Warszawa, dnia 29 stycznia 2025 r.

Poz. 4

ZARZĄDZENIE NR 4

MINISTRA RODZINY, PRACY I POLITYKI SPOŁECZNEJ

z dnia 27 stycznia 2025 r.

w sprawie Polityki ochrony danych osobowych w Ministerstwie Rodziny, Pracy i Polityki Społecznej

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, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35) zarządza się, co następuje:

§ 1. W Ministerstwie Rodziny, Pracy i Polityki Społecznej, zwanym dalej „Ministerstwem", wprowadza się Politykę ochrony danych osobowych w Ministerstwie, stanowiącą załącznik do zarządzenia.

§ 2. Traci moc zarządzenie nr 6 Ministra Rodziny i Polityki Społecznej z dnia 19 lutego 2021 r. w sprawie wprowadzenia Polityki ochrony danych osobowych w Ministerstwie Rodziny i Polityki Społecznej (Dz. Urz. Min. Rodz. i Pol. Społ. poz. 6).

§ 3. Upoważnienia wydane na podstawie zarządzenia, o którym mowa w § 2, zachowują ważność nie dłużej niż przez okres 1 roku od dnia wejścia w życie zarządzenia, o ile nie wystąpią okoliczności powodujące konieczność wydania nowego upoważnienia na podstawie niniejszego zarządzenia.

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

MINISTER

RODZINY, PRACY I POLITYKI

SPOŁECZNEJ

AGNIESZKA DZIEMIANOWICZ-BĄK

Załącznik do zarządzenia nr 4
Ministra Rodziny, Pracy i Polityki Społecznej
z dnia 27.01.2025 r. (poz. 4)

POLITYKA OCHRONY DANYCH OSOBOWYCH

W MINISTERSTWIE RODZINY, PRACY I POLITYKI SPOŁECZNEJ

ROZDZIAŁ I

Podstawowe pojęcia

1) **Administrator** – Minister Rodziny, Pracy i Polityki Społecznej;
2) **BM** – Biuro Ministra, komórka organizacyjna, która zgodnie z Regulaminem organizacyjnym Ministerstwa Rodziny, Pracy i Polityki Społecznej koordynuje sprawy związane z ochroną danych osobowych w Ministerstwie Rodziny, Pracy i Polityki Społecznej;
3) **dane dotyczące wyroków skazujących** – dane osobowe, o których mowa w art. 10 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.);
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) **departament –** departament albo biuro w Ministerstwie Rodziny, Pracy i Polityki Społecznej;
7) **dyrektor** – dyrektor departamentu albo biura w Ministerstwie lub osoba przez niego upoważniona;
8) **Inspektor Ochrony Danych (IOD)** – pracownik powołany przez Administratora, którego status i zadania są określone w art. 38 i 39 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.);
9) **kierownictwo Ministerstwa** – Minister, Sekretarze Stanu i Podsekretarze Stanu, Dyrektor Generalny i szef Gabinetu Politycznego Ministra;
10) **Minister** – Minister Rodziny, Pracy i Polityki Społecznej;
11) **Ministerstwo** – Ministerstwo Rodziny, Pracy 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) **Polityka** – Polityka ochrony danych osobowych w Ministerstwie Rodziny, Pracy i Polityki Społecznej;
18) **PUODO** – Prezes Urzędu Ochrony Danych Osobowych, organ nadzorczy;
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) **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) **system elektronicznego zarządzania dokumentacją** – funkcjonujący w Ministerstwie system elektronicznego zarządzania dokumentacją;
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 Stanu i Podsekretarz Stanu, Dyrektor Generalny, szef Gabinetu Politycznego Ministra, dyrektor, zastępca dyrektora departamentu w Ministerstwie, pracownik Ministerstwa, stażysta, praktykant, wolontariusz lub osoba realizująca zadania na podstawie umowy cywilnoprawnej na rzecz danego departamentu Ministerstwa;
24) **współadministrator** – jeden z co najmniej dwóch administratorów wspólnie ustalających cele i sposoby przetwarzania, o którym mowa w art. 26 RODO;
25) **zastępca dyrektora** – zastępca dyrektora departamentu albo biura w Ministerstwie;

26) **zastępca IOD** – pracownik zatrudniony na Samodzielnym Stanowisku do Spraw Ochrony Danych Osobowych, wykonujący swoje zadana zgodnie z opisem stanowiska pracy, którego Minister wyznaczył do pełnienia funkcji zastępcy podczas nieobecności IOD;

27) **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 w:

1) systemie elektronicznego zarządzania dokumentacją, innych systemach teleinformatycznych, poczcie elektronicznej, dyskach komputerów, dyskach sieciowych, pendrive'ach, telefonach oraz innych nośnikach danych;
2) kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych Ministerstwa.

3. Zasady zawarte w Polityce stosuje się także do przetwarzanych w Ministerstwie danych osobowych w sytuacji, kiedy Minister występuje w roli współadministratora albo podmiotu przetwarzającego, 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, 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;

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, taką jak:

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

2. Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

3. Pseudonimizacja oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

§ 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, art. 9 i art. 10 RODO;
2) rzetelności – dane powinny być przetwarzane z uwzględnieniem interesów i uzasadnionych oczekiwań osób, których dane dotyczą;
3) przejrzystości – osoba, której dane osobowe 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 – dane osobowe powinny być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych;
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

Udzielanie upoważnień do przetwarzania danych osobowych

§ 6. 1. Do przetwarzania danych osobowych, mogą być dopuszczeni jedynie użytkownicy posiadający upoważnienie do przetwarzania danych osobowych, udzielane użytkownikom przez

Administratora lub osobę, którą Administrator upoważnił do takich działań w jego imieniu, zwane dalej „upoważnieniem”.

2. Upoważnienie dla pracowników Ministerstwa wynika z:

1) zakresu zadań wymienionych w opisie stanowiska pracy – w przypadku członków korpusu służby cywilnej;
2) zakresu obowiązków – w przypadku pracowników, którzy nie są członkami korpusu służby cywilnej.

3. Upoważnienie udzielane jest na wniosek dyrektora, złożony za pośrednictwem systemu elektronicznego zarządzania dokumentacją do sekretariatu BM. Wzór wniosku określa załącznik nr 1 do Polityki.

4. Dyrektor wnioskuje o upoważnienie dla użytkownika, jeśli w przypadku użytkownika doszło do:

1) podjęcia pracy w Ministerstwie;
2) zmiany zakresu obowiązków skutkującej zmianą zakresu przetwarzanych danych osobowych;
3) zmiany stanowiska służbowego;
4) przeniesienia do innego departamentu niż departament, w którym zatrudniony był użytkownik;
5) zmiany nazwy departamentu, w którym zatrudniony był użytkownik;
6) podjęcia stażu lub praktyki lub wolontariatu;
7) realizacji umowy cywilnoprawnej

– jeżeli realizowane przez użytkownika zadania wiążą się z przetwarzaniem danych osobowych w Ministerstwie.

5. Upoważnienia udziela Dyrektor BM lub Zastępca Dyrektora BM na mocy upoważnienia wydanego przez Ministra.

6. Upoważnienie udzielane jest w postaci elektronicznej za pośrednictwem systemu elektronicznego zarządzania dokumentacją.

7. Wzór upoważnienia określa załącznik nr 2 do Polityki, z zastrzeżeniem ust. 12.

8. W przypadku oddelegowania użytkownika z jednego departamentu do realizacji zadań w innym departamencie – dyrektor, do którego oddelegowano użytkownika, zobowiązany jest do zgłoszenia do sekretariatu BM wniosku o nowe upoważnienie dla tego użytkownika.

9. Upoważnienie do przetwarzania danych osobowych zawiera w szczególności:

1) numer upoważnienia;
2) datę wydania upoważnienia;
3) imię i nazwisko użytkownika;
4) stanowisko służbowe w przypadku użytkownika będącego pracownikiem albo informację o formie wykonywania pracy na rzecz Ministerstwa (stażysta, praktykant, wolontariusz,

wykonawca w ramach umowy cywilnoprawnej wraz z numerem i datą zawarcia umowy) - w przypadku innych użytkowników;

5) nazwę departamentu, w którym zatrudniony jest użytkownik albo w którym użytkownik odbywa staż, praktykę albo wolontariat albo na rzecz którego użytkownik realizuje umowę cywilnoprawną;
6) procesy, w ramach których użytkownik będzie przetwarzać dane osobowe (zgodnie z rejestrem czynności właściwym dla danego departamentu);
7) kategorie przetwarzanych danych osobowych (dane osobowe, dane osobowe szczególne, dane dotyczące wyroków skazujących);
8) informację czy dane osobowe są przetwarzane: w postaci papierowej albo w postaci elektronicznej w systemach teleinformatycznych albo w obu tych postaciach;
9) systemy teleinformatyczne, w ramach których dane osobowe będą przetwarzane;
10) okres obowiązywania upoważnienia;
11) podpis Dyrektora BM lub Zastępcy Dyrektora BM.

10. Każdy dyrektor prowadzi rejestr upoważnień do przetwarzania danych osobowych dla departamentu, o których wydanie wnioskował. Wzór rejestru upoważnień dla departamentu jest określony w załączniku nr 3 do Polityki. Rejestr upoważnień departamentu prowadzony jest w postaci elektronicznej i nie obejmuje osób, dla których w związku z zawartymi umowami powierzenia przetwarzania danych osobowych, obowiązek wydania upoważnień spoczywa na podmiocie przetwarzającym.

11. Rejestr upoważnień dla Ministerstwa prowadzi Dyrektor BM lub Zastępca Dyrektora BM. Rejestr upoważnień dla Ministerstwa prowadzony jest w postaci elektronicznej. Przepisy ust. 10 dotyczące wzoru rejestru dla departamentu stosuje się odpowiednio do rejestru upoważnień dla Ministerstwa.

12. Rejestr osób upoważnionych, w związku z powierzeniem Ministrowi przetwarzania danych osobowych w ramach realizacji programów operacyjnych, projektów oraz innych zadań, dla których Minister lub Ministerstwo występuje w roli podmiotu przetwarzającego, prowadzi departament właściwy w obszarze przetwarzania powierzonych danych. Upoważnienia mogą być wydane na wzorze obowiązującym u administratora, z którym została podpisana umowa powierzenia przetwarzania danych osobowych, zgodnie z zapisami umowy w tym zakresie.

13. Każdy użytkownik, przed rozpoczęciem przetwarzania danych osobowych, powinien zapoznać się z Polityką.

14. Użytkownik składa:

1) niezwłocznie po otrzymaniu upoważnienia – oświadczenie o przestrzeganiu przepisów dotyczących ochrony danych osobowych oraz do zachowania poufności;

2) w terminie 10 dni roboczych od dnia wejścia w życie Polityki lub nawiązania stosunku prawnego zobowiązującego go do stosowania Polityki – oświadczenie o zapoznaniu się i zobowiązaniu się do przestrzegania Polityki,

– których wzory są określone w załącznikach nr 4 i nr 5 do Polityki.

15. Oświadczenia, o których mowa w ust. 14, składane są za pośrednictwem systemu elektronicznego zarządzania dokumentacją do sekretariatu BM oraz do wiadomości dyrektora, a w przypadku braku dostępu do tego systemu oświadczenie jest składane za pośrednictwem poczty elektronicznej na adres sekretariatu BM oraz do wiadomości dyrektora. Informacje o złożeniu oświadczeń, o których mowa w ust. 14, są odnotowywane odpowiednio w rejestrach, o których mowa w ust. 10 i 11.

16. Upoważnienie, o którym mowa w ust. 1, wygasa w przypadku:

1) ustania stosunku pracy;
2) zmiany nazwy departamentu, w którym zatrudniony był użytkownik, upoważnienie wygasa z dniem wydania nowego upoważnienia;
3) zmiany zakresu obowiązków użytkownika powodujących zaprzestanie czynności przetwarzania danych osobowych, określonych w upoważnieniu, które posiadał, upoważnienie wygasa z dniem poinformowania BM o zmianie zakresu;
4) wygaśnięcia upoważnienia wydanego na czas określony (np. zakończenie realizacji zadań/usług w związku z zawartą umową, udziału w komisjach/zespołach powołanych przez Administratora);
5) zakończenia wykonywania innych obowiązków realizowanych na rzecz Administratora (np. obowiązków stażystów, praktykantów, wolontariuszy, ekspertów).

17. Prawo dostępu do danych osobowych przetwarzanych w systemie teleinformatycznym mogą mieć wyłącznie użytkownicy, którym udzielono upoważnienia, o którym mowa w ust. 1, wyłącznie w zakresie w jakim dostęp ten jest niezbędny do realizacji powierzonych zadań.

18. Prawo dostępu do danych osobowych przyznane użytkownikom upoważnionym do przetwarzania danych osobowych w systemie teleinformatycznym, którzy nie są pracownikami Ministerstwa, ma charakter czasowy i może być przyznane na okres obowiązywania umowy, stażu, wolontariatu lub praktyki.

ROZDZIAŁ V

Rejestr czynności przetwarzania danych osobowych oraz rejestr kategorii czynności przetwarzania danych osobowych

§ 7. 1. W Ministerstwie prowadzi się rejestr czynności przetwarzania danych osobowych oraz rejestr kategorii czynności przetwarzania danych osobowych, o których mowa w art. 30 ust. 1 i 2 RODO, których wzory określone są w załączniku nr 6 i załączniku nr 7 do Polityki.

2. W każdym departamencie prowadzony jest rejestr czynności przetwarzania danych osobowych lub rejestr kategorii czynności przetwarzania danych osobowych.

3. Rejestry, o których mowa w ust. 1 i 2 prowadzone są w postaci elektronicznej i zamieszczane w systemie elektronicznego zarządzania dokumentacją.

4. Rejestr czynności przetwarzania danych osobowych Ministerstwa i Rejestr kategorii czynności przetwarzania danych osobowych Ministerstwa są zbiorami poszczególnych rejestrów prowadzonych przez departamenty.

5. Rejestry, o których mowa w ust. 4, są łączone z poszczególnych rejestrów czynności przetwarzania danych osobowych oraz rejestrów kategorii czynności przetwarzania danych osobowych, prowadzonych przez departamenty.

6. Rejestry prowadzone w departamentach są zatwierdzane przez dyrektorów w systemie elektronicznego zarządzania dokumentacją i są przekazywane w systemie elektronicznego zarządzania dokumentacją do sekretariatu BM w celu włączenia ich do odpowiedniego rejestru, o którym mowa w ust. 5.

7. Zatwierdzone rejestry departamentu nie są udostępniane użytkownikom z innych departamentów, o ile nie jest to niezbędne do realizacji zadań wykonywanych przez te departamenty lub użytkowników z tych departamentów.

8. Za sporządzenie rejestru czynności przetwarzania danych osobowych i rejestru kategorii czynności przetwarzania danych osobowych – w zakresie każdego departamentu oraz właściwą treść i poprawną formę zapisów w tych rejestrach prowadzonych przez departament i przekazywanie tych rejestrów do sekretariatu BM odpowiada dyrektor.

9. W przypadku zmiany czynności przetwarzania danych lub kategorii przetwarzania danych, zamieszczonych w rejestrach, o których mowa w ust. 8, dyrektor jest zobowiązany do zaktualizowania odpowiedniego rejestru i niezwłocznego przekazania go do sekretariatu BM.

10. IOD jest uprawniony do przeglądu rejestrów wymienionych w ust. 2 w celu wspierania Administratora w przestrzeganiu i właściwym stosowaniu przepisów o ochronie danych osobowych.

ROZDZIAŁ VI

Umowy lub porozumienia w sprawie powierzenia przetwarzania danych osobowych

§ 8. 1. Minister realizując swoje zadania skutkujące przetwarzaniem danych osobowych może być podmiotem, który:

1) zleca przetwarzanie danych w swoim imieniu innemu podmiotowi;
2) na zlecenie i w imieniu innego podmiotu przetwarza dane osobowe (podmiot przetwarzający).

2. Dyrektor, realizując zadania skutkujące powierzeniem przetwarzania danych osobowych innemu podmiotowi, odpowiada za wybór podmiotu przetwarzającego, spełniającego wymogi

wskazane w art. 28 RODO, który zapewni wystarczającą gwarancję wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie chroniło prawa osób, których dane osobowe dotyczą oraz monitorowanie i kontrolę umowy lub porozumienia w zakresie przestrzegania przepisów RODO przez podmiot przetwarzający.

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

4. Dyrektor na żądanie IOD udostępnia 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, dyrektor dokonuje oceny zgodności dalszych umów powierzenia przetwarzania z umową powierzenia przetwarzania oraz RODO.

6. Dane dotyczące umowy lub porozumienia w sprawie powierzenia przetwarzania danych osobowych odnotowuje się w rejestrze czynności przetwarzania danych osobowych prowadzonym przez dyrektora – jeśli Minister zleca przetwarzanie danych w swoim imieniu innemu podmiotowi albo w rejestrze kategorii przetwarzania danych osobowych prowadzonym przez dyrektora – jeśli Minister jest podmiotem przetwarzającym i na zlecenie i w imieniu innego podmiotu przetwarza dane osobowe.

7. Kategorie czynności, które zostały Administratorowi powierzone do przetwarzania, zawarte są w rejestrze kategorii czynności przetwarzania danych prowadzonym przez dyrektora.

8. Dyrektorzy obowiązani są informować IOD z wyprzedzeniem co najmniej 10 dni roboczych o zamiarze powierzenia przetwarzania danych osobowych i przekazać mu niezbędne informacje w tym zakresie, tj. wskazując szczegółowy opis na czym ma polegać przetwarzanie danych osobowych przez podmiot przetwarzający oraz szczegółowe wskazanie, z czego wynika konieczność konsultacji z IOD nieujęta w przepisach Polityki.

9. Jeżeli potrzebna będzie konsultacja z IOD w zakresie powierzenia Ministrowi przetwarzania danych osobowych w drodze umowy lub porozumienia wówczas dyrektor informuje IOD o planowanym przedsięwzięciu z wyprzedzeniem co najmniej 10 dni roboczych, aby umożliwić IOD zajęcie stanowiska w przedmiotowej kwestii.

10. IOD ma prawo do występowania do departamentów o przekazanie informacji na temat zawartych umów, porozumień lub aneksów w sprawie powierzenia przetwarzania danych w imieniu Ministra.

11. Umowa w zakresie powierzenia przetwarzania danych osobowych powinna w szczególności zawierać:

1) przedmiot i czas trwania przetwarzania;
2) charakter i cel przetwarzania danych;

3) oświadczenie podmiotu przetwarzającego o zapewnieniu wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie powierzonych danych osobowych spełniało wymogi prawem przewidziane i chroniło prawa osób, których dane dotyczą;
4) rodzaj i zakres powierzonych danych osobowych;
5) informacje o zasadach dotyczących przeprowadzania audytu lub kontroli w podmiotach przetwarzających dane osobowe w imieniu Ministra;
6) informacje o sposobie upoważniania osób, które w imieniu podmiotu przetwarzającego będą przetwarzały dane osobowe;
7) informacje o zasadach podpowierzania przetwarzania danych przez podmiot przetwarzający;
8) informacje o sposobach zgłaszania naruszeń z zakresu ochrony danych osobowych;
9) informacje o sposobach postępowania z danymi osobowymi po zakończeniu realizacji umowy;
10) wykaz środków technicznych i organizacyjnych wymienionych w celu zapewnienia bezpieczeństwa danych, z tym zastrzeżeniem, że środki techniczne i organizacyjne należy opisać szczegółowo, a nie w sposób ogólny z uwzględnieniem charakteru, zakresu, kontekstu i celu przetwarzania, a także ryzyka naruszenia praw i wolności osób fizycznych.

12. Postanowienia dotyczące powierzenia przetwarzania danych osobowych mogą być zawarte w umowie zasadniczej (głównej), tj. umowie w związku w którą miały zostać zawarta umowa powierzenia, pod warunkiem, że będą zgodne z wymaganiami dla umowy powierzenia przetwarzania danych osobowych, określonymi w ust. 11.

13. Czynności kontrolne w podmiotach, którym zostało powierzone przetwarzanie danych osobowych, odbywają się w trybie i na zasadach określonych w umowach, o których mowa w ust. 11 i 12.

14. Przeprowadzenie czynności kontrolnych w podmiotach, którym zostało powierzone przetwarzanie danych osobowych, Administrator może zlecić innej osobie lub podmiotom zewnętrznym.

15. Z przeprowadzonych czynności kontrolnych sporządzana jest informacja pokontrolna wraz z zaleceniami, do których podmiot kontrolowany może zgłosić swoje uwagi.

16. Kopia informacji pokontrolnej, w przypadku zgłoszenia uwag przez podmiot kontrolowany, również zawierająca stanowisko kontrolującego do zgłoszonych uwag, przekazywana jest do wiadomości Administratorowi.

17. Umowy powierzenia przetwarzania danych osobowych przechowuje dyrektor merytorycznie właściwy do zawarcia umowy, chyba że procedury wewnętrzne Ministerstwa dotyczące przechowywania umów określają inny tryb.

18. Przy wypełnianiu obowiązków, o których mowa w ust. 1–3, dyrektor może skorzystać ze standardowych klauzul umownych:

1) w przypadku powierzenia do przetwarzania danych pomiędzy administratorami a podmiotami przetwarzającymi, którzy podlegają prawu Unii lub prawu państwa członkowskiego – określonych w decyzji wykonawczej Komisji (UE) 2021/915 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz art. 29 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 (Dz. Urz. UE L 199 z 07.06.2021, str. 18);

2) w przypadku powierzenia do przetwarzania danych osobowych do państw trzecich – określonych w decyzji wykonawczej Komisji (UE) 2021/914 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (Dz. Urz. UE L 199 z 07.06.2021, str. 31).

ROZDZIAŁ VII

Prawa osób, których dane osobowe 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 osobowych. Ministerstwo realizuje to prawo, wykonując obowiązek informacyjny.

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

§ 10. 1. W przypadku zbierania danych osobowych od osoby, której dane dotyczą, Administrator w momencie pozyskiwania danych osobowych, w celu dalszego ich przetwarzania, przekazuje tej osobie informacje wskazane w art. 13 RODO, w szczególności:

1) tożsamość administratora danych;
2) cele przetwarzania danych osobowych;
3) prawa przysługujące osobie, której dane osobowe są przetwarzane.

2. Wzór minimalnego zakresu danych ujętych w klauzuli informacyjnej w przypadku zbierania danych od osoby, której dane dotyczą, określa załącznik nr 8 do Polityki.

§ 11. 1. W przypadku zbierania danych osobowych w sposób inny niż od osoby, której dane osobowe dotyczą, Administrator przekazuje tej osobie informacje wskazane w art. 14 RODO, w szczególności:

1) tożsamość administratora danych;
2) cele przetwarzania danych osobowych;

3) prawa przysługujące osobie, której dane osobowe są przetwarzane;

4) źródło pozyskania danych osobowych.

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 9 do Polityki.

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 dyrektor , w którym dane osobowe będą przetwarzane.

2. Realizacja obowiązku informacyjnego następuje pisemnie, w postaci papierowej lub elektronicznej, przez zamieszczenie informacji na tablicy informacyjnej w miejscu ogólnodostępnym lub przez stronę internetową Ministerstwa, lub Biuletyn Informacji Publicznej, a w szczególnych przypadkach – kiedy osobie nie można przedstawić informacji pisemnie – przez odczytanie.

3. W przypadku właściwości kilku departamentów obowiązek informacyjny realizuje departament udzielający zbiorczej odpowiedzi.

4. W przypadku przetwarzania przez więcej niż jeden departament danych pozyskanych w związku z zawieraną umową lub porozumieniem – za realizację obowiązku informacyjnego, o którym mowa w ust. 1, odpowiada dyrektor zawierający tę umowę lub porozumienie.

5. Za rozliczalność w zakresie wypełniania obowiązków informacyjnych, o których mowa w ust. 1–3, jest odpowiedzialny dyrektor właściwy w obszarze przetwarzania danych lub podmiot, jeżeli został zobowiązany treścią umowy powierzenia przetwarzania danych osobowych zawarcie której wynika z art. 28 RODO.

6. Za aktualność i zgodność z przepisami klauzul informacyjnych na formularzach, w tym formularzach funkcjonujących na portalach i serwisach Ministerstwa, odpowiedzialni są dyrektorzy właściwi w obszarze przetwarzania danych.

ROZDZIAŁ VIII

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

§ 13. 1. Osoba, której dane dotyczą, jest uprawniona do uzyskania potwierdzenia, czy w Ministerstwie przetwarzane są jej dane osobowe, o ile wystąpi do Administratora w sposób umożliwiający weryfikację jej tożsamości, w szczególności z wykorzystaniem profilu zaufanego.

2. W przypadku przetwarzania danych, osoba, której dane dotyczą ma prawo do uzyskania informacji w następującym zakresie:

1) celu przetwarzania danych osobowych;

2) kategorii danych osobowych, których dotyczy przetwarzanie;

3) odbiorcy lub kategorii odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności odbiorcy w państwach trzecich lub organizacjach międzynarodowych;
4) planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
5) prawach do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
6) prawie wniesienia skargi do PUODO;
7) źródle danych, jeżeli nie zostały zebrane od osoby, której dotyczą.

3. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach związanych z przekazaniem.

4. Jeżeli osoba, której dane dotyczą, zwróci się z wnioskiem o dostarczenie kopii jej danych osobowych podlegających przetwarzaniu, żądanie takie realizuje się bezpłatnie. Za wszelkie kolejne kopie, o które zwróci się ta osoba, można pobrać opłatę ustaloną zgodnie z zasadami określonymi w art. 15 ust. 3 RODO.

5. Kopię danych wydaje się w postaci wydruku po ich przepisaniu lub skopiowaniu do ustrukturyzowanego powszechnie używanego formatu nadającego się do odczytu maszynowego. Nie wydaje się skanów dokumentów ani ich kserokopii, gdyż mogą zawierać dodatkowe dane niedotyczące osoby występującej z wnioskiem. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się drogą elektroniczną, po weryfikacji tożsamości osoby.

§ 14. 1. Osoba, której dane dotyczą, ma prawo żądania niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.

2. Osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym przez przedstawienie dodatkowego oświadczenia.

3. Wniosek o sprostowanie lub uzupełnienie danych może być przekazany w formie pisemnej lub drogą elektroniczną na adres Ministerstwa. Pracownik, który w ramach wykonywanych zadań przetwarza dane osoby wnioskującej, obowiązany jest dokonać weryfikacji przetwarzanych danych. Uzupełnienie danych następuje z uwzględnieniem celów przetwarzania.

4. Prawo do sprostowania danych nie znajduje zastosowania do danych osobowych, w odniesieniu do których tryb ich sprostowania lub uzupełnienia określają odrębne przepisy.

§ 15. 1. Osoba, której dane dotyczą, ma prawo żądać od Administratora niezwłocznego usunięcia dotyczących go danych osobowych, a Administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli spełnione są przesłanki określone w art. 17 ust. 1 RODO.

2. W przypadku braku możliwości realizacji wniosku osoby, której dane dotyczą, z uwagi na przesłanki określone w art. 17 ust. 3 RODO, dyrektor właściwy do realizacji wniosku informuje osobę, której dane dotyczą o przyczynach nieuwzględnienia jej wniosku w całości lub w części.

§ 16. 1. Osoba, której dane dotyczą, ma prawo żądania ograniczenia przetwarzania jej danych osobowych w przypadkach określonych w art. 18 RODO.

2. Ograniczenie przetwarzania oznacza, że dane osobowe można jedynie przechowywać. Inne formy przetwarzania mogą mieć miejsce wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

3. Ograniczenia przetwarzania dokonuje się przez odpowiednie oznaczenie danych osobowych, których dotyczy żądanie, przetwarzanych zarówno w formie tradycyjnej, jak i elektronicznej, tak aby każdy użytkownik upoważniony do przetwarzania tych danych był świadomy, że dane te można jedynie przechowywać.

§ 17. 1. Jeżeli przetwarzanie oparte jest na przesłance wykonania zadania realizowanego w interesie publicznym lub przesłance celów wynikających z prawnie uzasadnionych interesów, osoba, której dane dotyczą, z przyczyn związanych z jej szczególną sytuacją, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych.

2. Dyrektor, który przetwarza dane takiej osoby, zaprzestaje przetwarzania danych osobowych, względem których wniesiono sprzeciw, chyba że wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

3. W przypadku przyjęcia, że istnieją prawnie uzasadnione podstawy do przetwarzania, ważniejsze niż interes osoby wnioskującej, właściwy dyrektor informuje osobę wnioskującą o odmowie realizacji prawa wraz z uzasadnieniem decyzji.

4. IOD koordynuje przyjmowanie i rozpatrywanie wniosków osób w zakresie praw związanych z ochroną danych osobowych wpływających do Ministerstwa.

5. Korespondencję pisemną lub przesłaną za pośrednictwem e-PUAP, której treść wskazuje na wniosek osoby w zakresie praw związanych z ochroną danych osobowych, Kancelaria Ogólna Ministerstwa rejestruje w systemie elektronicznego zarządzania dokumentacją i przekazuje bezpośrednio do IOD, za pomocą systemu elektronicznego zarządzania dokumentacją.

6. Korespondencję, której treść wskazuje na wniosek osoby w zakresie praw związanych z ochroną danych osobowych, przesłaną na adres poczty elektronicznej wskazanej na stronie

internetowej Ministerstwa do kontaktu z obywatelami komórka odpowiedzialna za obsługę tego adresu w BM przekazuje do IOD.

7. W przypadku korespondencji, o której mowa w ust. 5 i 6, IOD weryfikuje kompletność danych adresowych oraz informacji umożliwiających zidentyfikowanie dyrektora merytorycznie odpowiadającego za przetwarzanie danych osobowych.

8. W przypadku braku wystarczających informacji umożliwiających zidentyfikowanie departamentu, do którego powinien być przekazany wniosek, IOD występuje do osoby o uszczegółowienie informacji.

9. IOD przekazuje korespondencję do dyrektora właściwego w sprawie rozpatrzenia wniosku, który jest obowiązany do zrealizowania wniosku. Projekt odpowiedzi na wniosek jest uzgadniany z IOD.

10. W przypadku braku możliwości realizacji wniosku, informację o przyczynach braku realizacji dyrektor właściwy w sprawie rozpatrzenia wniosku przesyła osobie oraz IOD.

11. W przypadku, gdy korespondencja, której treść wskazuje na wniosek osoby w zakresie przysługujących jej praw związanych z ochroną danych osobowych, została przesłana bezpośrednio do departamentu Ministerstwa, dyrektor właściwy w sprawie rozpatrzenia wniosku jest obowiązany do niezwłocznego przekazania wniosku do IOD.

12. Dyrektor właściwy w sprawie rozpatrzenia wniosku, o którym mowa w ust. 1, informuje osobę, której wniosek dotyczy oraz IOD o sposobie załatwienia wniosku.

13. W Ministerstwie prowadzi się rejestr wniosków osób w zakresie praw związanych z ochroną danych osobowych wpływających do Ministerstwa.

14. W każdym departamencie prowadzony jest rejestr wniosków osób w zakresie realizacji ich praw związanych z ochroną danych osobowych wpływających do departamentu i rozpatrywanych przez departament.

15. Rejestry, o których mowa w ust. 13 i 14, prowadzone są w postaci elektronicznej. i zawierają w szczególności następujące informacje:

1) dane wnioskodawcy – imię i nazwisko;
2) data wpływu;
3) informacja czego dotyczy żądanie;
4) departament właściwy;
5) sposób załatwienia;
6) data załatwienia;
7) uwagi.

16. Wzór rejestrów, o których mowa w ust. 15, określa załącznik nr 10 do Polityki.

ROZDZIAŁ IX

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

§ 18. 1. W przypadku, gdy przetwarzanie danych osobowych nie może być oparte na jednej z przesłanek legalności, określonych w art. 6 ust. 1 lit. b–f i art. 9 ust. 1 lit. b–j RODO, podstawą przetwarzania danych osobowych może być zgoda osoby, której dane dotyczą określona wart. 6 ust. 1 lit. a RODO lub art. 9 ust. 2 lit. a RODO.

2. W celu realizacji zasady rozliczalności zgoda osoby, której dane dotyczą, na przetwarzanie jej danych osobowych, zwana dalej „zgodą”, powinna być udokumentowana w formie pisemnej.

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

4. Ramowy wzór treści zgody jest określony w załączniku nr 11 do Polityki.

5. Dyrektor właściwy dla realizacji zadania, z którym wiąże się wyrażenie zgody, prowadzi rejestr zgód, w tym w systemie elektronicznego zarządzania dokumentacją. Rejestr zgód powinien zawierać elementy pozwalające na identyfikację osoby, która udzieliła zgody, i okoliczności udzielenia zgody, w szczególności:

1) imię i nazwisko osoby;
2) adres do korespondencji lub adres poczty elektronicznej osoby;
3) data udzielenia zgody;
4) okoliczność, w związku z którą zgoda została udzielona.

6. Wzór rejestru, o którym mowa w ust. 5, określa załącznik nr 12 do Polityki.

ROZDZIAŁ X

Przekazanie danych osobowych do państw trzecich

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

2. Dyrektor właściwy dla planowanego przekazania danych, 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. Dyrektor właściwy dla przekazania danych, 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

§ 20. 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. Każdy użytkownik, który stwierdził lub podejrzewa wystąpienie zdarzenia, które może stanowić naruszenie ochrony danych osobowych, ma obowiązek zgłosić ten fakt dyrektorowi.

3. Do zadań dyrektora właściwego dla zdarzenia, o którym mowa w ust. 2, należy:

1) zgłaszanie IOD zdarzeń noszących znamiona incydentu lub naruszenia, które wystąpiły w departamencie;
2) konsultowanie z IOD w przypadku wystąpienia zdarzenia mogącego stanowić naruszenie ochrony danych osobowych w zakresie wyjaśnienia przyczyn i okoliczności;
3) przygotowanie dokumentów wymaganych przez PUODO w związku ze zgłaszaniem naruszenia przez Administratora;
4) informowanie osób, których dane dotyczą o naruszeniu, w przypadku zaistnienia takiej konieczności;
5) dokonanie oceny wagi naruszenia;
6) wdrożenie działań minimalizujących niekorzystne skutki wystąpienia zdarzenia mogącego stanowić naruszenie ochrony danych osobowych oraz działań zaradczych na przyszłość;
7) dokumentowanie spraw z zakresu naruszeń w departamencie.

4. W przypadku, gdy zgłoszenie dotyczy zdarzenia noszącego znamiona incydentu lub naruszenia, które wystąpiło w systemie informatycznym, zgłoszenie należy przekazać równocześnie do Departamentu Informatyki, zgodnie z zasadami określonymi w obowiązującej w Ministerstwie Polityce Bezpieczeństwa Informacji w obszarze IT, zwanej dalej „PBI IT”.

5. Zgłoszenie zdarzenia mogącego stanowić naruszenie ochrony danych osobowych powinno zawierać:

1) opisanie symptomów naruszenia ochrony danych osobowych;

2) określenie okoliczności i czasu, w jakim prawdopodobnie nastąpiło naruszenie ochrony danych osobowych;
3) określenie okoliczności i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych;
4) określenie istotnych informacji, które mogą wskazywać na przyczynę naruszenia;
5) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

6. Ustalenie, czy zdarzenie może stanowić naruszenie ochrony danych osobowych, należy do IOD. Stwierdzenie naruszenia następuje w momencie, kiedy IOD ma wystarczający stopień pewności co do tego, że miało miejsce zdarzenie, które może prowadzić do naruszenia bezpieczeństwa danych osobowych.

7. Jeżeli naruszenie ochrony danych osobowych dotyczy systemu informatycznego, Administrator Systemów Informatycznych, o którym mowa w PBI IT, w porozumieniu z IOD podejmuje niezbędne działania zabezpieczające, niezwłocznie po otrzymaniu informacji, o której mowa w ust. 5. Szczegółowe zasady postępowania określone są w PBI IT.

8. Jeżeli naruszenie ochrony danych nie dotyczy systemu informatycznego odpowiednie czynności zabezpieczające podejmuje IOD, tj. w szczególności:
1) może nakazać przerwanie pracy, zwłaszcza w zakresie przetwarzania danych osobowych, do czasu powiadomienia o zaistniałej sytuacji Dyrektora Generalnego lub osoby przez niego upoważnionej;
2) działa w celu wyjaśnienia okoliczności zdarzenia;
3) przedstawia zalecenia w celu umożliwienia dalszego bezpiecznego przetwarzania danych.

9. Odmowa udzielenia wyjaśnień lub współpracy z IOD traktowana jest jako naruszenie obowiązków pracowniczych.

10. W przypadku zgłaszania naruszenia ochrony danych osobowych PUODO zgłoszenie takie opracowuje dyrektor właściwy dla wystąpienia naruszenia ochrony danych osobowych, według wzoru określonego przez PUODO.

11. Zgłoszenia naruszenia ochrony danych osobowych PUODO dokonuje Administrator, inny właściwy członek Kierownictwa Ministerstwa albo dyrektor właściwy dla wystąpienia naruszenia ochrony danych osobowych - bez zbędnej zwłoki, nie później jednak niż w terminie 72 godzin po stwierdzeniu naruszenia.

12. Do zgłoszenia przekazanego PUODO po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

13. W przypadku stwierdzenia w toku dalszych czynności, że do naruszenia nie doszło, informację o tym należy przekazać PUODO w ramach uzupełnienia zgłoszenia lub pisma wyjaśniającego,

a następnie zarejestrować zaistniałe zdarzenie jako niestanowiące naruszenia ochrony danych osobowych.

14. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, bez zbędnej zwłoki zawiadamia się o tym osoby, których dane dotyczą.

15. Za realizację obowiązku wskazanego w ust. 13 odpowiada dyrektor właściwy dla wystąpienia naruszenia ochrony danych osobowych.

16. Zawiadomienie należy przygotować jasnym i prostym językiem.

17. Zawiadomienie osób, których dane dotyczą, o naruszeniu nie jest wymagane, jeżeli w Ministerstwie:

1) wdrożono odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie eliminując prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
2) zawiadomienie takie wymagałoby niewspółmiernie dużego wysiłku; w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostaną poinformowane w równie skuteczny sposób.

18. O każdym naruszeniu skutkującym zgłoszeniem do PUODO jest informowany Minister. Informację o naruszeniu przekazuje dyrektor właściwy dla wystąpienia naruszenia ochrony danych osobowych.

19. W każdym departamencie prowadzony jest rejestr zdarzeń, incydentów i naruszeń ochrony danych osobowych, zwany dalej „rejestrem naruszeń”, którego wzór określony jest w załączniku nr 13 do Polityki. Za prowadzenie rejestru naruszeń odpowiada dyrektor.

20. Po zaistnieniu zdarzenia, incydentu lub naruszenia w departamencie uzupełniony rejestr naruszeń jest udostępniany BM za pośrednictwem systemu elektronicznego zarządzania dokumentacją w celu dołączenia do zbiorczego rejestru naruszeń Ministerstwa, który stanowi zbiór rejestrów naruszeń z poszczególnych departamentów.

21. Zbiorczy rejestr naruszeń Ministerstwa jest na każde żądanie przedstawiany Ministrowi lub Dyrektorowi Generalnemu.

ROZDZIAŁ XII

Przeprowadzenie oceny skutków dla ochrony danych osobowych

§ 21. 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 departament, w którym będzie odbywało się lub odbywa się przetwarzanie danych osobowych wymagające jej przeprowadzenia.

3. Dyrektor realizujący proces wskazany w ust. 1, jest obowiązany 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.

4. Za przeprowadzenie oceny skutków dla ochrony danych osobowych odpowiedzialny jest dyrektor, w którego właściwości pozostaje proces.

§ 22. 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 osobowe 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 osobowe dotyczą, i innych osób, których sprawa dotyczy.

2. W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z procesu przetwarzania, dyrektor, w którego właściwości pozostaje 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, dyrektor powinien ten fakt skonsultować z IOD.

4. Nie przeprowadza się oceny skutków dla ochrony danych osobowych w przypadku, o którym mowa w art. 35 ust. 10 RODO.

§ 23. 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 PUODO.

2. Departament, który przeprowadził ocenę, konsultuje się z PUODO po uzyskaniu opinii 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 PUODO.

ROZDZIAŁ XIII

Inspektor Ochrony Danych (IOD)

§ 24. 1. W celu wywiązania się z obowiązków nałożonych na Administratora w art. 37 ust. 1 RODO Administrator powołał IOD.

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;
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;
6) koordynuje procedurę rozpatrywania wniosków, o których mowa w art. 15–22 RODO skierowanych do Ministerstwa za pośrednictwem adresu służbowej poczty elektronicznej przeznaczonej do komunikacji z IOD: iodo@mrpips.gov.pl;
7) udziela zaleceń co do oceny skutków dla ochrony danych osobowych oraz monitoruje ich wykonanie;
8) współpracuje z PUODO i pełni funkcję punktu kontaktowego dla PUODO w kwestiach związanych z przetwarzaniem danych osobowych, w tym poprzez uprzednie konsultacje, oraz w stosownych przypadkach prowadzi konsultacje w innych sprawach.

3. IOD wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, kontekst i cele przetwarzania.

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

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

6. Administrator może powołać zastępcę lub zastępców IOD, który/którzy realizuje/ją swoje zadania zgodnie z wewnętrznymi przepisami Regulaminu wewnętrznego BM.

7. IOD podlega bezpośrednio Ministrowi, któremu składa roczne sprawozdanie w zakresie podejmowanych działań.

ROZDZIAŁ XIV

Środki techniczne i organizacyjne zapewniające bezpieczeństwo danych osobowych przetwarzanych w Ministerstwie

§ 25. 1. Środki techniczne i organizacyjne w systemach teleinformatycznych stosowane w celu zapewnienia bezpieczeństwa danych osobowych przetwarzanych w Ministerstwie są określone w PBI IT.

2. Środki techniczne i organizacyjne dotyczące fizycznego dostępu do obszaru, w którym przetwarzane są dane osobowe, są określone w regulacjach wewnętrznych Ministerstwa.

3. Uwzględniając ochronę danych w fazie projektowania oraz domyślną ochronę danych Administrator wdraża środki techniczne i organizacyjne, o których mowa w ust. 1 i 2, dobrane na podstawie przeprowadzonej analizy ryzyka naruszenia praw lub wolności osób fizycznych, uwzględniając 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. Środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych – art. 5 i 25 RODO.

ROZDZIAŁ XV

Analiza ryzyka w obszarze ochrony danych osobowych

§ 26. 1. W Ministerstwie przeprowadzana jest analiza ryzyka dla procesów, w ramach których przetwarzane są dane osobowe.

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 wagi naruszenia ujawnienia danych osobowych tj. ocena 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

§ 27. 1. Członkowie kierownictwa Ministerstwa są upoważnieni do przetwarzania danych osobowych zgodnie ze swoim zakresem czynności.

2. Członkowie kierownictwa Ministerstwa sprawują, zgodnie z ustalonym podziałem pracy w kierownictwie, nadzór nad przetwarzaniem danych osobowych w podległych departamentach.

3. Członek kierownictwa Ministerstwa, jest uprawniony do wykonywania czynności Administratora, w zakresie w jakim jest to niezbędne do wykonywania jego zadań – zgodnie z ustalonym podziałem pracy w kierownictwie.

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

umów i porozumień oraz udzielania upoważnień do wydawania upoważnień do przetwarzania danych osobowych lub zgłaszania naruszeń w zakresie przetwarzania danych osobowych do PUODO.

5. Dyrektor Generalny, 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 poprzez dostarczenie mu zasobów niezbędnych do wykonywania jego zadań oraz utrzymania wiedzy fachowej, a także zapewniając 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.

6. Dyrektorzy i zastępcy dyrektorów są upoważnieni do przetwarzania danych osobowych zgodnie ze swoim zakresem czynności.

7. Dyrektorzy i zastępcy dyrektorów są uprawnieni do zawierania umów i porozumień dotyczących przetwarzania danych osobowych, umów powierzenia przetwarzania danych osobowych, a także zawierania aneksów do tych umów i porozumień oraz zgłaszania naruszeń w zakresie przetwarzania danych osobowych do PUODO, zgodnie ze swoim zakresem czynności.

§ 28. 1. Dyrektor, przy uwzględnieniu ryzyka dotyczącego zarządzanego obszaru przetwarzania, odpowiada za zorganizowanie właściwej ochrony danych osobowych przetwarzanych w departamencie, w tym za zgodne z przepisami przetwarzanie tych danych przez podległych pracowników i użytkowników niebędących pracownikami, w ramach realizacji zadań na stanowiskach pracy, realizacji umów lub wykonywania innych zobowiązań wobec Ministra albo Ministerstwa.

2. Do dyrektorów należy, w zakresie właściwości, 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, umów powierzenia przetwarzania danych osobowych;
3) 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;
4) realizacja obowiązku informacyjnego, o którym mowa w rozdziale VII;
5) 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;

6) prowadzenie rejestru upoważnień do przetwarzania danych osobowych, o które wnioskował;
7) prowadzenie rejestru czynności przetwarzania danych osobowych oraz rejestru kategorii przetwarzania danych osobowych, a także ich aktualizacja;
8) prowadzenie rejestru wniosków osób w zakresie realizacji ich praw związanych z ochroną danych osobowych;
9) prowadzenie rejestru zgód osób, których dane dotyczą, na przetwarzanie ich danych osobowych;
10) prowadzenie rejestru naruszeń ochrony danych osobowych;
11) współpraca z IOD przy realizacji jego zadań;
12) informowanie IOD o pracach dotyczących planowania różnego rodzaju przedsięwzięć o charakterze programowym, legislacyjnym lub projektowym, jeżeli ich realizacja będzie związana z przetwarzaniem danych osobowych oraz umożliwienie IOD włączenia się w te prace;
13) zapewnienie prawidłowego przetwarzania danych osobowych.

§ 29. 1. Dyrektor wyznacza koordynatora do spraw ochrony danych osobowych, zwanego dalej „koordynatorem”, w celu wspierania dyrektora w realizacji niektórych lub wszystkich zadań, o których mowa w § 28 ust. 2.

2. Do zadań koordynatora należy wspieranie dyrektora w szczególności w zakresie:
1) przestrzegania przepisów dotyczących przetwarzania danych osobowych;
2) współpracy z IOD w zakresie prawidłowego przetwarzania danych osobowych w departamencie;
3) prowadzenia rejestru upoważnień, o którym mowa w § 28 ust. 1 pkt 8;
4) prowadzenia rejestru czynności przetwarzania danych i rejestru kategorii czynności przetwarzania danych w departamencie oraz aktualizacji tych rejestrów;
5) prowadzenia rejestru wniosków osób w zakresie realizacji ich praw związanych z ochroną danych osobowych;
6) prowadzenia rejestru zgód osób, których dane dotyczą, na przetwarzanie ich danych osobowych;
7) prowadzenia rejestru naruszeń ochrony danych osobowych;
8) udziału w opiniowaniu w ramach właściwości departamentu projektów umów powierzenia przetwarzania danych, oraz projektów wewnętrznych regulacji Ministerstwa w zakresie ochrony danych osobowych;
9) udziału w przeprowadzaniu, jeżeli zaistnieje taka konieczność, czynności kontrolnych przestrzegania zasad ochrony przetwarzania danych osobowych w podmiotach przetwarzających, którym zostało powierzone przetwarzanie danych osobowych, w trybie i na zasadach określonych w umowie;

10) współpracy z IOD w zakresie audytów oraz monitorowania przestrzegania RODO oraz Polityki Administratora lub podmiotu przetwarzającego w obszarze ochrony danych osobowych zgodnie z właściwością departamentu.

3. Zakres uprawnień i obowiązków koordynatora określa opis jego stanowiska pracy.

4. O wyznaczeniu koordynatora oraz o zakresie jego obowiązków dyrektor niezwłocznie informuje BM, przekazując informacje w tym zakresie do sekretariatu BM.

5. Dyrektor może wyznaczyć zastępcę koordynatora, w którym mowa w ust. 1. Przepisy ust. 2, 3 i 4 dotyczące koordynatora – stosuje się odpowiednio do zastępcy koordynatora.

§ 30. 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;
4) bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania danych w systemach teleinformatycznych, określonych w PBI IT;
5) niszczenia wszystkich niepodlegających archiwizacji, zbędnych dokumentów zawierających dane osobowe;
6) uczestniczenia w szkoleniach z obszaru ochrony danych osobowych;
7) współpracy z IOD przy realizacji jego zadań;
8) nieudzielania innym podmiotom informacji o przetwarzanych danych osobowych, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione;
9) informowania przełożonego o wszelkich zauważonych nieprawidłowościach i zdarzeniach skutkujących lub mogących skutkować obniżeniem poziomu ochrony danych osobowych;

10) zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych osobowych oraz niewłaściwym funkcjonowaniem systemu ochrony danych osobowych, zgodnie z trybem przewidzianym w § 20.

2. W przypadku pracy zdalnej wykonywanej poza siedzibą Ministerstwa, obowiązki o których mowa w ust. 1, użytkownik stosuje odpowiednio.

3. Odpowiedzialność za naruszenie przepisów dotyczących ochrony danych osobowych określają przepisy odrębne.

4. Każdy użytkownik, przed rozpoczęciem przetwarzania danych osobowych, jest obowiązany potwierdzić zapoznanie się z Polityką poprzez złożenie oświadczenia w terminie 10 dni roboczych od dnia wejścia w życie Polityki lub nawiązania stosunku prawnego zobowiązującego ich do stosowania Polityki, na wzorze potwierdzają zapoznanie się z Polityką, składając oświadczenie według wzoru stanowiącego załącznik nr 5, tak aby w sposób jednoznaczny zapewnić potwierdzenie tego faktu w zakresie spełnienia zasady rozliczalności. Oświadczenie jest składane za pośrednictwem systemu elektronicznego zarządzania dokumentacją do sekretariatu BM i do wiadomości dyrektora. W przypadku braku dostępu do tego systemu oświadczenie jest składane za pośrednictwem poczty elektronicznej na adres sekretariatu BM i do wiadomości dyrektora.

§ 33. Ustala się następujące załączniki do Polityki:

1) załącznik nr 1 – Wzór wniosku o udzielenie upoważnienia dla użytkownika do przetwarzania danych osobowych;
2) załącznik nr 2 – Wzór upoważnienia dla użytkownika do przetwarzania danych osobowych;
3) załącznik nr 3 – Wzór rejestru upoważnień do przetwarzania danych osobowych udzielanych użytkownikom, prowadzonego przez departamenty i Biuro Ministra;
4) załącznik nr 4 – Wzór oświadczenia użytkownika o przestrzeganiu przepisów dotyczących ochrony danych osobowych oraz zobowiązaniu się do zachowania poufności;
5) załącznik nr 5 – Wzór oświadczenia użytkownika o zapoznaniu się i zobowiązaniu się do przestrzegania Polityki ochrony danych osobowych w Ministerstwie Rodziny, Pracy i Polityki Społecznej;
6) załącznik nr 6 – Wzór rejestru czynności przetwarzania danych osobowych;
7) załącznik nr 7 – Wzór rejestru kategorii czynności przetwarzania danych osobowych;
8) załącznik nr 8 – Wzór minimalnego zakresu danych ujętych w klauzuli informacyjnej w przypadku zbierania danych osobowych od osoby, której dane dotyczą;
9) załącznik nr 9 – Wzór minimalnego zakresu danych ujętych w klauzuli informacyjnej w przypadku zbierania danych osobowych w sposób inny niż od osoby, której dane osobowe dotyczą;

10) załącznik nr 10 – Wzór rejestru wniosków osób w zakresie realizacji ich praw związanych z ochroną danych osobowych;
11) załącznik nr 11 – Wzór zgody osoby, której dane są przetwarzane w Ministerstwie Rodziny, Pracy i Polityki Społecznej;
12) załącznik nr 12 – Wzór rejestru zgód osób, których dane dotyczą, na przetwarzanie ich danych osobowych;
13) załącznik nr 13 – Wzór rejestru naruszeń ochrony danych osobowych.

Załącznik nr 1

Wzór wniosku o udzielenie upoważnienia dla użytkownika do przetwarzania danych osobowych

……..

Nazwa departamentu

Warszawa, dnia [kliknij i wybierz z kalendarza] r. lub /elektroniczny znacznik czasu/

Dyrektor

Biura Ministra

Wniosek o udzielenie upoważnienia do przetwarzania danych osobowych

1. Wniosek o udzielenie upoważnienia dla:

l.p.	Imię i nazwisko użytkownika	Stanowisko / status (stażysta / praktykant/ wolontariusz / realizacja umowy cywilnoprawnej)	Departament/Biuro	Okres ważności upoważnienia[1]

2. Wnioskuję o udzielenie upoważnienia do przetwarzania danych osobowych ww. użytkownikowi w związku z[2]:

1) podjęciem pracy w Ministerstwie,

2) zmianą zakresu obowiązków skutkującą zmianą zakresu przetwarzanych danych osobowych,

3) zmianą stanowiska służbowego,

4) przejściem do innego departamentu niż departament, w którym dotychczas zatrudniony był użytkownik;

5) zmianą nazwy departamentu, w którym zatrudniony był użytkownik;

[1] Należy wstawić odpowiednio:

- na czas trwania stosunku pracy (umowa o pracę),

- do dnia…….. (w przypadku pozostałych osób, które będą przetwarzały dane osobowe w imieniu administratora).

[2] Niewłaściwe należy skreślić.

6) podjęciem stażu /praktyki /wolontariatu[3],

7) realizacją umowy cywilnoprawnej nr …… z dnia ……..

3. Dane osobowe będą przetwarzane przez użytkownika[4]:

1) w postaci papierowej,

2) w postaci elektronicznej w systemach informatycznych,

3) w postaci papierowej i w postaci elektronicznej w systemach teleinformatycznych.

4. Główne systemy teleinformatyczne, w których następuje przetwarzanie danych to:

1) …….

2) ……..

3) ……..

5. Dane osobowe będą przetwarzane w ramach następujących procesów (zgodnie z rejestrem czynności właściwym dla danego departamentu):

1) ……..

2) ……..

…….

6. Kategorie danych, które będą przetwarzane[5]:

1) dane osobowe;

2) dane osobowe szczególne;

3) dane dotyczące wyroków skazujących.

……..

(imię i nazwisko)

……

(stanowisko wnioskującego)

(podpisano kwalifikowanym podpisem elektronicznym)

3 Niewłaściwe należy skreślić.

4 Niewłaściwe należy skreślić.

5 Niewłaściwe należy skreślić.

Załącznik nr 2

Wzór upoważnienia dla użytkownika do przetwarzania danych osobowych

Nr upoważnienia ……../…./……. Warszawa, dnia ……. r.

(nr kolejny/skrót nazwy departamentu/rok)

MINISTERSTWO
RODZINY, PRACY I POLITYKI SPOŁECZNEJ
00-513 Warszawa, ul. Nowogrodzka 1/3/5,
Regon: 015725935, NIP: 526-28-95-101

UPOWAŻNIENIE

DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 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.) upoważniam:

Panią /Pana[1]

……

(imię i nazwisko)

zatrudnioną / zatrudnionego na stanowisku ……. / wykonującą/wykonującego pracę jako …….. *(należy podać odpowiednio - stażysta, praktykant, wolontariusz albo wykonawca w ramach umowy cywilnoprawnej nr ……..)* w …….*(należy podać nazwę departamentu)* w Ministerstwie Rodziny, Pracy i Polityki Społecznej do przetwarzania danych osobowych w celach związanych z realizacją ……. *(należy podać odpowiednio – zadań służbowych powierzonych przez przełożonego, zadań służbowych określonych w opisie stanowiska pracy, zadań wynikających z udziału w stażu, praktyce lub wolontariacie, zadań niezbędnych do wykonania umowy cywilnoprawnej)* oraz wynikających z realizacji czynności wskazanych w rejestrze czynności przetwarzania danych w zakresie właściwości ……..*(należy podać nazwę departamentu)* tj.:

1…….

2…….

3…….

[1] Niepotrzebne skreślić.

Upoważnienie obejmuje przetwarzanie danych osobowych:

1) w postaci papierowej, zlokalizowanych w systemach tradycyjnych: w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych, w związku z realizacją powierzonych obowiązków pracowniczych;
2) w postaci elektronicznej w systemach teleinformatycznych, w zakresie niezbędnym do wykonywania obowiązków na ww. stanowisku:
   a) …….……
   b) …….….
   c) ……..;
3) w postaci papierowej i postaci elektronicznej w systemach teleinformatycznych w zakresie niezbędnym do wykonywania obowiązków na ww. stanowisku:
   a) ……..
   b) ……..
   c) ……..

Upoważnienie obejmuje przetwarzanie danych osobowych ……(*należy podać odpowiednio*: danych osobowych /danych osobowych szczególnych /danych dotyczących wyroków skazujących*)*.

Upoważnienie ważne jest …….. (*należy podać:* na czas trwania stosunku pracy.- *w przypadku pracowników albo* do dnia zakończenia …… (*należy podać odpowiednio* - stażu, praktyki, wolontariatu, realizacji umowy cywilno-prawnej) tj. na czas nieokreślony/do dnia ……. (*należy podać datę zakończenia wykonywania pracy lub obowiązywania umowy*).

Administrator danych

Z up.

…….

(imię i nazwisko)

……

(stanowisko wystawiającego upoważnienie)

(podpisano kwalifikowanym podpisem elektronicznym)

Załącznik nr 3

Wzór rejestru upoważnień do przetwarzania danych osobowych udzielanych użytkownikom, prowadzonego przez departamenty i Biuro Ministra

Lp.	Departament	Imię i nazwisko użytkownika	Stanowisko służbowe albo informacja o formie wykonywania pracy[1]	Data wydania upoważnienia	Data ustania upoważnienia	Procesy przetwarzania danych osobowych[2]	Kategorie przetwarzanych danych osobowych (dane osobowe, dane osobowe szczególne, dane dotyczące wyroków skazujących)	Informacja o zmianie imienia lub nazwiska użytkownika	Informacja o zmianie stanowiska służbowego niestanowiącej podstawy do zmiany zakresu upoważnienia	Informacja o złożeniu przez użytkownika oświadczania o przestrzeganiu przepisów dotyczących ochrony danych osobowych oraz do zachowania poufności oraz data złożenia oświadczenia	Informacja o złożeniu przez użytkownika oświadczania o zapoznaniu się i zobowiązaniu się do przestrzegania Polityki ochrony danych osobowych oraz data złożenia oświadczenia

[1] Należy podać odpowiednio – stanowisko służbowe w przypadku użytkownika będącego pracownikiem albo informację o formie wykonywania pracy na rzecz Ministerstwa (stażysta, praktykant, wolontariusz, wykonawca w ramach umowy cywilnoprawnej.

[2] Należy podać procesy przetwarzania danych osobowych, w ramach którego użytkownik będzie przetwarzał dane (z rejestru czynności przetwarzania danych osobowych departamentu).

Załącznik nr 4

Wzór oświadczenia użytkownika o przestrzeganiu przepisów dotyczących ochrony danych osobowych oraz zobowiązaniu się do zachowania poufności

Warszawa, dnia ……. / …… / ……

…….

(imię i nazwisko użytkownika)

……

(stanowisko albo informacja o formie wykonywania pracy na rzecz Ministerstwa – stażysta, praktykant, wolontariusz, wykonawca w ramach umowy cywilnoprawnej)

……..

(nazwa departamentu)

Oświadczenie użytkownika o przestrzeganiu przepisów dotyczących ochrony danych osobowych oraz zobowiązaniu się do zachowania poufności.[1]

1. *Zobowiązuję się do przetwarzania danych osobowych zgodnie z powszechnie obowiązującymi przepisami prawa, w szczególności rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* (*Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.) oraz zgodnie z obowiązującymi w Ministerstwie regulacjami wewnętrznymi.*
2. *Oświadczam, że znane mi są przepisy dotyczące ochrony danych osobowych.*
3. *Zobowiązuję się do zapewnienia ochrony przetwarzanych danych osobowych, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnieniem, zabraniem, uszkodzeniem oraz modyfikacją lub zniszczeniem. Zobowiązuję się do natychmiastowego zgłaszania zaobserwowanej próby lub faktu naruszenia zabezpieczenia fizycznego pomieszczenia, bezpieczeństwa danych lub systemu informatycznego przełożonemu i dyrektorowi departamentu.*
4. *Zobowiązuję się do zachowania poufności i nieujawniania osobom trzecim informacji dotyczących przetwarzanych danych.*
5. *Zobowiązuję się do nierozpowszechniania i niewykorzystywania poufnych informacji zdobytych w trakcie wykonywania powierzonych prac, w szczególności informacji dotyczących funkcjonowania systemów służących do przetwarzania danych osobowych, do których zostałam(-em) upoważniona(-y) oraz haseł i zasad dostępu do tych systemów także po ustaniu umowy wiążącej mnie z Ministerstwem. Z chwilą ustania umowy zobowiązuję się do niezwłocznego zwrócenia Ministerstwu wszelkich dokumentów oraz innych materiałów dotyczących danych osobowych.*
6. *Przyjmuję do wiadomości, iż przetwarzanie danych osobowych z naruszeniem udzielonego upoważnienia może skutkować poniesieniem odpowiedzialności dyscyplinarnej i karnej.*

……

podpis użytkownika

/-podpis elektroniczny albo akceptacja elektroniczna-/

[1] Oświadczenie składane jest za pośrednictwem systemu elektronicznego zarządzania dokumentacją do sekretariatu Biura Ministra i do wiadomości dyrektora, a w przypadku braku dostępu do tego systemu oświadczenie jest niezwłocznie przekazywane za pośrednictwem poczty elektronicznej do sekretariatu Biura Ministra i do wiadomości dyrektora.

Załącznik nr 5

Wzór oświadczenia użytkownika o zapoznaniu się i zobowiązaniu się do przestrzegania Polityki ochrony danych osobowych w Ministerstwie Rodziny, Pracy i Polityki Społecznej

Warszawa, dnia ……. / …… / ……

……

(imię i nazwisko użytkownika)

……

(stanowisko albo informacja o formie wykonywania pracy

na rzecz Ministerstwa – stażysta, praktykant, wolontariusz,

wykonawca w ramach umowy cywilnoprawnej)

……

(nazwa departamentu)

Oświadczenie użytkownika o zapoznaniu się i zobowiązaniu się do przestrzegania Polityki ochrony danych osobowych w Ministerstwie Rodziny, Pracy i Polityki

Społecznej[1]

Oświadczam, że zapoznałam się / zapoznałem się[2] z Polityką ochrony danych osobowych w Ministerstwie Rodziny, Pracy i Polityki Społecznej i zobowiązuję się do przestrzegania zawartych w tym dokumencie zasad, reguł i postanowień.

…….

podpis użytkownika/

/-podpis elektroniczny albo akceptacja elektroniczna

[1] Oświadczenie składane jest za pośrednictwem systemu elektronicznego zarządzania dokumentacją, a w przypadku braku dostępu do tego systemu oświadczenie jest niezwłocznie składane za pośrednictwem poczty elektronicznej do sekretariatu BM i do wiadomości dyrektora.

[2] Niepotrzebne skreślić.

Załącznik nr 6

Wzór rejestru czynności przetwarzania danych osobowych

Rejestr czynności przetwarzania danych osobowych	
Nazwa i dane kontaktowe administratora	
Nazwa	
Adres	
Email	
Telefon	

Inspektor Ochrony Danych (jeśli powołano)	
Nazwa	
Adres	
Email	
Telefon	

Przedstawiciel (jeśli wyznaczono)	
Nazwa	
Adres	
Email	
Telefon	

REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

LP.	Nazwa czynności przetwarzania	Jednostka organizacyjna (departament, dział itp.)	Cel przetwarzania	Kategorie osób	Kategorie danych	Podstawa prawna	Źródło danych	Planowany termin usunięcia kategorii danych (jeżeli jest to możliwe)	Nazwa współadministratora i dane kontaktowe (jeśli dotyczy)	Nazwa podmiotu przetwarzającego i dane kontaktowe (jeśli dotyczy)	Kategorie odbiorców (innych niż podmiot przetwarzający)	Nazwa systemu lub oprogramowania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 (jeżeli jest to możliwe)	DPIA (jeśli tak, lokalizacja raportu)	Transfer do kraju trzeciego lub org. międzynarodowej	
															Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń
			Art.. 30 ust. 1 pkt b	Art.. 30 ust. 1 pkt c	Art.. 30 ust. 1 pkt c			Art.. 30 ust. 1 pkt f	Art.. 30 ust. 1 pkt a	Art.. 30 ust. 1 pkt d	Art.. 30 ust. 1 pkt d		Art.. 30 ust. 1 pkt g		Art. 30 ust. 1 pkt e	Art. 30 ust. 1 pkt e
1																
2																
3																
4																
5																
	*Kolorem czerwonym oznaczono informacje wymagane w rejestrze przez art. 30 ust. 1 RODO															

Załącznik nr 7

Wzór rejestru kategorii czynności przetwarzania danych osobowych

Rejestr kategorii czynności przetwarzania danych osobowych	
Nazwa i dane kontaktowe podmiotu przetwarzającego	
Nazwa	
Adres	
Email	
Telefon	
Inspektor Ochrony Danych (jeśli powołano)	
Nazwa	
Adres	
Email	
Telefon	
Administrator w imieniu którego działa podmiot przetwarzający	
Nazwa	
Adres	
Email	
Telefon	

REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Jednostka organizacyjna Ministerstwa odpowiedzialna za przetwarzanie powierzonych danych (departament, biuro, wydział itp.);	Kategorie przetwarzań	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	Administrator	Administrator	Administrator	Administrator		Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit 2 RODO	Podprzetwarzający (podwykonawca) - jeśli dotyczy:	Podprzetwarzający (podwykonawca) - jeśli dotyczy:
		Art.. 30 ust. 2 lit. b	Art.. 30 ust. 2 lit. d, art.32 ust. 1	Nazwa i dane kontaktowe administratora	Nazwa i dane kontaktowe współadministratora (jeśli dotyczy)	Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono)	Inspektor ochrony danych administratora (jeśli powołano)	Czas trwania przetwarzania	(art. 30 ust. 2 lit. c RODO)	(art. 30 ust. 2 lit. c RODO	Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy),	Kategorie podpowierzonych przetwarzań.
				art. 30 ust. 2 lit. a RODO)	art. 30 ust. 2 lit. a RODO)	art. 30 ust. 2 lit. a RODO)	art. 30 ust. 2 lit. a RODO)					
1												
2												
3												
4												
	*Kolorem czerwonym oznaczono informacje wymagane w rejestrze przez art. 30 ust. 1 RODO											

Załącznik nr 8

Wzór minimalnego zakresu danych ujętych w klauzuli informacyjnej w przypadku zbierania danych osobowych od osoby, której dane dotyczą

Klauzula informacyjna kierowana do osoby w przypadku zbierania danych osobowych od osoby, której dane dotyczą – minimalny zakres danych

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.) (RODO) informuję:

1. Administratorem Pani/ Pana danych osobowych jest Minister Rodziny, Pracy i Polityki Społecznej z siedzibą w Warszawie przy ul. Nowogrodzkiej 1/3/5, 00 513 Warszawa.
2. Z administratorem danych można się skontaktować przez adres mailowy ……. (*należy wstawić aktualny adres poczty elektronicznej przeznaczonej do kontaktu z obywatelami, zamieszczony na stronie internetowej Ministerstwa np. info@mrpips.gov.pl*), lub pisemnie na adres siedziby administratora.
3. Z Inspektorem Ochrony Danych można się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych w szczególności w zakresie korzystania z praw związanych z ich przetwarzaniem przez adres mailowy ……. (*należy wstawić aktualny adres poczty elektronicznej przeznaczonej do kontaktów z Inspektorem Ochrony Danych np. iodo@mrpips.gov.pl*) lub pisemnie na adres siedziby administratora.
4. Podstawą prawną przetwarzania Pani/Pana danych jest[1]:
   1) art. 6 ust 1 lit. a RODO, tj. zgoda osoby, której dane dotyczą, w każdej chwili przysługuje Pani/Panu prawo do wycofania zgody na przetwarzanie danych osobowych, ale cofnięcie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie Pani/Pana zgody przed jej wycofaniem.
   2) art. 6 ust 1 lit. b RODO, tj. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
   3) art. 6 ust. 1 lit. c RODO, tj. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze w związku z (należy wskazać proces lub przepis prawa, z którego wynika konieczność przetwarzania danych, jak najbardziej precyzyjnie podać podstawę prawną, z której wynika obowiązek, tj. odwołanie się do konkretnego przepisu z ustawy np. art. 22^1 Kodeksu pracy);
   4) art. 6 ust. 1 lit. e RODO, tj. przetwarzanie jest niezbędne do wykonania zdania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej

[1] Niepotrzebne skreślić

powierzonej Ministrowi w związku z (należy wskazać proces, z którym wiąże się konieczność przetwarzania danych);

5) art. 6 ust. 1 lit. f RODO, tj. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora, tj. (należy wskazać proces, z którym wiąże się konieczność przetwarzania danych)[1].

5. Pani/Pana dane przetwarzane są w celu (wskazać cel).
6. Pani/Pana dane osobowe mogą być udostępnione (należy wskazać, komu dane mogą być udostępniane albo wskazać, że dane nie będą udostępnianie z wyjątkiem określonych sytuacji i wskazać te sytuacje).
7. Pani/Pana dane będą przechowywane do momentu wygaśnięcia obowiązku przechowywania danych wynikającego z przepisów, tj. przez okres (wskazać okres).
8. Przysługuje Pani/Panu – z zastrzeżeniem ograniczeń wynikających z przepisów prawa – prawo do dostępu do swoich danych osobowych, prawo żądania ich sprostowania oraz ograniczenia ich przetwarzania.
9. Przysługuje Pani/ Panu prawo do żądania usunięcia danych osobowych, jeżeli dane osobowe nie są niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane[2].
10. W zakresie udostępnienia danych – z zastrzeżeniem ograniczeń wynikających z przepisów prawa – przysługuje Pani/Panu prawo do wniesienia sprzeciwu wobec przetwarzania.
11. Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych w państwie członkowskim zwykłego pobytu, miejsca pracy lub miejsca popełnienia domniemanego naruszenia.
12. Pani/Pana dane nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.
13. Podanie danych osobowych jest dobrowolne/obowiązkowe[1] i wynika z wyżej wskazanych przepisów prawa (*należy pozostawić właściwe*), ale niezbędne do rozpatrzenia Pani/Pana sprawy.

[1] Art. 6 ust 1 lit f RODO – nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.
Akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.
Na prawnie uzasadniony interes nie mogą powoływać się – zgodnie z zastrzeżeniem poczynionym w art. 6 ust. 1 *in fine* RODO – organy publiczne w ramach realizacji swoich zadań [zob. W. Chomiczewski, D. Lubasz, A. Maciaszczyk, A. Szkurłat, *Wybrane podstawy prawne przetwarzania danych osobowych: ochrona żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, zadania realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej, prawnie uzasadniony interes realizowany przez administratora lub stronę trzecią*, LEX/el. 2023.

[2] Uwzględnić w przypadku, gdy przetwarzanie odbywa się na podstawie zgody.

Załącznik nr 9

Wzór minimalnego zakresu danych ujętych w klauzuli informacyjnej w przypadku zbierania danych osobowych w sposób inny niż od osoby, której dane osobowe dotyczą

Klauzula informacyjna kierowana do osoby w przypadku zbierania danych osobowych w sposób inny niż od osoby, której dane osobowe dotyczą – minimalny zakres danych

Zgodnie z art. 14 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.) (RODO) informuję, że:

1. Administratorem Pani/Pana danych osobowych jest Minister Rodziny, Pracy i Polityki Społecznej z siedzibą w Warszawie przy ul. Nowogrodzkiej 1/3/5, 00 513 Warszawa.
2. Z administratorem danych można się skontaktować przez adres mailowy ……. (*należy wstawić aktualny adres poczty elektronicznej przeznaczonej do kontaktu z obywatelami, zamieszczony na stronie internetowej Ministerstwa np. info@mrpips.gov.pl)* lub pisemnie na adres siedziby administratora.
3. Z Inspektorem Ochrony Danych można się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych, w szczególności w zakresie korzystania z praw związanych z ich przetwarzaniem przez adres mailowy ……. (*należy wstawić aktualny adres poczty elektronicznej przeznaczonej do kontaktów z Inspektorem Ochrony Danych np. iodo@mrpips.gov.pl)* lub pisemnie na adres siedziby administratora.
4. Podstawą prawną przetwarzania Pani/Pana danych osobowych jest[1]
    1) art. 6 ust. 1 lit. b RODO, tj. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
    2) art. 6 ust. 1 lit. c RODO, tj. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze w związku z (należy wskazać proces lub przepis prawa, z którego wynika konieczność przetwarzania danych);
    3) art. 6 ust. 1 lit. e RODO, tj. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Ministrowi w związku z (należy wskazać proces, z którym wiąże się konieczność przetwarzania danych);
    4) art. 6 ust. 1 lit. f RODO, tj. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora, tj. (należy wskazać proces, z którym wiąże się konieczność przetwarzania danych).
5. Pani/Pana dane osobowe zostały przekazane przez (należy wskazać kto jest źródłem danych).
6. Przetwarzanie danych osobowych obejmuje następujące kategorie Pani/Pana danych: (należy wskazać dane, które są przetwarzane).

[1] Niepotrzebne skreślić

7. Pani/Pana dane osobowe mogą być udostępniane (należy wskazać, komu dane mogą być udostępniane albo wskazać, że dane nie będą udostępnianie z wyjątkiem określonych sytuacji i wskazać te sytuacje).
8. Pani/Pana dane osobowe będą przechowywane do momentu wygaśnięcia obowiązku przechowywania danych wynikającego z przepisów, tj. przez okres (wskazać okres).
9. Przysługuje Pani/Panu – z zastrzeżeniem ograniczeń wynikających z przepisów prawa – prawo do dostępu do swoich danych osobowych, prawo żądania ich sprostowania oraz ograniczenia ich przetwarzania.
10. Przysługuje Pani/Panu prawo do żądania usunięcia danych osobowych[2], jeżeli dane osobowe nie są niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane.
11. W zakresie udostępnienia danych przysługuje Pani/Panu – z zastrzeżeniem ograniczeń wynikających z przepisów prawa – prawo do wniesienia sprzeciwu wobec przetwarzania.
12. Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych w państwie członkowskim Pani/Pana zwykłego pobytu, miejsca pracy lub miejsca popełnienia domniemanego naruszenia.
13. Pani/Pana dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

[2] Uwzględnić w przypadku, gdy przetwarzanie odbywa się na podstawie zgody.

Załącznik nr 11

Wzór zgody osoby, której dane są przetwarzane w Ministerstwie Rodziny, Pracy i Polityki Społecznej

……

miejscowość, data,

……

imię i nazwisko

……

Adres

……

Adres poczty elektronicznej

Zgoda na przetwarzanie danych osobowych

Czy wyraża Pan/Pani zgodę na przetwarzanie Pana/Pani danych osobowych [wskazać zakres i kategorie danych] przez …… [wskazać administratora][1] z siedzibą przy [.....] w celu …….[wskazać cel]? [2]

□ TAK

□ NIE

Jestem świadoma(-my) przysługującego mi prawa do wycofania zgody, jak również faktu, że wycofanie zgody nie ma wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

Zgodę mogę odwołać przez wysłanie maila na adres ……. (*należy wstawić aktualny adres poczty elektronicznej przeznaczonej do kontaktów z Inspektorem Ochrony Danych np. (iodo@mrpips.gov.pl)*lub za pośrednictwem potwierdzonego profilu e-PUAP z informacją o jej odwołaniu (w treści maila wskażę swoje imię

[1]np. Minister Rodziny, Pracy i Polityki Społecznej w Warszawie z siedzibą ul. Nowogrodzka 1/3/5, 00-513 Warszawa.

[2] Jeśli administrator zbiera kilka zgód dot. różnych celów przetwarzania, zgody te muszą zostać wyrażone osobno. Niedozwolone jest zbiorcze zbieranie zgód. Należy pamiętać, że ponieważ dla organów publicznych podstawę prawną przetwarzania danych osobowych powinien określić ustawodawca, w sytuacji, gdy administrator ma inną przesłankę przetwarzania danych osobowych niż zgoda, to wtedy nie powinien pozyskiwać zgody. osoba wyrażająca zgodę musi zrozumieć istotę zgody, jej cel i skutki, posiadać pełne rozeznanie konkretnie przez kogo i w jakim ściśle określonym celu jej dane będą przetwarzane. Podmioty publiczne co do zasady przetwarzają dane na podstawie i w granicach określonych przez przepisy prawa odnoszące się do jego działalności. Z tego względu w przypadku tych podmiotów właściwymi podstawami do przetwarzania danych osobowych powinna być przesłanka określona w art. 6 ust. 1 lit. c lub e RODO, w połączeniu z właściwymi przepisami szczególnymi określającymi zadania konkretnych organów i instytucji, a zatem gdy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze lub gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. **Zgoda osoby, której dane dotyczą, mogłaby stanowić podstawę przetwarzania danych przez podmiot publiczny w sytuacjach, gdyby przewidywały to przepisy prawa** (przykładem jest art. 4 ust. 3 ustawy z dnia 11 lipca 2014 r. o petycjach (Dz. U. z 2018 r. poz. 870), zgodnie z którym petycja może zawierać zgodę na ujawnienie na stronie internetowej podmiotu rozpatrującego petycję lub urzędu go obsługującego danych osobowych podmiotu wnoszącego petycję). co do zasady aby podmiot publiczny mógł przetwarzać dane osobowe na podstawie zgody osoby, której dane dotyczą, takie uprawnienie lub obowiązek musiałby wynikać z przepisów prawa.

i nazwisko, a w tytule wiadomości wpiszę „……*), lub listownie na adres Ministerstwa Rodziny, Pracy i Polityki Społecznej.

.....

Podpis osoby wyrażającej zgodę

*W tym miejscu należy podać datę i nazwę czynności, w ramach której udzielono zgody, np. udział w konferencji/ szkoleniu.

Załącznik nr 10

Wzór rejestru wniosków osób w zakresie realizacji ich praw związanych z ochroną danych osobowych

Lp.	**Informacje o wystąpieniu zdarzenia i stwierdzeniu naruszenia**			**Okoliczności naruszenia**				**Skutki naruszenia**	**Środki naprawcze i zaradcze**			**Zgłoszenie naruszenia do Prezesa Urzędu Ochrony Danych Osobowych**			**Uwagi**
	Data zdarzenia	Data i źródło uzyskania informacji	Data i godzina stwierdzenia naruszenia	Charakter naruszenia	Kategorie osób	Liczba osób	Kategoria i liczba wpisów	Opis konsekwencji naruszenia	Czy poinformowano osoby, których dane dotyczą? (jeśli tak, to w jaki sposób, jeśli nie, to dlaczego)	Działania naprawcze	Działania zaradcze	Czy dokonano zgłoszenia? (jeśli nie, przyczyna niedokonania zgłoszenia)	Data zgłoszenia	Data zgłoszenia uzupełniającego	

Załącznik nr 12

Wzór rejestru zgód osób, których dane dotyczą, na przetwarzanie ich danych osobowych

Lp.	Dane wnioskodawcy - imię i nazwisko	Adres do korespondencji lub adres poczty elektronicznej osoby	Data udzielenia zgody	Okoliczność, w związku z którą zgoda została udzielona	Kategorie danych, których dotyczy zgoda	Data wycofania zgody (jeżeli dotyczy)	Uwagi

Załącznik nr 13

Wzór rejestru naruszeń ochrony danych osobowych

Lp.	**Informacje o wystąpieniu zdarzenia i stwierdzeniu naruszenia**			**Okoliczności naruszenia**				**Skutki naruszenia**	**Środki naprawcze i zaradcze**			**Zgłoszenie naruszenia do Prezesa Urzędu Ochrony Danych Osobowych**			**Uwagi**
	Data zdarzenia	Data i źródło uzyskania informacji	Data i godzina stwierdzenia naruszenia	Charakter naruszenia	Kategorie osób	Liczba osób	Kategoria i liczba wpisów	Opis konsekwencji naruszenia	Czy poinformowano osoby, których dane dotyczą? (jeśli tak, to w jaki sposób, jeśli nie, to dlaczego)	Działania naprawcze	Działania zaradcze	Czy dokonano zgłoszenia? (jeśli nie, przyczyna niedokonania zgłoszenia)	Data zgłoszenia	Data zgłoszenia uzupełniającego	