regulacji dotyczących analizy ryzyka i sposobu wdrożenia tych regulacji pod kątem właściwego uwzględnienia ryzyka dotyczącego ochrony danych osobowych;
15) sporządzanie i przekazywanie Administratorowi rocznego sprawozdania z wykonywania zadań z zakresu ochrony i sposobu przetwarzania danych osobowych, zgodnie z ustawą policyjną;
16) okresowe raportowanie do Administratora o najważniejszych wynikach weryfikacji zgodności przetwarzania danych osobowych z przepisami;
17) opiniowanie odstępstw od wymagań technicznych lub organizacyjnych w odniesieniu do systemów teleinformatycznych służących do przetwarzania danych osobowych.

§ 14. Każdy pracownik jest obowiązany do należytego przestrzegania zasad ochrony danych osobowych określonych w RODO, ustawie policyjnej – jeśli ma zastosowanie, oraz w Polityce, w szczególności do:

1) przetwarzania danych osobowych w zakresie swojego upoważnienia i zgodnie z celami przetwarzania;

2) przestrzegania zasad bezpieczeństwa dotyczących eksploatacji systemów teleinformatycznych i ochrony antywirusowej, określonych w PBT, a także korzystania z systemów teleinformatycznych służących do przetwarzania danych osobowych wyłącznie zgodnie z ich przeznaczeniem i w zakresie swoich zadań, a także do ochrony przed nieupoważnionym dostępem do tych systemów;
3) informowania przełożonego o wszelkich zauważonych nieprawidłowościach i zdarzeniach skutkujących lub mogących skutkować obniżeniem poziomu ochrony danych osobowych;
4) zgłaszania zdarzeń mogących stanowić naruszenie ochrony danych osobowych, zgodnie z procedurą zarządzania incydentami i uczestniczenia w czynnościach wyjaśniających;
5) zapewnienia poufności przetwarzanych danych osobowych oraz poufności sposobów zabezpieczenia danych osobowych, w trakcie wykonywania powierzonych zadań i po ich zakończeniu, w tym zapewnienia ochrony danych osobowych przed nieuprawnionym dostępem (w tym fizycznym), nieuzasadnioną modyfikacją, zniszczeniem, ujawnieniem lub pozyskaniem danych;
6) zapoznania się z Polityką i potwierdzenia tego w formie pisemnej.

§ 15. 1. Do zadań koordynatora do spraw ochrony danych osobowych w komórce organizacyjnej w Ministerstwie należy:

1) bieżąca współpraca z IOD MF oraz DB w zakresie stosowania zasad ochrony danych osobowych, określonych w Polityce;
2) wspieranie pracowników komórki organizacyjnej w Ministerstwie w uwzględnianiu zasad ochrony danych osobowych w realizowanych czynnościach przetwarzania, w szczególności w fazie projektowania oraz – w razie konieczności – w realizacji obowiązku zawarcia umowy powierzenia przetwarzania danych osobowych, a także w innych kwestiach związanych z ochroną danych osobowych;
3) prowadzenie, w przypadku takiego uzgodnienia z IOD MF, szkoleń wstępnych w zakresie ochrony danych osobowych dla pracowników komórki organizacyjnej w Ministerstwie;
4) przekazywanie pracownikom komórki organizacyjnej w Ministerstwie zaleceń IOD MF;
5) przekazywanie IOD MF niezbędnych informacji dotyczących operacji przetwarzania danych osobowych dokonywanych w ramach właściwości komórki organizacyjnej w Ministerstwie, w tym realizowanych w systemach teleinformatycznych służących do przetwarzania danych osobowych, zarówno na żądanie IOD, jak i z własnej inicjatywy na bieżąco;
6) koordynowanie wprowadzania i aktualizowania czynności przetwarzania w rejestrach, o których mowa w § 8 pkt 4 i 5;

7) uczestnictwo w okresowych szkoleniach, spotkaniach i warsztatach dotyczących ochrony danych osobowych;
8) udzielanie pomocy DB i IOD MF w wyjaśnianiu naruszeń ochrony danych osobowych w zakresie działania komórki organizacyjnej w Ministerstwie;
9) przekazywanie pracownikom informacji oraz koordynowanie zadań zainicjowanych przez IOD MF lub przez DB.

2. Do zadań koordynatora do spraw ochrony danych osobowych w IAS należy:

1) bieżąca współpraca z IOD MF oraz DB w zakresie stosowania zasad ochrony danych osobowych, określonych w Polityce;
2) wspieranie pracowników IAS, a także koordynatorów do spraw ochrony danych osobowych w US i UCS, w uwzględnianiu zasad ochrony danych osobowych w realizowanych czynnościach przetwarzania, w szczególności w fazie projektowania oraz – w razie konieczności – w realizacji obowiązku zawarcia umowy powierzenia przetwarzania danych osobowych;
3) prowadzenie, lub koordynowanie prowadzenia, w uzgodnieniu z IOD MF szkoleń wstępnych w zakresie ochrony danych osobowych dla pracowników IAS, podległych US oraz UCS;
4) przekazywanie pracownikom IAS, a także koordynatorom do spraw ochrony danych osobowych w US i UCS, zaleceń IOD MF;
5) przekazywanie IOD MF niezbędnych informacji dotyczących operacji przetwarzania danych osobowych dokonywanych w ramach właściwości IAS, podległych US oraz UCS, w tym realizowanych w systemach teleinformatycznych służących do przetwarzania danych osobowych;
6) przekazywanie na żądanie DB raportów dotyczących naruszeń, które wystąpiły w IAS oraz podległych US i UCS;
7) uczestnictwo w okresowych szkoleniach, spotkaniach i warsztatach dotyczących ochrony danych osobowych;
8) udzielanie pomocy DB i IOD MF w wyjaśnianiu naruszeń ochrony danych osobowych w zakresie działania IAS, podległych US oraz UCS;
9) przekazywanie pracownikom IAS, podległych US oraz UCS, w szczególności koordynatorom do spraw ochrony danych osobowych w US i UCS, informacji oraz koordynowanie realizacji zadań zainicjowanych przez IOD MF lub przez DB.

3. Do zadań koordynatora do spraw ochrony danych osobowych w US lub UCS należy:

1) bieżąca współpraca z koordynatorem do spraw ochrony danych osobowych w IAS w zakresie stosowania zasad ochrony danych osobowych, określonych w Polityce;
2) wspieranie pracowników US lub UCS w uwzględnianiu zasad ochrony danych osobowych w realizowanych czynnościach przetwarzania;

3) prowadzenie w uzgodnieniu z koordynatorem do spraw ochrony danych osobowych w IAS szkoleń wstępnych w zakresie ochrony danych osobowych dla pracowników odpowiednio US lub UCS;
4) przekazywanie pracownikom US lub UCS zaleceń przekazywanych przez IOD MF lub koordynatora do spraw ochrony danych osobowych w IAS;
5) przekazywanie IOD MF lub koordynatorowi do spraw ochrony danych osobowych w IAS niezbędnych informacji dotyczących operacji przetwarzania danych osobowych dokonywanych w ramach właściwości US lub UCS, w tym realizowanych w systemach teleinformatycznych służących do przetwarzania danych osobowych;
6) przekazywanie na żądanie koordynatora do spraw ochrony danych osobowych w IAS raportów dotyczących naruszeń, które wystąpiły w US lub UCS;
7) uczestnictwo w okresowych szkoleniach, spotkaniach i warsztatach dotyczących ochrony danych osobowych;
8) udzielanie pomocy DB i IOD MF w wyjaśnianiu naruszeń ochrony danych osobowych w zakresie działania US lub UCS;
9) przekazywanie pracownikom informacji oraz koordynowanie zadań zainicjowanych przez IOD MF, DB lub koordynatora do spraw ochrony danych osobowych w IAS.

4. Do zadań koordynatora do spraw ochrony danych osobowych w KIS, KSS i CI RF należy:

1) bieżąca współpraca z IOD MF oraz DB w zakresie stosowania zasad ochrony danych osobowych, określonych w Polityce;
2) wspieranie pracowników Jednostki w uwzględnianiu zasad ochrony danych osobowych w realizowanych czynnościach przetwarzania, w szczególności w fazie projektowania oraz – w razie konieczności – w realizacji obowiązku zawarcia umowy powierzenia przetwarzania danych osobowych;
3) prowadzenie w uzgodnieniu z IOD MF szkoleń wstępnych w zakresie ochrony danych osobowych dla pracowników Jednostki;
4) doradzanie pracownikom Jednostki, w zakresie ochrony danych osobowych zgodnie z Polityką i zaleceniami przekazywanymi przez IOD MF;
5) przekazywanie IOD MF niezbędnych informacji dotyczących operacji przetwarzania danych osobowych dokonywanych w ramach właściwości Jednostki, w tym realizowanych w systemach teleinformatycznych służących do przetwarzania danych osobowych;
6) przekazywanie na żądanie DB raportów dotyczących naruszeń, które wystąpiły w Jednostce;
7) uczestnictwo w okresowych szkoleniach, spotkaniach i warsztatach dotyczących ochrony danych osobowych;

8) udzielanie pomocy DB i IOD MF w wyjaśnianiu naruszeń ochrony danych osobowych w zakresie działania Jednostki;
9) przekazywanie pracownikom informacji oraz koordynowanie zadań zainicjowanych przez IOD MF lub przez DB.

§ 16. Do zadań koordynatora merytorycznego systemu teleinformatycznego służącego do przetwarzania danych osobowych należy koordynacja zadań właściciela biznesowego systemu teleinformatycznego, określonych w § 27 ust. 1 pkt 7 regulaminu organizacyjnego Ministerstwa oraz:
1) zarządzanie ryzykiem związanym z przetwarzaniem danych osobowych w systemie teleinformatycznym, zgodnie z procedurą zarządzania ryzykiem;
2) udzielanie wsparcia w zakresie znajomości funkcjonalności systemu;
3) zapewnienie zgodności systemu teleinformatycznego z wymaganiami wynikającymi z Polityki oraz przywołanych w niej dokumentów, w tym polityk szczegółowych, procedur i instrukcji dotyczących systemów teleinformatycznych oraz ochrony danych osobowych;
4) zarządzanie procesem nadawania, modyfikacji i odbierania uprawnień, zgodnie z procedurą zarządzania uprawnieniami w systemach teleinformatycznych służących do przetwarzania danych osobowych;
5) inicjowanie działań mających na celu rozwój systemu teleinformatycznego;
6) współpraca z IOD MF w zakresie ochrony danych osobowych w systemie teleinformatycznym.

§ 17. Do zadań Administratora Systemu Informatycznego (ASI), w zakresie systemu teleinformatycznego służącego do przetwarzania danych osobowych, należy w szczególności:
1) zabezpieczenie systemu teleinformatycznego, zgodnie z wymaganiami określonymi w PBT oraz wytycznymi przekazanymi przez DB, a także koordynacja działań związanych z poprawnym funkcjonowaniem tego systemu;
2) współpraca z właścicielem biznesowym w zakresie analizy ryzyka w odniesieniu do przetwarzania danych osobowych w systemie teleinformatycznym;
3) informowanie, zgodnie z procedurą zarządzania incydentami, o wszelkich incydentach lub anomaliach związanych z systemem teleinformatycznym służącym do przetwarzania danych osobowych;
4) w przypadku otrzymania informacji o naruszeniu lub podejrzeniu naruszenia zabezpieczeń podejmowanie natychmiastowych działań mających na celu zabezpieczenie stanu systemu teleinformatycznego, przeciwdziałanie skutkom naruszenia oraz podejmowanie działań związanych z wdrożeniem zabezpieczeń w systemie, a także współpraca z IOD MF oraz DB w ramach czynności wyjaśniających naruszenia;

5) nadzór nad funkcjonowaniem zabezpieczeń dotyczących przesyłania danych osobowych drogą teletransmisji;
6) realizacja zadań wynikających z procedury wykonywania i zarządzania kopiami zapasowymi;
7) wykonywanie zadań AZU, jeśli AZU nie został wyznaczony odrębnie.

§ 18. Do zadań Administratora Zarządzającego Uprawnieniami (AZU) należy:
1) nadawanie, modyfikacja lub odbieranie uprawnień w systemie teleinformatycznym służącym do przetwarzania danych osobowych;
2) zapewnienie ewidencjonowania wniosków o nadanie, modyfikację lub odebranie uprawnień, w systemie, o którym mowa w ust. 1, o ile wnioskowanie nie odbywa się za pośrednictwem dedykowanego systemu teleinformatycznego;
3) przeprowadzanie okresowych i doraźnych przeglądów kont i uprawnień użytkowników w systemie teleinformatycznym, o którym mowa w ust. 1, zgodnie z procedurą zarządzania uprawnieniami.

Rozdział 3

Dopuszczanie osób do przetwarzania danych osobowych

§ 19. 1. Dostęp do danych osobowych mają wyłącznie osoby upoważnione do przetwarzania danych osobowych w odpowiednim zakresie.

2. Administrator upoważnia Sekretarzy Stanu w Ministerstwie, Podsekretarzy Stanu w Ministerstwie, Dyrektora Generalnego Ministerstwa, dyrektorów komórek organizacyjnych w Ministerstwie, dyrektorów IAS do przetwarzania danych osobowych objętych Polityką, w zakresie wynikającym z realizacji powierzonych zadań.

3. Administrator upoważnia Naczelników US i UCS do przetwarzania danych osobowych objętych Polityką, w zakresie wynikającym z realizacji powierzonych zadań.

§ 20. 1. Upoważnienia wydawane są w formie pisemnej albo elektronicznej.

2. Za prowadzenie ewidencji wydanych upoważnień odpowiadają osoby upoważnione do ich wydawania.

3. Ewidencja zawiera:
1) wskazanie administratora;
2) imię i nazwisko osoby upoważnionej;
3) identyfikator - login domenowy albo – w przypadku jego braku – inny niepowtarzalny numer lub symbol;
4) zakres upoważnienia;

5) daty obowiązywania upoważnień – data początkowa oraz data końcowa obowiązywania upoważnienia.

4. Szczegółową procedurę dot. nadawania i cofania upoważnień, wzory upoważnień, a także sposób ich ewidencjonowania określa dyrektor DB w Procedurze zarządzania upoważnieniami do przetwarzania danych osobowych.

5. Nie rzadziej niż raz do roku dyrektor, o którym mowa w § 7, § 9, § 11 i § 12 lub naczelnik, o którym mowa w § 10, dokonuje analizy poprawności prowadzonej ewidencji, a także analizy wydanych upoważnień pod kątem ich aktualności oraz prawidłowości ich zakresu. W przypadku stwierdzenia nieaktualności lub błędów w ewidencji, dyrektor lub naczelnik poprawia dane zawarte w ewidencji, a w przypadku stwierdzenia braku upoważnień lub niewłaściwego ich zakresu – nadaje upoważnienia lub je cofa. Przeprowadzenie analizy i jej wyników dyrektor lub naczelnik odpowiednio odnotowuje.

6. Analiza obejmuje także przegląd uprawnień w systemach teleinformatycznych służących do przetwarzania danych osobowych.

Rozdział 4

Zasady przetwarzania danych osobowych

Zgodność z prawem

§ 21. 1. Dane osobowe (tzw. zwykłe) mogą być przetwarzane, o ile spełniony jest jeden z warunków zawartych w art. 6 ust. 1 RODO, art. 10 RODO lub art. 13 ustawy policyjnej:

1) przetwarzanie jest niezbędne do wypełnienia przez Administratora obowiązku wynikającego z przepisów (art. 6 ust. 1 lit. c RODO);
2) przetwarzanie jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów (art. 13 ust. 1 ustawy policyjnej);
3) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi (art. 6 ust. 1 lit. e RODO – stosowany, kiedy nie ma wyraźnego przepisu prawa, ale może być wykazany interes publiczny lub sprawowanie władzy publicznej w odpowiednim zakresie, wynikającym z przepisów);
4) przetwarzanie jest niezbędne do wykonania umowy z osobą, która jest jej stroną, lub w celu zawarcia takiej umowy (art. 6 ust. 1 lit. b RODO);
5) przetwarzanie jest niezbędne do celów, które wynikają z prawnie uzasadnionych interesów realizowanych przez Administratora (art. 6 ust. 1 lit. f RODO – przesłanki tej nie można stosować, kiedy Administrator wykonuje zadania organu);

6) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (art. 6 ust. 1 lit. d RODO).

2. Dane szczególnych kategorii (tzw. dane wrażliwe) mogą być przetwarzane, o ile spełniony jest jeden z warunków zawartych w art. 9 ust. 2 RODO lub art. 14 ustawy policyjnej:

1) przepisy prawa pozwalają na przetwarzanie takich danych (art. 14 ust. 2 pkt 1 ustawy policyjnej);
2) przetwarzanie jest niezbędne dla ochrony życia lub zdrowia lub interesów osoby, której dane dotyczą lub innej osoby (art. 14 ust. 2 pkt 2 ustawy policyjnej lub art. 9 ust. 2 lit. c RODO, przy czym w przypadku przesłanki opartej o przepis RODO, dodatkowo musi być spełniony warunek, że osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody);
3) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone przepisami prawa (art. 9 ust. 2 lit. b RODO);
4) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, na podstawie przepisów prawa (art. 9 ust. 2 lit. h RODO);
5) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym i odbywa się na podstawie przepisów spełniających warunki określone w art. 9 ust. 2 lit. g RODO;
6) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń (art. 9 ust. 2 lit. f RODO);
7) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, na podstawie przepisów prawa (art. 9 ust. 2 lit. i RODO);
8) dane zostały upublicznione przez osobę, której dotyczą (art. 14 ust. 2 pkt 3 ustawy policyjnej oraz art. 9 ust. 2 lit. e RODO);
9) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych (art. 9 ust. 2 lit. j RODO).

3. W przypadku, gdy przetwarzanie danych osobowych (zwykłych lub wrażliwych) nie może być oparte na jednej z przesłanek legalności, określonych w ust. 1 lub 2, podstawą przetwarzania danych osobowych może być zgoda osoby, której dane dotyczą (art. 6 ust. 1 lit. a RODO lub art. 9 ust. 2 lit. a RODO).

4. Każdy pracownik odbierający zgodę osoby, której dane dotyczą, tworzy warunki, aby zgoda była udzielona dobrowolnie, świadomie i wobec konkretnego celu, a także w przypadku, kiedy zgoda nie jest składana na piśmie, dokumentuje, w szczególności adnotacją, czy była złożona przez oświadczenie czy wyraźne działanie osoby, której dane dotyczą, potwierdzające przyzwolenie na

przetwarzanie dotyczących jej danych osobowych. Zgoda na przetwarzanie danych wrażliwych musi być wyrażona na piśmie.

5. Ministerstwo lub Jednostka przetwarzająca dane osobowe na podstawie zgody, zapewnia – przed wyrażeniem zgody przez osobę, której dane dotyczą – poinformowanie jej, że zgoda może być cofnięta w każdym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

6. W przypadku cofnięcia zgody przez osobę, której dane dotyczą, Ministerstwo lub Jednostka niezwłocznie podejmuje czynności zmierzające do zaprzestania dalszego przetwarzania danych osobowych, dokonywanego w oparciu o przesłankę zgody.

7. Dane osobowe dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa mogą być przetwarzane, na podstawie przesłanek zawartych w art. 6 ust. 1 RODO, na podstawie przepisów prawa.

8. Przetwarzanie danych osobowych, które nie spełnia warunku określonego w ust. 1–3, stanowi naruszenie ochrony danych osobowych.

Zasada rzetelności i przejrzystości

§ 22. 1. Osoby przetwarzające dane osobowe dbają, aby zachowana była zasada rzetelności i przejrzystości dla osoby, której dane dotyczą.

2. Jednym ze sposobów realizacji zasady przejrzystości jest sposób realizacji obowiązków informacyjnych, które zostały określone w § 43.

3. Zasada przejrzystości nie jest stosowana w przypadku przetwarzania danych przez organy KAS na podstawie przepisów ustawy policyjnej, jeśli przepis prawa pozwala przetwarzać dane osobowe bez wiedzy osoby, której dane dotyczą.

Zasada ograniczenia celów przetwarzania danych osobowych

§ 23. 1. Osoby odpowiedzialne za przetwarzanie danych osobowych dbają o to, aby były one przetwarzane w konkretnych, wyraźnych i prawnie uzasadnionych celach, określonych w momencie ich zbierania.

2. Przetwarzanie w innym celu, niż cel pierwotny, jest możliwe tylko w sytuacji, kiedy zmiana celu ma uzasadnienie i podstawy prawne, a także kiedy zostanie zrealizowany obowiązek informacyjny przed dalszym przetwarzaniem. Obowiązek informacyjny nie musi być realizowany, jeśli istnieją przesłanki zwalniające z obowiązku informacyjnego.

3. Dalsze przetwarzanie danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami przetwarzania.

4. Dopuszczalne jest dalsze przetwarzanie danych osobowych, które są niezbędne do ustalenia, dochodzenia lub obrony roszczeń.

5. Przetwarzanie danych osobowych w innych celach, niż te dla których zostały zebrane, jest dopuszczalne na podstawie przepisów art. 13 ust. 2 ustawy policyjnej oraz art. 52b ustawy o KAS.

Zasada minimalizacji danych osobowych

§ 24. 1. Osoby odpowiedzialne za przetwarzanie danych osobowych dbają o to, aby były one przetwarzane w sposób adekwatny, stosowny i ograniczony do tego, co jest niezbędne do celów, dla których są one przetwarzane.

2. Zabronione jest zbieranie danych osobowych nadmiarowych i nieistotnych dla realizacji celu oraz o większym stopniu szczegółowości, niż wynika to z oznaczonego celu.

3. Osoby odpowiedzialne za prowadzenie procesu legislacyjnego stosują zasadę minimalizacji danych osobowych, oceniając zakres danych, które mają być przetwarzane na podstawie projektowanego aktu prawnego.

Prawidłowość danych osobowych

§ 25. 1. Właściciel biznesowy danych dąży do tego, aby przetwarzane dane osobowe były prawidłowe i w razie potrzeby uaktualniane.

2. Jeżeli cele przetwarzania nie zostały jeszcze zrealizowane, a dane osobowe są nieprawidłowe, muszą być niezwłocznie usunięte, sprostowane lub uzupełnione, dokonując odpowiedniej adnotacji.

3. Jeżeli osoba, której dane osobowe dotyczą, wystąpi o sprostowanie lub uzupełnienie danych, a właściciel biznesowy danych, po sprawdzeniu tożsamości osoby wnioskującej lub na podstawie przekazanego lub udostępnionego dokumentu, stwierdzi nieprawidłowość danych, niezwłocznie dokonuje sprostowania lub uzupełnienia, zapewniając odnotowanie daty i treści sprostowania lub uzupełnienia.

4. Jeżeli nieprawidłowość lub nieaktualność danych zostanie stwierdzona z urzędu, właściciel biznesowy danych, poprawia je lub uaktualnia, chyba że przepisy szczególne przewidują inny tryb postępowania.

5. Prawidłowość danych osobowych, przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, jest zapewniona zgodnie z art. 24–25 i art. 28 ustawy policyjnej.

Zasada czasowego ograniczenia przechowywania

§ 26. 1. Właściciel biznesowy danych zapewnia, aby dane osobowe były przechowywane w formie umożliwiającej identyfikację osoby, której dane osobowe dotyczą, przez okres nie dłuższy,

niż jest to niezbędne do celów, w których dane te są przetwarzane, zgodnie z procedurą przeglądu i usuwania danych osobowych.

2. Dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych, w komórce organizacyjnej odpowiednio w Ministerstwie albo Jednostce, która prowadzi sprawę, przez okres określony w instrukcji kancelaryjnej. Następnie sprawa jest przekazywana do archiwum zakładowego.

3. Archiwizowanie danych osobowych wykonuje się zgodnie z obowiązującym odpowiednio w Ministerstwie albo Jednostce jednolitym rzeczowym wykazem akt, instrukcją kancelaryjną określającą zasady i tryb postępowania z dokumentacją oraz instrukcją w sprawie organizacji i zakresu działania archiwum zakładowego.

4. Właściciel biznesowy danych weryfikuje dane osobowe przetwarzane w celu realizacji ustawowych zadań realizowanych przez organy KAS, nie rzadziej niż co 5 lat od dnia ich uzyskania, zgodnie z art. 127 ust. 5 ustawy o KAS. Dane zbędne właściciel biznesowy danych niezwłocznie usuwa, zgodnie z procedurą, o której mowa w ust. 1.

5. Organy KAS, z wyłączeniem wskazanych w art. 11 ust. 1 pkt 1 i 2 ustawy o KAS, są obowiązane do opracowania procedury przeglądu i usuwania danych osobowych, o których mowa w ust. 5, przetwarzanych w postaci papierowej oraz w systemach teleinformatycznych, które nie wchodzą w skład centralnej infrastruktury teleinformatycznej.

6. Procedurę, o której mowa w ust. 5, przetwarzanych w systemach teleinformatycznych wchodzących w skład centralnej infrastruktury teleinformatycznej, opracowuje właściciel biznesowy systemu teleinformatycznego, w którym te dane są przetwarzane.

Zasada zachowania poufności i integralności

§ 27. 1. Właściciel biznesowy danych zapewnia, aby w procesie przetwarzania danych osobowych była zapewniona ich poufność. Oznacza to, że dane te mogą być udostępniane wyłącznie osobom upoważnionym i uprawnionym do dostępu do nich, tylko w zakresie niezbędnym do realizacji zadań. Jeśli dane mają być przekazane lub powierzone innemu podmiotowi, właściciel biznesowy danych realizuje to wyłącznie w przypadkach przewidzianych przepisami prawa.

2. Właściciel biznesowy danych zapewnia, aby w procesie przetwarzania danych osobowych była zapewniona ich integralność. Oznacza to, że dane nie mogą być zmodyfikowane w sposób nieuprawniony.

3. Właściciel biznesowy danych zapewnia ich ochronę za pomocą środków technicznych i organizacyjnych, o których mowa w § 5 i § 6, zastosowanych odpowiednio do przeprowadzonej oceny ryzyka, w szczególności przed:

1) przetwarzaniem niedozwolonym lub niezgodnym z prawem;
2) przypadkową utratą, zniszczeniem, uszkodzeniem lub nieuprawnioną modyfikacją;
3) nieuprawnionym wykorzystaniem, w tym przekazaniem osobie nieuprawnionej.

Zasada rozliczalności

§ 28. 1. Właściciel biznesowy danych zapewnia stosowanie zasady rozliczalności, która polega na zapewnieniu możliwości udokumentowania, że dane osobowe są przetwarzane zgodnie z zasadami określonymi w § 21–30, bez względu na formę i sposób ich przetwarzania, w szczególności przez wskazanie wdrożonych środków organizacyjnych i technicznych, w kontekście konkretnego przetwarzania danych osobowych.

2. Udokumentowanie, o którym mowa w ust. 1, może nastąpić w dowolnej formie.

Zasada uwzględniania ochrony danych osobowych w fazie projektowania

§ 29. 1. We wszelkich działaniach zmierzających do przetwarzania danych osobowych, począwszy od etapu planowania, właściciel biznesowy danych uwzględnia konieczność zapewnienia ich ochrony, biorąc pod uwagę:

1) stan wiedzy technicznej;
2) koszt wdrożenia zabezpieczeń;
3) charakter, zakres, kontekst i cele przetwarzania;
4) ryzyko naruszenia praw lub wolności osób fizycznych.

2. Przy tworzeniu lub modyfikacji systemów teleinformatycznych służących do przetwarzania danych osobowych, a także innych rozwiązań wspierających czynności przetwarzania danych osobowych, właściciel biznesowy systemu teleinformatycznego odpowiada za uwzględnienie ochrony danych osobowych – od fazy koncepcyjnej – zarówno w architekturze systemu, jak i w procesach biznesowych, które są przez ten system obsługiwane.

3. Środki służące realizacji zasady uwzględniania ochrony danych osobowych w fazie projektowania polegają między innymi na:

1) minimalizacji zakresu przetwarzanych danych osobowych;
2) minimalizacji okresu przetwarzania danych osobowych;
3) pseudonimizacji danych osobowych;
4) umożliwieniu zapewnienia realizacji praw osób, których dane dotyczą;
5) zaplanowaniu i wdrożeniu zabezpieczeń w celu spełnienia zasad ochrony danych osobowych, określonych w Polityce.

4. Właściciel biznesowy danych realizuje tę zasadę na etapie przygotowywania dokumentacji we wszystkich zamówieniach publicznych, które przewidują przetwarzanie danych osobowych.

Zasada domyślnej ochrony danych

§ 30. 1. Właściciel biznesowy danych stosuje zasadę domyślnej ochrony danych, która polega na tym, że dopuszczalne jest przetwarzanie wyłącznie tych danych osobowych, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania. Obowiązek ten odnosi się do zakresu zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności.

2. Właściciel biznesowy systemu teleinformatycznego zapewnia, aby każdy system, aplikacja czy proces domyślnie zapewniał najwyższą ochronę danych osobowych oraz żeby zmniejszenie ochrony było możliwe jedynie na wyraźne żądanie użytkownika tego systemu, aplikacji, czy procesu.

Anonimizacja

§ 31. 1. W przypadku, gdy nie ma już potrzeby dalszego przetwarzania danych osobowych, a dane są potrzebne do prowadzenia prac analitycznych, statystycznych lub testowych, właściciel biznesowy danych zapewnia anonimizację danych osobowych, polegającą na nieodwracalnym ich usunięciu lub takiej ich modyfikacji, która uniemożliwi identyfikację osoby fizycznej.

2. Za prawidłową anonimizację dokumentu, wykonaną w odpowiednim momencie przetwarzania danych osobowych, w szczególności przed ich udostępnieniem, niezależnie od postaci danych, elektronicznej czy papierowej, jest odpowiedzialny pracownik prowadzący sprawę oraz jego bezpośredni przełożony. DB publikuje w intranecie instrukcję anonimizowania dokumentów.

Pseudonimizacja

§ 32. W celu zabezpieczenia danych osobowych, które będą potrzebne do późniejszego wykorzystania, przed nieuprawnionym ujawnieniem, właściciel biznesowy danych stosuje pseudonimizację, polegającą na przetworzeniu danych osobowych w taki sposób, by nie była możliwa identyfikacja osoby fizycznej, bez użycia dodatkowych informacji (np. klucza pseudonimizacyjnego). Te dodatkowe informacje właściciel biznesowy danych przechowuje osobno, zabezpieczając je technicznie i organizacyjnie przed nieuprawnionym użyciem mającym na celu odwrócenia procesu pseudonimizacji.

Rozdział 5

Obszar przetwarzania danych osobowych

§ 33. 1. Obszar przetwarzania danych osobowych obejmuje budynki i znajdujące się w nich pomieszczenia, w których przetwarzane są dane osobowe, w tym:

1) miejsca, w których wykonywane są operacje na danych osobowych, realizowane w postaci papierowej lub elektronicznej, w tym w systemach teleinformatycznych;

2) miejsca, w których przechowuje się wszelkie nośniki informacji zawierające dane osobowe, w tym dokumentację papierową, nośniki komputerowe, urządzenia służące do przetwarzania danych osobowych, w tym komputery, serwery, macierze dyskowe;
3) pomieszczenia, gdzie składowane są uszkodzone komputerowe nośniki danych, zawierające dane osobowe.

2. W skład obszaru przetwarzania danych osobowych wchodzą również:
1) budynki i lokale, będące siedzibami podmiotów zewnętrznych związanych z Administratorem umową powierzenia przetwarzania danych osobowych lub innym instrumentem prawnym dotyczącym powierzenia przetwarzania danych osobowych;
2) pojazdy w użytkowaniu KAS przewożące korespondencję między organami KAS;
3) pomieszczenia wykorzystywane przez pracowników do wykonywania pracy w formie telepracy, zgodnie z procedurą dotyczącą wykonywania pracy w formie telepracy;
4) pomieszczenia wykorzystywane przez pracowników do wykonywania pracy w formie pracy zdalnej.

Rozdział 6

Zarządzanie ryzykiem w zakresie ochrony danych osobowych

Ocena ryzyka

§ 34. 1. Zarządzanie ryzykiem odbywa się w ramach kontroli zarządczej oraz w ramach Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z normą ISO 27001, ze szczególnym uwzględnieniem ryzyka dotyczącego danych osobowych.

2. Ocena ryzyka jest prowadzona okresowo, zgodnie z procedurą oceny ryzyka, przez właścicieli biznesowych danych, dla poszczególnych czynności przetwarzania danych osobowych określonych w rejestrze, o którym mowa w § 8 pkt 4, oraz na bieżąco aktualizowana.

3. W przypadku, kiedy dane osobowe są przetwarzane w systemie teleinformatycznym, a właściciel biznesowy danych nie jest jednocześnie właścicielem biznesowym systemu teleinformatycznego, właściciel biznesowy danych prowadzi ocenę ryzyka z uwzględnieniem opinii właściciela biznesowego systemu teleinformatycznego.

Ocena skutków dla ochrony danych osobowych

§ 35. 1. Ocenę skutków dla ochrony danych osobowych przeprowadza się dla:
1) operacji przetwarzania danych osobowych, dla których określono wysokie ryzyko naruszenia praw lub wolności osób fizycznych;

2) operacji wymienionych przez Prezesa UODO w wykazie rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych osobowych.

2. Przeprowadzenie oceny skutków dla ochrony danych osobowych ma na celu ustalenie, czy po uwzględnieniu ryzyk oraz planowanych zabezpieczeń, ryzyko naruszenia praw lub wolności osób fizycznych pozostaje wysokie.

3. W przypadku wykazania wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, mimo zastosowanych zabezpieczeń, przed rozpoczęciem przetwarzania danych osobowych, właściciel biznesowy danych, na podstawie odrębnego upoważnienia, we współpracy z IOD MF, przeprowadza uprzednie konsultacje z Prezesem UODO, zgodnie z art. 36 RODO lub art. 38 ustawy policyjnej.

Rozdział 7

Działania zwiększające świadomość obowiązków dotyczących ochrony danych osobowych

Szkolenia z ochrony danych osobowych

§ 36. 1. Szkolenia z zakresu ochrony danych osobowych są prowadzone przez IOD MF i inne wyznaczone osoby, w formie szkoleń bezpośrednich, z wykorzystaniem technologii informatycznych, w szczególności w formie e-learningu lub w innych formach adekwatnych do celów szkolenia. Dopuszczalne jest również samokształcenie kierowane pod warunkiem zapewnienia możliwości konsultacji niejasnych zagadnień.

2. Zakres, formy i tematykę szkoleń ustala IOD MF lub inne osoby odpowiedzialne za szkolenie pracowników, w porozumieniu z IOD MF.

3. Szkolenia przeprowadzane są dla nowo przyjętych pracowników, a także według potrzeb. W ramach szkolenia nowo przyjęty pracownik jest zobowiązany do zapoznania się z przepisami prawa w zakresie ochrony danych osobowych.

Rozdział 8

Postępowanie w przypadkach naruszenia ochrony danych osobowych oraz innych zdarzeń związanych z bezpieczeństwem danych osobowych

§ 37. 1. Każdy jest zobowiązany zawiadomić o przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych, niezależnie od tego, czy miało ono miejsce w systemie teleinformatycznym służącym do przetwarzania danych osobowych, czy poza systemem, lub o innym zdarzeniu wskazującym na naruszenie ochrony danych osobowych lub mogącym skutkować obniżeniem poziomu ochrony danych osobowych.

2. Sposób i tryb zgłaszania naruszeń oraz proces obsługi naruszeń ochrony danych osobowych uregulowany jest w procedurze zarządzania incydentami.

Rozdział 9

Powierzanie przetwarzania danych osobowych

§ 38. 1. W przypadku wystąpienia potrzeby zapewnienia podmiotowi zewnętrznemu dostępu do danych osobowych, jest wymagane uprzednie:

1) zawarcie odrębnej umowy powierzenia przetwarzania danych osobowych, albo
2) zawarcie stosownych regulacji dotyczących powierzenia przetwarzania danych osobowych w umowie podstawowej, albo
3) zawarcie stosownych regulacji dotyczących powierzenia przetwarzania danych osobowych w innym instrumencie prawnym.

2. W sytuacji, w której Minister Finansów, Funduszy i Polityki Regionalnej, w działach administracji rządowej: budżet, finanse publiczne i instytucje finansowe, działa jako podmiot przetwarzający dane osobowe na rzecz innego podmiotu, odbywa się to na podstawie jednego z instrumentów wymienionych w ust. 1.

3. Tryb i sposób powierzenia danych osobowych reguluje procedura powierzania przetwarzania danych osobowych.

Rozdział 10

Udostępnianie danych

§ 39. 1. Właściciel biznesowy danych udostępnia dane osobowe innym podmiotom lub osobom wyłącznie na podstawie przepisów prawa.

2. W przypadku, kiedy wniosek o udostępnienie danych nie zawiera podstawy prawnej lub zawiera wadliwą podstawę prawną właściciel biznesowy danych wzywa wnioskodawcę do uzupełnienia lub odmawia udostępnienia danych osobowych. W przypadku wniosku osoby fizycznej, właściciel biznesowy danych dokłada starań w celu ustalenia właściwej podstawy prawnej udostępnienia.

3. Właściciel biznesowy danych weryfikuje żądanie udostępnienia danych osobowych, z którym występują organy publiczne, w szczególności pod kątem tego, czy ma formę pisemną, jest uzasadnione, ma charakter wyjątkowy i nie prowadzi do udostępniania wszystkich danych osobowych zawartych w określonym zbiorze lub systemie oraz czy nie prowadzi do łączenia zbiorów danych osobowych.

4. Właściciel biznesowy danych może udostępniać dane osobowe na podstawie wniosku podmiotu w sprawie stałego udostępnienia określonych danych osobowych drogą elektroniczną, zgodnie z przepisami prawa. W takim przypadku zawiera się porozumienie określające podstawy udostępnienia, a także ustalenia techniczne zapewniające współpracę dwóch systemów teleinformatycznych w taki sposób, aby była zapewniona rozliczalność działań oraz wykazanie trybu wnioskowego.

5. Informacje zawierające dane osobowe właściciel biznesowy danych przekazuje uprawnionym podmiotom lub osobom w następujący sposób:

1) w postaci papierowej – przesyłką pocztową;
2) w postaci elektronicznej – za pomocą teletransmisji danych, w postaci zabezpieczonej;
3) w inny sposób – określony konkretnym wymogiem prawnym, umową lub porozumieniem.

§ 40. 1. W celu zapewnienia osobie, której dane dotyczą, dostępu do informacji o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały ujawnione, w tym o odbiorcach w państwach trzecich lub organizacjach międzynarodowych, właściciel biznesowy systemu teleinformatycznego służącego do przetwarzania danych osobowych prowadzi rejestr udostepnień zawierający:

1) imię i nazwisko osoby lub nazwę podmiotu, któremu udostępniono dane osobowe;
2) datę udostępnienia;
3) podstawę prawną udostępnienia;
4) zakres udostępnionych danych osobowych.

2. W rejestrze nie odnotowuje się udostepnień realizowanych w trybie, o którym mowa w § 39 ust. 4.

3. Właściciel biznesowy danych zapewnia odpowiednie rejestrowanie udostępnień, które nie są realizowane w systemach teleinformatycznych.

Rozdział 11

Przekazywanie danych do państw trzecich lub organizacji międzynarodowej

§ 41. 1. Przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić zgodnie z art. 44–46 RODO.

2. W przypadku niespełnienia warunków, o których mowa w ust. 1, przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić wyłącznie zgodnie z art. 49 RODO.

Rozdział 12

Realizacja obowiązków informacyjnych i praw osób, których dane dotyczą

Obowiązki informacyjne

§ 42. 1. Właściciel biznesowy danych odpowiada za realizację obowiązku informacyjnego zgodnie z art. 13 ust. 1 i 2 RODO, chyba że osoba, której dane dotyczą dysponuje już wszystkimi informacjami.

2. Obowiązek, o którym mowa w ust. 1, jest realizowany przez udostępnienie w odpowiedni sposób klauzuli informacyjnej opracowanej na podstawie wzorów klauzul opublikowanych w intranecie przez DB i zaakceptowanej przez IOD MF.

3. Organy KAS, zgodnie z art. 47d ustawy o KAS, mogą realizować obowiązki informacyjne przez umieszczenie klauzul informacyjnych w miejscu publicznie dostępnym w siedzibie organu KAS oraz udostępnienie w Biuletynie Informacji Publicznej na stronie podmiotowej tego organu, pod warunkiem przekazania osobie – podczas pozyskiwania danych osobowych – informacji o miejscu udostępnienia informacji o przetwarzaniu danych osobowych.

4. Klauzule informacyjne zamieszcza się we wszystkich systemach teleinformatycznych służących do przetwarzania danych osobowych, udostępnionych osobom zewnętrznym za pośrednictwem sieci Internet.

5. Obowiązek informacyjny, w ściśle określonych sytuacjach, jest realizowany w innym czasie lub w innym trybie, zgodnie z przepisami szczególnymi, zawartymi np. w ustawie z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2020 r. poz. 256, z późn. zm.).

6. Właściciel biznesowy danych odpowiada za realizację obowiązku informacyjnego obowiązującego w przypadku pozyskiwania danych osobowych w sposób inny niż bezpośrednio od osoby, której dane osobowe dotyczą zgodnie z art. 14 ust. 1–3 RODO, biorąc pod uwagę wyłączenia tego obowiązku przewidziane w art. 14 ust. 5 RODO.

7. Właściciel biznesowy danych odpowiada za realizację obowiązku informacyjnego zgodnie z art. 22 ustawy policyjnej.

§ 43. 1. Właściciel biznesowy danych, w uzgodnieniu z IOD MF, rozpatruje następujące wnioski osób, których dane dotyczą, w zakresie ich praw na podstawie art. 15–21 RODO i art. 22–26 ustawy policyjnej:

1) wniosek o dostęp do danych osobowych;
2) wniosek o sprostowanie danych osobowych;
3) wniosek o usunięcie danych osobowych;
4) wniosek o ograniczenie przetwarzania danych osobowych;
5) wniosek o przeniesienie danych osobowych;
6) wniosek o zrealizowanie prawa do sprzeciwu.

2. Szczegółowe zasady i tryb postępowania z wnioskami, o których mowa w ust. 1, określa dyrektor DB w procedurze rozpatrywania wniosków osób, których dotyczą dane osobowe przetwarzane przez Administratora.

Rozdział 13

Audyt zgodności przetwarzania danych

§ 44. 1. Audyty, kontrole i sprawdzenia prowadzone przez IOD MF w Ministerstwie i Jednostkach dotyczą oceny zgodności przetwarzania danych osobowych z RODO, ustawą policyjną oraz innymi przepisami prawa oraz z wewnętrznymi regulacjami dotyczącymi ochrony danych osobowych, a także oceny realizacji działań naprawczych.

2. W celu realizacji audytów, kontroli i sprawdzeń, o których mowa w ust. 1, IOD MF może korzystać ze wsparcia:

1) DB – komórki właściwej w Ministerstwie do prowadzenia audytów bezpieczeństwa informacji, o których mowa w przepisach o Krajowych Ramach Interoperacyjności, minimalnych wymaganiach dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymaganiach dla systemów;
2) komórki audytu wewnętrznego w Ministerstwie, działającej na podstawie przepisów o audycie wewnętrznym oraz informacji o pracy i wynikach tego audytu;
3) odpowiedniej komórki organizacyjnej w Jednostce.

3. Sprawdzenia stosowania przepisów ustawy policyjnej, zlecone przez Prezesa UODO, są wykonywane przez IOD MF lub osobę przez niego wskazaną.

4. IOD MF informuje Administratora o zaplanowanych audytach, kontrolach i sprawdzeniach.

5. Audyt i kontrola w zakresie ochrony danych osobowych mogą być częścią składową odpowiednio audytu lub kontroli z innych obszarów działalności Jednostki, pod warunkiem, że w zakresie dotyczącym ochrony danych osobowych audyt lub kontrolę prowadzi IOD MF lub osoba przez niego wskazana.

§ 45. 1. W przypadku uzyskania przez IOD MF informacji o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia, IOD MF ma prawo do przeprowadzenia kontroli doraźnej przedmiotowego obszaru.

2. W przypadku, kiedy Administrator podejmie decyzję o przeprowadzeniu kontroli doraźnej w oparciu o przepisy o kontroli w administracji rządowej, IOD MF ma prawo wziąć udział w tej kontroli osobiście lub skierować do niej wskazaną przez siebie osobę.

Współpraca IOD MF z koordynatorem do spraw ochrony danych osobowych w Jednostce

§ 46. 1. IOD MF ma prawo zwrócić się do właściwego koordynatora do spraw ochrony danych osobowych w Jednostce, o pomoc w przeprowadzeniu audytu, sprawdzenia lub kontroli w tej lub innej Jednostce, informując o tym odpowiedniego dyrektora Jednostki.

2. Koordynator do spraw ochrony danych osobowych w Jednostce wspiera Jednostkę w zakresie realizacji wskazanych przez IOD MF działań korygujących lub naprawczych.

3. Wnioski wynikające z przeprowadzonych przez IOD Jednostki audytów, sprawdzeń i kontroli z zakresu ochrony danych osobowych w zakresie właściwości Jednostki, które mają wpływ na ochronę danych osobowych objętych Polityką, są niezwłocznie przekazywane przez Jednostkę do wiadomości IOD MF.

Rozdział 14

Kontrole zewnętrzne dotyczące przetwarzania danych osobowych

§ 47. 1. Administrator niezwłocznie włącza IOD MF w działania wykonywane w ramach kontroli prowadzonych przez zewnętrzne organy kontrolne w Ministerstwie lub Jednostce, dotyczące ochrony danych osobowych, o których mowa w § 3 ust. 1, w szczególności w zakresie:

1) uczestnictwa IOD MF w spotkaniach z przedstawicielami organu kontrolnego lub czynnościach kontrolnych;
2) opiniowania treści odpowiedzi na zapytania organu kontrolnego, w tym zakresu i treści dokumentów przekazywanych organowi kontrolnemu;
3) przedstawiania organowi kontrolnemu stanowiska IOD MF w kwestiach ochrony danych osobowych;
4) zapoznania się z projektem protokołu z czynności kontrolnych, możliwości przedstawienia Administratorowi uwag IOD MF do jego treści, a także zapoznania się z ostateczną wersją protokołu;
5) zapoznania się z projektem wystąpienia pokontrolnego, a także możliwości przedstawienia Administratorowi uwag IOD MF do jego treści, zapoznania IOD MF z ostateczną wersją wystąpienia pokontrolnego oraz opiniowania treści odpowiedzi na zarzuty stawiane przez organ kontrolny;
6) ustalania sposobu realizacji zaleceń organu kontrolnego, terminów oraz osób lub komórek organizacyjnych w Ministerstwie albo w Jednostce zobowiązanych do ich realizacji.

2. Administrator nie może wyznaczać IOD MF do reprezentowania MF lub Jednostki przed organami kontrolnymi.

Rozdział 15

Odpowiedzialność (sankcje)

§ 48. Odpowiedzialność karną, dyscyplinarną lub służbową za naruszenie przepisów dotyczących ochrony danych osobowych określają przepisy odrębne.

Rozdział 16

Przeglądy i aktualizacja Polityki oraz powiązanych dokumentów

§ 49. 1. Właścicielem biznesowym Polityki jest DB.

2. Polityka podlega okresowym przeglądom pod kątem jej adekwatności, nie rzadziej niż raz do roku.

3. Przeglądu Polityki dokonuje DB, we współpracy z IOD MF oraz właścicielami biznesowymi danych i właścicielami biznesowymi systemów informatycznych.

4. Przegląd obejmuje w szczególności ocenę adekwatności Polityki do:

1) obowiązujących przepisów prawa w zakresie ochrony danych osobowych, którym podlega Administrator;
2) procesów funkcjonujących w Ministerstwie i Jednostkach.

5. Przegląd Polityki jest wykonywany niezwłocznie w każdym przypadku, gdy zmianie ulegają przepisy prawa będące źródłem wskazanych w Polityce obowiązków lub zaistnieją istotne zmiany organizacyjne, a także na skutek zaleceń i rekomendacji wynikających z kontroli, audytów, sprawdzeń oraz z wykrytych naruszeń ochrony danych osobowych.

6. Jeżeli w wyniku przeglądu Polityki stwierdzona zostanie konieczność aktualizacji jej przepisów, DB podejmuje niezwłocznie działania mające na celu aktualizację Polityki w wymaganym zakresie.

7. Regulacje określone w ust. 1–6 stosuje się odpowiednio do powiązanych polityk szczegółowych, procedur i instrukcji i ich właścicieli biznesowych, chyba że regulują one inaczej kwestię ich aktualizacji.

8. Wykaz procedur powiązanych z Polityką określa załącznik do Polityki.

9. Procedury i instrukcje, o których mowa w ust. 8, których właścicielem biznesowym jest komórka organizacyjna w Ministerstwie inna niż DB, podlegają zatwierdzeniu przez dyrektora DB.

Załącznik do Polityki Ochrony Danych Osobowych

Wykaz procedur i instrukcji powiązanych z PODO

L.p.	Wskazanie dokumentu	Właściciel biznesowy
1	Procedura dotycząca bezpieczeństwa teleinformatycznego	DI
2	Procedura dotycząca ciągłości działania	DB
3	Procedura dotycząca bezpieczeństwa fizycznego	DB
4	Procedura zarządzania upoważnieniami do przetwarzania danych osobowych	DB
5	Procedura powierzania przetwarzania danych osobowych	DB
6	Procedura zarządzania uprawnieniami w systemach teleinformatycznych służących do przetwarzania danych osobowych	DI
7	Procedura zarządzania ryzykiem	DB
8	Procedura przeglądu i usuwania danych osobowych	DB
9	Procedura zarządzania incydentami	DB
10	Procedura wykonywania i zarządzania kopiami zapasowymi	DI
11	Procedura dotycząca wykonywania pracy w formie telepracy	BDG
12	Procedura rozpatrywania wniosków osób, których dotyczą dane osobowe przetwarzane przez Administratora	DB
13	Instrukcja dotycząca oceny podmiotów zewnętrznych	DB
14	Instrukcja anonimizowania dokumentów	DB