Spis treści:

1. Ustawa o ochronie danych osobowych a RODO. Co zmieniło się 25 maja 2018 r.?

Regulacja prawna	Ustawa z dnia 29.08.2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922)	RODO i ustawa z dnia 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000)
Obowiązek posiadania polityki bezpieczeństwa danych	Rozdział 5. ustawy – art. od 36 do 39a	Art. 24 RODO
Podstawa prawna przetwarzania danych	Art. 23 ustawy	Art. 6 RODO
Zasady odpowiedzialności	?	Art. 82, 83 i 84 RODO

Rozdział 5 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U.2016.922 t.j.)

Art. 36 1. Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1.

Art. 36a. 1. Administrator danych może powołać administratora bezpieczeństwa informacji.

2. Do zadań administratora bezpieczeństwa informacji należy:

1) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,

b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych,

c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

2) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7.

3. Rejestr, o którym mowa w ust. 2 pkt 2, jest jawny. Przepis art. 42 ust. 2 stosuje się odpowiednio.

4. Administrator danych może powierzyć administratorowi bezpieczeństwa informacji wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań, o których mowa w ust.2.

5. Administratorem bezpieczeństwa informacji może być osoba, która:

1) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;

2) posiada odpowiednią wiedzę w zakresie ochrony danych osobowych;

3) nie była karana za umyślne przestępstwo.

6. Administrator danych może powołać zastępców administratora bezpieczeństwa informacji, którzy spełniają warunki określone w ust. 5.

7. Administrator bezpieczeństwa informacji podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych.

8. Administrator danych zapewnia środki i organizacyjną odrębność administratora bezpieczeństwa informacji niezbędne do niezależnego wykonywania przez niego zadań, o których mowa w ust. 2.

9. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia:

1) tryb i sposób realizacji zadań, o których mowa w ust. 2 pkt 1 lit. a i b,

2) sposób prowadzenia rejestru zbiorów danych, o którym mowa w ust. 2 pkt 2

–uwzględniając konieczność zapewnienia prawidłowości realizacji zadań administratora bezpieczeństwa informacji oraz niezależności i organizacyjnej odrębności w wykonywaniu przez niego zadań.

Art. 36b. W przypadku niepowołania administratora bezpieczeństwa informacji zadania określone w art. 36a ust. 2 pkt 1, z wyłączeniem obowiązku sporządzania sprawozdania, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, wykonuje administrator danych.

Artykuł 24 RODO

Obowiązki administratora

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.
2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.
3. Stosowanie zatwierdzonych kodeksów postępowania, o których mowa wart. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa wart. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

Artykuł 25 RODO

Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania –wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.
2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.
3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 i 2 niniejszego artykułu, można wykazać między innymi poprzez wprowadzenie zatwierdzonego mechanizmu certyfikacji określonego w art. 42.

2. RODO – czym jest i jaki jest zakres jego zastosowania.

„RODO" to 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).

Jest to wspólnotowy akt prawny normujący zasady ochrony danych osobowych – zastępuje dyrektywę 95/46/WE z 1995 r. RODO tym się różni od dyrektywy 95/46/WE, że nie będzie implementowane, czyli nie będzie trzeba przepisów RODO przyjąć w polskiej ustawie, jak to się dzieje w przypadku dyrektyw. RODO obowiązuje bezpośrednio, jest bezpośrednio stosowane i bezpośrednio skuteczne.

3. Urząd Ochrony Danych Osobowych – czym jest i jakie ma kompetencje?

Urząd Ochrony Danych Osobowych zapewnia wykonanie zadań wynikających z kompetencji Prezesa Urzędu Ochrony Danych Osobowych, zwanego dalej „Prezesem Urzędu", określonych w rozporządzeniu 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 (Dz. U. UE. L. z 2016 r. Nr 119), zwanego dalej „rozporządzeniem 2016/679", ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000), a także w innych przepisach powszechnie obowiązującego prawa (§ 1 statutu).

Co może UODO? -> regulacja art. 9 ustawy o ochronie danych osobowych „Kontrola przestrzegania przepisów o ochronie danych osobowych"

Art. 78 ustawy

1. Prezes Urzędu przeprowadza kontrolę przestrzegania przepisów o ochronie danych osobowych.
2. Kontrolę prowadzi się zgodnie z zatwierdzonym przez Prezesa Urzędu planem kontroli lub na podstawie uzyskanych przez Prezesa Urzędu informacji lub w ramach monitorowania przestrzegania stosowania rozporządzenia 2016/679.

Art. 82 ustawy

1. Prezes Urzędu może upoważnić do udziału w kontroli osobę posiadającą wiedzę specjalistyczną, jeżeli przeprowadzenie czynności kontrolnych wymaga takiej wiedzy. Przepisy art. 80 i art. 81 ust. 2 stosuje się.
2. Zakres uprawnień osoby, o której mowa w ust. 1, Prezes Urzędu określa w upoważnieniu.
3. Osoba, o której mowa w ust. 1, jest obowiązana do zachowania w tajemnicy informacji, o których dowiedziała się w toku kontroli.

Art. 83 ustawy

1. Czynności kontrolnych dokonuje się w obecności kontrolowanego lub osoby przez niego upoważnionej.
2. Kontrolowany jest obowiązany do pisemnego wskazania osoby upoważnionej do reprezentowania go w trakcie kontroli.
3. W razie nieobecności kontrolowanego lub osoby przez niego upoważnionej, upoważnienie do przeprowadzenia kontroli oraz legitymacja służbowa lub dokument potwierdzający tożsamość mogą być okazane:

1)osobie czynnej w lokalu przedsiębiorstwa w rozumieniu art. 97 ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny (Dz. U. z 2017 r. poz. 459, 933 i 1132 oraz z 2018 r. poz. 398 i 650) lub

2)przywołanemu świadkowi, jeżeli jest funkcjonariuszem publicznym w rozumieniu art. 115 § 13 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny (Dz. U. z 2017 r. poz. 2204 oraz z 2018 r. poz. 20, 305 i 663), niebędącemu pracownikiem Urzędu albo osobą, o której mowa w art. 80 ust. 1.

Art. 84 ustawy

1. Kontrolujący ma prawo:

1)wstępu w godzinach od 6^{00} do 22^{00} na grunt oraz do budynków, lokali lub innych pomieszczeń;

2)wglądu do dokumentów i informacji mających bezpośredni związek z zakresem przedmiotowym kontroli;

3)przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych;

4)żądać złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwać w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego;

5)zlecać sporządzanie ekspertyz i opinii.

2. Kontrolowany zapewnia kontrolującemu oraz osobom upoważnionym do udziału w kontroli warunki i środki niezbędne do sprawnego przeprowadzenia kontroli, a w szczególności sporządza we własnym

zakresie kopie lub wydruki dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub systemach, o których mowa w ust. 1 pkt 3.

3. Kontrolowany dokonuje potwierdzenia za zgodność z oryginałem sporządzonych kopii lub wydruków, o których mowa w ust. 2. W przypadku odmowy potwierdzenia za zgodność z oryginałem kontrolujący czyni o tym wzmiankę w protokole kontroli.

4. W uzasadnionych przypadkach przebieg kontroli lub poszczególne czynności w jej toku, po uprzednim poinformowaniu kontrolowanego, mogą być utrwalane przy pomocy urządzeń rejestrujących obraz lub dźwięk. Informatyczne nośniki danych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570 oraz z 2018 r. poz. 1000), na których zarejestrowano przebieg kontroli lub poszczególne czynności w jej toku, stanowią załącznik do protokołu kontroli.

Art. 85 ustawy

1. Prezes Urzędu lub kontrolujący może zwrócić się do właściwego miejscowo komendanta Policji o pomoc, jeżeli jest to niezbędne do wykonywania czynności kontrolnych.

2. Policja udziela pomocy przy wykonywaniu czynności kontrolnych, po otrzymaniu pisemnego wezwania na co najmniej 7 dni przed terminem tych czynności.

3. W pilnych przypadkach, w szczególności gdy kontrolujący trafi na opór uniemożliwiający lub utrudniający wykonywanie czynności kontrolnych, udzielenie pomocy następuje również na ustne wezwanie Prezesa Urzędu lub kontrolującego, po okazaniu imiennego upoważnienia do przeprowadzenia kontroli oraz legitymacji służbowej kontrolującego.

4. W przypadku, o którym mowa w ust. 3, Prezes Urzędu przekazuje potwierdzenie wezwania na piśmie, nie później niż w terminie 3 dni po zakończeniu czynności kontrolnych.

5. Udzielenie pomocy Policji przy wykonywaniu czynności kontrolnych polega na zapewnieniu kontrolującemu bezpieczeństwa osobistego oraz dostępu do miejsca wykonywania kontroli i porządku w tym miejscu.

6. Policja, udzielając pomocy kontrolującemu przy wykonywaniu czynności kontrolnych, zapewnia bezpieczeństwo również innym osobom uczestniczącym przy wykonywaniu czynności kontrolnych, mając w szczególności na względzie poszanowanie godności osób biorących udział w kontroli.

7. Koszty poniesione przez Policję z tytułu udzielonej pomocy przy wykonywaniu czynności kontrolnych rozlicza się według stawki zryczałtowanej w wysokości 1,5% przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw bez wypłat nagród z zysku w czwartym kwartale roku poprzedniego, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego na podstawie art. 7 ust. 1 ustawy z dnia 17 lipca 1998 r. o pożyczkach i kredytach studenckich (Dz. U. z 2017 r. poz. 357).

Art. 86. ustawy

1. Kontrolujący może przesłuchać pracownika kontrolowanego w charakterze świadka.
2. Za pracownika kontrolowanego uznaje się osobę zatrudnioną na podstawie stosunku pracy lub wykonującą pracę na podstawie umowy cywilnoprawnej.
3. Do przesłuchania pracownika kontrolowanego stosuje się przepis art. 83 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego.

Art. 87 ustawy

Kontrolujący ustala stan faktyczny na podstawie dowodów zebranych w postępowaniu kontrolnym, a w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń.

Art. 89 ustawy

1. Kontrolę prowadzi się nie dłużej niż 30 dni od dnia okazania kontrolowanemu lub innej osobie wskazanej w przepisach imiennego upoważnienia do przeprowadzenia kontroli oraz legitymacji służbowej lub innego dokumentu potwierdzającego tożsamość. Do terminu nie wlicza się terminów przewidzianych na zgłoszenie zastrzeżeń do protokołu kontroli lub podpisanie i doręczenie protokołu kontroli przez kontrolowanego.
2. Terminem zakończenia kontroli jest dzień podpisania protokołu kontroli przez kontrolowanego albo dzień dokonania wzmianki, o której mowa w art. 88 ust. 8.

4. Ocena skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Analiza ryzyka i standardy zabezpieczeń.

.

Założeniem RODO jest minimalizacja formalizmu i dokumentacji przy jednoczesnej maksymalizacji efektów w postaci rzeczywistej ochrony danych osobowych.

RODO odchodzi od praktyki polegającej na wskazywaniu w przepisach prawa konkretnych środków zabezpieczenia danych osobowych, jakie mają zostać wdrożone przez administratora lub podmiot przetwarzający. Zamiast tego, RODO wprowadza tzw. **podejście oparte na ryzyku.**

Istota podejścia opartego na ryzyku sprowadza się do tego, że każdy podmiot przetwarzający dane osobowe powinien samodzielnie określić, jakie konkretne środki zabezpieczenia danych należy wdrożyć.

Dobór środków zabezpieczenia powinien być oparty o:

a) charakter, zakres, kontekst i cele przetwarzania,

b) ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia,

c) stan wiedzy technicznej,

d) koszt wdrażania.

Każdy podmiot przetwarzający dane osobowe powinien więc:

a) ustalić, jakie dane osobowe, w jakim charakterze, po co i w jakim środowisku przetwarza,

b) określić ryzyko naruszenia praw lub wolności osób fizycznych związane z takim przetwarzaniem,

c) dobrać odpowiednie środki zabezpieczenia danych, uwzględniając istniejące możliwości techniczne i własne możliwości finansowe.

Z czym się to wiąże w praktyce ośrodków pomocy społecznej? Możemy sformułować kilka podstawowych założeń i celów, które będą musiały być wprowadzone w praktyce:

1) **Punktem wyjścia będzie przeprowadzenie wskazanej wcześniej analizy ryzyka.**
2) **W oparciu o przeprowadzoną analizę ryzyka należy dokonać analizy dotychczasowej polityki bezpieczeństwa informacji i wybrać docelową strukturę nowej dokumentacji.**
3) **Należy ustalić jakich dokumentów brakuje w dotychczasowej dokumentacji, a jakie dokumenty są zbędne i można z ich zrezygnować.**
4) **Należy opracować brakującą dokumentację.**
5) **Należy wdrożyć faktyczne procedury ochrony danych osobowych przewidziane w opracowanej dokumentacji.**

ANKIETA RYZYKA - propozycja

Pytania dotyczące charakteru przetwarzanych danych osobowych:

Czy przetwarzanie może skutkować:	BRAK RYZYKA	ZNIKOME RYZYKO	ŚREDNIE RYZYKO	WYSOKIE RYZYKO
dyskryminacją				
kradzieżą tożsamości lub oszustwem dotyczącym tożsamości				
stratą finansową				
naruszeniem dobrego imienia				
naruszeniem poufności danych osobowych chronionych tajemnicą zawodową				
wszelką inną znaczną szkodą gospodarczą lub społeczną				

Pytania dotyczące kwestii organizacyjno-technicznych:

Czy w odniesieniu do przetwarzanych danych osobowych:	BRAK RYZYKA	ZNIKOME RYZYKO	ŚREDNIE RYZYKO	WYSOKIE RYZYKO
istnieje ryzyko dostępu osób trzecich do dokumentacji papierowej zawierającej dane osobowe w godzinach pracy urzędu				
istnieje ryzyko dostępu osób trzecich do dokumentacji elektronicznej zawierającej dane osobowe w godzinach pracy urzędu				
istnieje ryzyko dostępu osób trzecich do dokumentacji papierowej zawierającej dane osobowe poza godzinami pracy urzędu				

istnieje ryzyko dostępu osób trzecich do dokumentacji elektronicznej zawierającej dane osobowe poza godzinami pracy urzędu				
istnieje ryzyko wyniesienia dokumentacji zawierającej dane osobowe poza budynek urzędu				
istnieje ryzyko skopiowania przez osobę trzecią dokumentów zawierających dane osobowe przetwarzane w urzędzie				
istnieje ryzyko kradzieży dokumentów zawierających dane osobowe przetwarzane w urzędzie				
istnieje ryzyko zagubienia dokumentów zawierających dane osobowe przetwarzane w urzędzie				
istnieje ryzyko stosowania przez osoby trzecie podsłuchu bezpośredniego lub akustycznego z wykorzystaniem mikrofonów kierunkowych lub instalacji technicznych				
istnieje ryzyko zagubienia elektronicznych nośników danych zawierających dane osobowe przetwarzane w urzędzie				

Pytania dotyczące zabezpieczenia sprzętu elektronicznego:

Czy w odniesieniu do przetwarzanych danych osobowych:	BRAK RYZYKA	ZNIKOME RYZYKO	ŚREDNIE RYZYKO	WYSOKIE RYZYKO
istnieje ryzyko włamania do systemu poprzez podszycie się pod uprawnionego użytkownika				
istnieje ryzyko nieuprawnionego instalowania urządzeń służących do naruszenia poufności przetwarzanych				
istnieje ryzyko nieuprawnionej, świadomej modyfikacji oprogramowania zainstalowanego na komputerze pracownika przez osoby trzecie				
istnieje ryzyko użycia oprogramowania zainstalowanego na komputerach pracowników w nieuprawniony sposób				
istnieje ryzyko korzystania z nielicencjonowanego oprogramowania na komputerach pracowników				
istnieje ryzyko przeglądania (przeszukiwania) pamięci operacyjnej i zewnętrznej komputerów w celu uzyskania określonych informacji				
istnieje ryzyko wykorzystania pozostawionych na dysku twardym komputera plików roboczych wytworzonych przez oprogramowanie				
istnieje ryzyko skopiowania/kradzieży danych osobowych podczas wykonywania napraw i konserwacji komputerów				
istnieje ryzyko przypadkowej zmiany ustawień konfiguracyjnych na komputerach				
istnieje ryzyko nieupoważnionego uruchomienia komputera z nośnika zewnętrznego (ominięcie mechanizmów bezpieczeństwa systemu operacyjnego i systemu plików NTFS i odczytanie zawartości przetwarzanych dokumentów)				

Szacowanie poziomu ryzyka

$$\text{Poziom ryzyka} = \frac{0\text{xBR} + 0{,}5\text{xZR} + 1\text{xŚR} + 1{,}5\text{xWR}}{\text{liczba czynników ryzyka}}$$

gdzie: BR – brak ryzyka, ZR – znikome ryzyko, ŚR – średnie ryzyko, WR – wysokie ryzyko

Skala oceny:

0 - 0,25 – brak ryzyka

0,26 – 0,75 – znikome ryzyko

0,76 – 1,25 – średnie ryzyko

1,26 - 1,5 – wysokie ryzyko

5. Jak powinna wyglądać polityka bezpieczeństwa danych osobowych dostosowana do RODO? Analiza przykładowej dokumentacji.

Administrator Danych – Kierownik Ośrodka Pomocy Społecznej w ……..

dnia 24.05.2018 r. w podmiocie o nazwie: Ośrodek Pomocy Społecznej w ……

(zwanym dalej „Ośrodkiem")

zgodnie z 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 (określanym dalej jako „RODO")

wdraża dokument o nazwie „Polityka Bezpieczeństwa Danych Osobowych".

Postanowienia tego dokumentu wchodzą w życie z dniem 25.05.2018 r.

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w podmiocie określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych, oraz w systemach informatycznych.

Polityka Bezpieczeństwa Danych Osobowych obejmuje następujące dokumenty:

1. Strategia bezpieczeństwa i zasady przetwarzania danych.
    a. Ocena skutków planowanych operacji przetwarzania dla ochrony danych osobowych;
    b. Procedury i sposoby zagwarantowania realizacji praw osób, których dane są przetwarzane;
    c. Zasady powoływania i funkcjonowania inspektora ochrony danych osobowych.
2. Rejestr operacji przetwarzania danych osobowych.
3. Polityka monitorowania i reagowania na naruszenia ochrony danych.
4. Rejestr incydentów.
5. Procedury zarządzania użytkownikami i dostępem do danych.
    a. Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe;
    b. Ewidencja osób upoważnionych do przetwarzania danych osobowych;
    c. Wzór oświadczenia o zachowaniu poufności;
    d. Wykaz podmiotów przetwarzających dane na zlecenie administratora danych.

1. Strategia bezpieczeństwa i zasady przetwarzania danych.

a) Ocena skutków planowanych operacji przetwarzania dla ochrony danych osobowych

Mając na uwadze unormowania art. 35 ust. 1 RODO w nawiązaniu do pkt 89-91 preambuły RODO, administrator danych dokonał oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Jednocześnie wskazuje się, że podstawą prawną przetwarzania danych jest niezbędność do wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c) RODO), co, zgodnie z treścią art. 35 ust. 10 RODO, nadaje niniejszej ocenie charakter fakultatywny.

Przedmiotowa ocena, zgodnie z regulacją art. 35 ust. 4 RODO, zawiera:

1) opis planowanych operacji przetwarzania i celów przetwarzania;

2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
3) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą dokonaną na podstawie przeprowadzonych dla poszczególnych procesów przetwarzania danych ankiet ryzyka;
4) wykaz zastosowanych oraz planowanych środków zabezpieczenia oraz mechanizmów bezpieczeństwa mających zapewnić ochronę danych osobowych.

Ad. 1

Opis planowanych operacji przetwarzania i celów przetwarzania

Przetwarzanie danych w tut. podmiocie dokonywane jest w celu wszczęcia oraz prowadzenia postępowań administracyjnych na podstawie:

- ustawy z dnia 12 marca 2004 r. o pomocy społecznej;
- ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu przemocy w rodzinie;
- ustawy z dnia 9 czerwca 2011 r. o wspieraniu rodziny i systemie pieczy zastępczej;
- ustawy z dnia 26 października 1982 roku o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi;
- ustawy z dnia 29 lipca 2005 roku o przeciwdziałaniu narkomanii;
- ustawy z dnia 21 czerwca 2001 r. o dodatkach mieszkaniowych;
- ustawy z dnia 10 kwietnia 1997 roku prawo energetyczne;
- ustawy z 19 sierpnia 1994 r. o ochronie zdrowia psychicznego;
- ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych;
- ustawy z dnia 28 listopada 2003 r. o świadczeniach rodzinnych;
- ustawy z dnia 4 kwietnia 2014 r. o ustaleniu i wypłacie zasiłków dla opiekunów;
- ustawy z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów;
- ustawy z dnia 11 lutego 2016r. o pomocy państwa w wychowywaniu dzieci;
- ustawy z dnia 5 grudnia 2014r o Karcie Dużej Rodziny;
- ustawy z dnia 4 listopada 2016r o wsparciu kobiet w ciąży i rodzin „Za życiem”.

Realizowane operacje przetwarzania danych:

1) operacje przetwarzania danych pracowniczych (rekrutacja; prowadzenie rejestru pracowników, akt pracowniczych, ewidencji czasu pracy; zgłaszanie pracowników i członków ich rodzin do ZUS, aktualizacja zgłoszeń i przekazywanie danych o zwolnieniach; prowadzenie rozliczeń z pracownikami;

2) operacje przetwarzania danych klientów oraz członków ich rodzin (przyjmowanie wniosków i podań o przyznanie różnych form pomocy lub świadczeń; samodzielne zbieranie danych przy przeprowadzaniu wywiadów środowiskowych; pozyskiwanie danych z rejestrów centralnych oraz od innych podmiotów – publicznych i prywatnych; profilowanie klientów w zakresie ustalenia możliwych dalszych form pomocy oraz eliminacji przyczyn, dla których konieczne było udzielenie pomocy; wydawanie decyzji administracyjnych; monitoring sytuacji rodzinnej i zawodowej w zakresie zasadności dalszego uzyskiwania pomocy lub świadczeń).

Ad. 2.

Ocena, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów.

Wszystkie realizowane operacje przetwarzania danych wynikają wprost z przepisów prawa powszechnie obowiązującego, stanowiąc wyraz wypełniania obowiązku prawnego ciążącego na administratorze, w związku z czym są one niezbędne oraz proporcjonalne w stosunku do celów.

Ad. 3.

Ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą została dokonana w oparciu o ankiety ryzyka przeprowadzone dla następujących procesów przetwarzania:

1) Przetwarzanie danych osobowych na potrzeby postępowań z zakresu pomocy społecznej.
2) Przetwarzanie danych osobowych na potrzeby postępowań z zakresu świadczeń rodzinnych i wychowawczych, funduszu alimentacyjnego, Karty Dużej Rodziny oraz dodatków mieszkaniowych.
3) Przetwarzanie danych osobowych na potrzeby postępowań z zakresu przeciwdziałania przemocy w rodzinie
4) Przetwarzanie danych osobowych przez opiekunów i asystentów rodziny.
5) Przetwarzanie danych osobowych na potrzeby kadrowo-płacowe.

Ankiety, w oparciu o które dokonana została ocena ryzyka praw lub wolności osób, których dane dotyczą stanowią załącznik do niniejszej polityki (załącznik nr 1 – zestawienie ankiet na potrzeby analizy ryzyka).

Ogólny poziom ryzyka związanego z przetwarzaniem danych osobowych oszacowany został:

Ad. 4.

Mając na uwadze przeprowadzoną ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, opracowany został następujący wykaz zastosowanych oraz wdrożonych środków zabezpieczenia oraz mechanizmów bezpieczeństwa mających zapewnić ochronę danych osobowych.

Środki w zakresie zabezpieczenia organizacyjno-technicznego pomieszczeń, w których przechowywane są dane osobowe:

Środki w zakresie zabezpieczenia sprzętu elektronicznego:

b) Procedury i sposoby zagwarantowania realizacji praw osób, których dane są przetwarzane

Procedura zapewnienia prawa dostępu do danych osobowych

1. Każda osoba, której dane której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

a) celu przetwarzania;

b) kategorie odnośnych danych osobowych;

c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;

d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;

f) informacje o prawie wniesienia skargi do organu nadzorczego;

g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle.

2. Osoba, która chce skorzystać z prawa wskazanego w pkt 1. jest obowiązana do złożenia na piśmie lub w formie elektronicznej z wykorzystaniem podpisu elektronicznego lub platformy ePUAP wniosku o uzyskanie od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, oraz ewentualnego zakresu żądanych informacji.

3. Udzielenie potwierdzenia oraz informacji, o których mowa w pkt 1 i 2. następuje w formie pisemnej. W przypadku złożenia wniosku w formie elektronicznej z zastrzeżeniem wynikającym z pkt 2, udzielenie potwierdzenia
oraz informacji, o których mowa w pkt 1 i 2. następuje także w formie elektronicznej.
4. Informacja, o której mowa w pkt 3. jest wydawane w terminie do 7 dni od dnia wpłynięcia wniosku, o którym mowa w pkt 2.

Wzór informacji w przedmiocie potwierdzenia przetwarzania danych osobowych stanowi załącznik nr 2 do niniejszej polityki bezpieczeństwa danych.

Procedura zapewnienia prawa do uzyskania kopii danych osobowych

1. Każda osoba, której dane dotyczą, ma prawo żądać wydania kopii danych osobowych podlegających przetwarzaniu.
2. Osoba, która chce skorzystać z prawa wskazanego w pkt 1. jest obowiązana do złożenia na piśmie lub w formie elektronicznej z wykorzystaniem podpisu elektronicznego lub platformy ePUAP wniosku o uzyskanie od administratora kopii danych osobowych podlegających przetwarzaniu.
3. Wydanie kopii danych osobowych podlegających przetwarzaniu polega na wykonaniu kserokopii odpowiedniego dokumentu zawierającego dane osobowe podlegające przetworzeniu bądź wydaniu wypisu zawierającego wykaz przedmiotowych danych.
4. W przypadku złożenia wniosku w formie elektronicznej z zastrzeżeniem wynikającym z pkt 2, wydanie kopii danych osobowych podlegających przetwarzaniu następuje także w formie elektronicznej.
5. Wybór jednej z form wskazanych w pkt 3. dokonywany jest każdorazowo przez pracownika organu, z uwzględnieniem nakładu pracy oraz kosztów wydania kopii danych.
6. Wydanie kopii danych osobowych podlegających przetwarzaniu następuje w terminie do 7 dni od dnia wpłynięcia wniosku, o którym mowa w pkt 2.

Procedura zapewnienia dostępu do informacji wskazanych w art. 13 ust. 1 i 2 RODO

1. Każdej osobie, której dane są przetwarzane w Ośrodku, podczas pozyskiwania danych podaje się następujące informacje:
a) tożsamość i dane kontaktowe administratora danych;
b) dane kontaktowe inspektora ochrony danych;

c) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;

d) informacje o ewentualnych odbiorcach danych osobowych;

e) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

f) informacje o prawach przysługujących osobie, której dane są przetwarzane;

g) informacje o podstawie prawnej przetwarzania danych osobowych oraz konsekwencjach niepodania danych.

2. W przypadku, gdy dane osobowe pozyskiwane są w związku ze złożeniem wniosku w formie pisemnej lub podczas wywiadu środowiskowego, osoba, której dane są pozyskiwane otrzymuje druk informacyjny zawierający pozycje wskazane w pkt 1.

3. W przypadku, gdy dane osobowe pozyskiwane są w związku ze złożeniem wniosku w formie elektronicznej, osoba, której dane są pozyskiwane otrzymuje drogą elektroniczną druk informacyjny zawierającą pozycje wskazane w pkt 1.

4. Druk informacyjny, o którym mowa w pkt 2 i 3 stanowi załącznik nr 3 do niniejszej polityki.

Procedura wyboru i weryfikacji podmiotu przetwarzającego dane.

1. Każdy podmiot zewnętrzny przetwarzający dane zgromadzone przez tut. organ ma obowiązek zapewnić adekwatne środki i standardy zabezpieczenia przekazanych mu danych.
2. Warunkiem przekazania podmiotowi zewnętrznemu danych zgromadzonych przez tut. organ jest zawarcie
   z podmiotem zewnętrznym umowy o powierzenie danych osobowych
3. Wzór umowy o powierzenie danych osobowych stanowi załącznik nr 4 do niniejszej polityki.

c) Zasady powoływania i funkcjonowania inspektora ochrony danych osobowych

1. Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań przewidzianych w przepisach prawa.
2. W przypadku powierzenia funkcji inspektora ochrony danych osobie dotychczas zatrudnionej w organie, zawierana jest z nim dodatkowa umowa o świadczenie usług.
3. W przypadku powierzenia funkcji inspektora ochrony danych osobie dotychczas niezatrudnionej w organie, zawierana jest z nim umowa o pracę lub umowa o świadczenie usług.

4. Inspektor ochrony danych bezpośrednio podlega bezpośrednio kierownikowi Ośrodka.
5. W związku z wykonywanymi zadaniami z zakresu ochrony danych osobowych, inspektor ochrony danych osobowych nie może być odwoływany ani karany.
6. Do zadań inspektora ochrony danych należy w szczególności:

   a) informowanie administratora oraz zatrudnionych przez niego pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów prawa o ochronie danych osobowych;

   b) świadczenie usług doradczych na rzecz administratora oraz zatrudnionych przez niego pracowników, którzy przetwarzają dane osobowe, w zakresie ochrony danych osobowych;

   c) bieżący i okresowy monitoring przestrzegania przepisów RODO oraz innych przepisów prawa o ochronie danych, a także polityk administratora w dziedzinie ochrony danych osobowych;

   d) podejmowanie działań zwiększających świadomość administratora oraz zatrudnionych przez niego pracowników w zakresie ochrony danych osobowych;

   e) przeprowadzanie wstępnych oraz okresowych szkoleń personelu uczestniczącego w operacjach przetwarzania;

   f) przeprowadzanie audytów oraz oceny przestrzegania przepisów RODO oraz procedur niniejszej polityki przez pracowników zatrudnionych przez administratora danych;

   g) współpraca z organem nadzorczym;

   f) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem.

2. Rejestr operacji przetwarzania danych osobowych.

Rejestr operacji przetwarzania danych osobowych sporządzony jest wg następującego schematu:

1) nazwa czynności przetwarzania;
2) jednostka organizacyjna;
3) cel przetwarzania;
4) kategorie osób;
5) kategorie danych;
6) podstawa prawna;
7) źródło danych;
8) planowany termin usunięcia danych;
9) kategorie odbiorców innych niż podmiot przetwarzający.

Rejestr operacji przetwarzania stanowi załącznik nr 5 do niniejszej polityki.

3. Polityka monitorowania i reagowania na naruszenia ochrony danych

Polityka monitorowania ochrony danych

1. Bieżący monitoring przestrzegania niniejszej polityki, stosowania przewidzianych nią procedur oraz adekwatności stosowanych środków zabezpieczeń dokonywany jest przez inspektora ochrony danych.
2. Inspektor ochrony danych przynajmniej raz na 6 miesięcy dokonuje audytu polityki bezpieczeństwa

   w zakresie stosowania przewidzianych nią procedur oraz adekwatności stosowanych środków zabezpieczeń. Po przeprowadzonym audycie inspektor zobowiązany jest opracować pisemny raport dla administratora danych. Raport powinien zawierać ocenę oraz propozycje w zakresie ewentualnych modyfikacji stosowanych procedur oraz środków zabezpieczeń.
3. Na podstawie raportu wskazanego w pkt 2. administrator danych określa kierunki ewentualnych zmian oraz określa termin na ich wprowadzenie.

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu,

   chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:
   a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie
   b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji
   c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych
   d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

4. Rejestr incydentów.

Rejestr incydentów sporządzony jest wg następującego schematu:

1. data zdarzenia;
2. imię i nazwisko osoby zgłaszającej incydent;
3. imię i nazwisko osoby przyjmującej zgłoszenie incydentu;
4. data i godzinę przyjęcia zgłoszenia incydentu;
5. określenie czasu i miejsca incydentu;
6. opis zgłoszonego incydentu oraz okoliczności towarzyszące;
7. przyczyny wystąpienia naruszenia;
8. opis podjętych działań naprawczych;
9. wyniki przeprowadzonego badania wyjaśniającego;
10. ocena skuteczności przeprowadzonego postępowania naprawczego;
11. podjęte środki techniczne, organizacyjne i dyscyplinarne w celu zapobiegania w przyszłości naruszenia ochrony danych osobowych.

Rejestr incydentów stanowi załącznik nr 6 do niniejszej polityki.

5. Procedury zarządzania użytkownikami i dostępem do danych

a) Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe – załącznik nr 7 do niniejszej polityki.
b) Ewidencja osób upoważnionych do przetwarzania danych osobowych – załącznik nr 8 do niniejszej polityki.
c) Wzór oświadczenia o zachowaniu poufności – załącznik nr 9 do niniejszej polityki.
d) Wykaz podmiotów przetwarzających dane na zlecenie administratora danych – załącznik nr 10 do niniejszej polityki.

Administrator Danych Osobowych

.....

Podpis

6. Inspektor Ochrony Danych – kto może pełnić tą funkcję, jakie są jego zadania, jaki status nadają mu obowiązujące przepisy.

Artykuł 37 RODO - Wyznaczenie inspektora ochrony danych

1. Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy:

a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;

b) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub

c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

2. Grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych, o ile można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej.

3. Jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego inspektora ochrony danych.

4. W przypadkach innych niż te, o których mowa w ust. 1, administrator, podmiot przetwarzający, zrzeszenia lub inne podmioty reprezentujące określone kategorie administratorów lub podmiotów przetwarzających mogą wyznaczyć lub jeżeli wymaga tego prawo Unii lub prawo państwa członkowskiego, wyznaczają inspektora ochrony danych. Inspektor ochrony danych może działać w imieniu takich zrzeszeń i innych podmiotów reprezentujących administratorów lub podmioty przetwarzające.

5. Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39.

6. Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług.

7. Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy.

Artykuł 38 RODO - Status inspektora ochrony danych

1. Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
2. Administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
3. Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.
4. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.
5. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego.
6. Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.

Artykuł 39 RODO - Zadania inspektora ochrony danych

1. Inspektor ochrony danych ma następujące zadania:

a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;

d) współpraca z organem nadzorczym;

e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

2. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

7. Podmioty przetwarzające dane na zlecenie Administratora Danych – umowa o powierzenie danych i procedura weryfikacji.

Artykuł 29 RODO

Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego

Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia _____ pomiędzy:

……

zwany w dalszej części umowy „Administratorem danych" lub Administratorem"

reprezentowana przez:

Kierownika Ośrodka, …….

oraz

_____

zwany w dalszej części umowy „Podmiotem przetwarzającym"

reprezentowana przez:

_____

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części

„Rozporządzeniem”) dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.

2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy następujące dane zgromadzone przez Administratora Danych:

   ……

   ……
2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji umowy zawartej z Administratorem danych z dnia ……. w przedmiocie ……

§3

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.

6. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu 48 godzin.

§4

Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 7-dniowym uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni.
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§5

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w §3 ust. 2 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.

2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Generalnego Inspektora Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§7

Czas obowiązywania umowy

Niniejsza umowa obowiązuje od dnia jej zawarcia do dnia …….

§8

Rozwiązanie umowy

1. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:

a. pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;

b. przetwarza dane osobowe w sposób niezgodny z umową;

c. powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych;

§9

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne”).
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§10

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora danych (*lub Podmiotu przetwarzającego w zależności od postanowień stron).

_____ _____

Administrator danych Podmiot przetwarzający

8. Polityka monitorowania

Polityka monitorowania powinna określać wewnętrzne zasady kontroli i weryfikacji stosowania polityki bezpieczeństwa danych oraz aktualizacji standardów zabezpieczeń.

Przykładowa polityka monitorowania ochrony danych

1. Bieżący monitoring przestrzegania niniejszej polityki, stosowania przewidzianych nią procedur oraz adekwatności stosowanych środków zabezpieczeń dokonywany jest przez inspektora ochrony danych.
2. Inspektor ochrony danych przynajmniej raz na 6 miesięcy dokonuje audytu polityki bezpieczeństwa w zakresie stosowania przewidzianych nią procedur oraz adekwatności stosowanych środków zabezpieczeń. Po przeprowadzonym audycie inspektor zobowiązany jest opracować pisemny raport dla administratora danych. Raport powinien zawierać ocenę oraz propozycje w zakresie ewentualnych modyfikacji stosowanych procedur oraz środków zabezpieczeń.
3. Na podstawie raportu wskazanego w pkt 2. administrator danych określa kierunki ewentualnych zmian oraz określa termin na ich wprowadzenie.

9. Incydenty – obowiązki administratora danych i zgłaszanie incydentów do UODO.

Artykuł 33 ust. 1 RODO

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

10. Obowiązek informacyjny wynikający z art. 13 RODO

Artykuł 13 RODO

Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą

1. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:

a) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;

b) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;

c) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;

d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;

e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

2. Poza informacjami, o których mowa w ust. 1, podczas pozyskiwania danych osobowych administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:

a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

b)informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

c)jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

d) informacje o prawie wniesienia skargi do organu nadzorczego;

e)informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;

f)informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

3. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2.

4. Ust. 1, 2 i 3 nie mają zastosowania, gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami.

Druk informacyjny dla osób, których dane są przetwarzane w Ośrodku

DANE ADMINISTRATORA	Ośrodek Pomocy Społecznej w Adres: E-mail:
DANE INSPEKTORA DANYCH	Imię i nazwisko: Telefon kontaktowy: E-mail:
CELE PRZETWARZANIA	Dane są w celu wszczęcia oraz prowadzenia postępowania administracyjnego.

PODSTAWA PRAWNA PRZETWARZANIA DANYCH	Podstawą prawną przetwarzania danych jest niezbędność do wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c) RODO)
KATEGORIE DANYCH OSOBOWYCH	Przetwarzanie są następujące kategorie danych: imię i nazwisko, data urodzenia, adres zamieszkania lub pobytu lub zameldowania na pobyt stały, miejsce zamieszkania lub pobytu, numer PESEL, numer dokumentu potwierdzającego tożsamość, płeć, stan cywilny, obywatelstwo, stopień pokrewieństwa z członkami rodziny, numer rachunku bankowego, dane dotyczące stanu zdrowia oraz niepełnosprawności, adres poczty elektronicznej, numer telefonu, a w przypadku cudzoziemców – data wydania, numer i rodzaj dokumentu określającego status cudzoziemca w RP.
ODBIORCY DANYCH	Pani / Pana dane osobowe mogą być przekazywane podmiotom nadzorującym i kontrolującym działalność administratora danych
OKRES PRZECHOWYWANIA DANYCH	Dane będą przetwarzane przez okres niezbędny do realizacji celów przetwarzania oraz przez wymagany prawem okres archiwizacji danych
PRAWA PODMIOTÓW DANYCH	Przysługuje Pani / Panu prawo dostępu do Pani / Pana danych, prawo żądania wydania kopii danych, prawo żądania ich sprostowania, ich usunięcia lub ograniczenia ich przetwarzania.
PRAWO WNIESIENIA SKARGI DO ORGANU NADZORCZEGO	Przysługuje Pani / Panu prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych, tj. Urzędu Ochrony Danych Osobowych.
ŹRÓDŁO POCHODZENIA DANYCH	Pani / Pana dane zostały uzyskane przez administratora od ……

11. Podstawa prawna przetwarzania danych osobowych

Artykuł 6 RODO - Zgodność przetwarzania z prawem

1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

b) 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;

c) Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

d) Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

e) Przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

f) Przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których 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.

3. Podstawa przetwarzania, o którym mowa w ust. 1 lit. c) i e), musi być określona w prawie Unii lub praw państwa członkowskiego. Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w ust. 1 lit. e) – musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Podstawa prawna może zawierać przepisy szczegółowe dostosowujące stosowanie przepisów niniejszego rozporządzenia, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX. Prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu.

4. Jeżeli przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, nie odbywa się na podstawie zgody osoby, której dane dotyczą, ani prawa Unii lub prawa państwa członkowskiego stanowiących w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący

zagwarantowaniu celów, o których mowa w art. 23 ust. 1, administrator – aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane – bierze pod uwagę między innymi:

a) wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania

b) kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a administratorem;

c) charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 9 lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa zgodnie z art. 10;

d) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą;

e) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji.

Artykuł 9 RODO - Przetwarzanie szczególnych kategorii danych osobowych

1. Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.
2. Ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:

a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;

b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;

c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;

d) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie

dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;

e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;

f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;

h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;

i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osoób, których dane dotyczą, w szczególności tajemnicę zawodową;

j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

3. Dane osobowe, o których mowa w ust. 1, mogą być przetwarzane do celów, o których mowa w ust. 2 lit. h), jeżeli są przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe.

4. Państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia.

12. Prawa osób, których dane są przetwarzane a obowiązki pracowników OPS.

Prawo dostępu

Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

a) celu przetwarzania;

b) kategorie odnośnych danych osobowych;

c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;

d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;

f) informacje o prawie wniesienia skargi do organu nadzorczego;

g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;

h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Prawo do uzyskania kopii danych

Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba,

której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

Prawo do sprostowania danych

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

Prawo do usunięcia danych („prawo do bycia zapomnianym")

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

a)dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a), i nie ma innej podstawy prawnej przetwarzania;

c) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania;

d) dane osobowe były przetwarzane niezgodnie z prawem;

e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;

f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1.

Zasady powyższe nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:

a) do korzystania z prawa do wolności wypowiedzi i informacji;

b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3;
d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
e) do ustalenia, dochodzenia lub obrony roszczeń.

Prawo do ograniczenia przetwarzania

Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania w następujących przypadkach:
a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;
b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
c) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
d) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Jeżeli na mocy przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, 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 lub państwa członkowskiego. Przed uchyleniem ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia.

Prawo do przenoszenia danych

Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli:

a) przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) lub na podstawie umowy w myśl art. 6 ust. 1 lit. b); oraz
b) przetwarzanie odbywa się w sposób zautomatyzowany.

Wykonując prawo do przenoszenia danych, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

Wykonanie prawa, o którym mowa w ust. 1 niniejszego artykułu, pozostaje bez uszczerbku dla art. 17. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Prawo do sprzeciwu

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f), w tym profilowania na podstawie tych przepisów. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on 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.

Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.
Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie sprzeciwu oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.

W związku z korzystaniem z usług społeczeństwa informacyjnego i bez uszczerbku dla dyrektywy 2002/58/WE osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.

Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Prawo wyłączenia zautomatyzowanego podejmowanie decyzji w indywidualnych przypadkach
Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

Zasada powyższa nie ma zastosowania, jeżeli ta decyzja:
a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;
b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub
c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

W przypadkach, o których mowa w lit. a) i c), administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.

13. Odpowiedzialność odszkodowawcza – ogólne zasady i zakres odpowiedzialności

Artykuł 82 RODO - Prawo do odszkodowania i odpowiedzialność

1. Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.
2. Każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym niniejsze rozporządzenie. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom.
3. Administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności wynikającej z ust. 2, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody.
4. Jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator lub podmiot przetwarzający lub uczestniczy w nim zarówno administrator jak i podmiot przetwarzający i zgodnie z ust. 2 i 3 odpowiadają za szkodę spowodowaną przetwarzaniem, ponoszą oni odpowiedzialność solidarną za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania.
5. Administrator lub podmiot przetwarzający, który zgodnie z ust. 4 zapłacił odszkodowanie za całą wyrządzoną szkodę, ma prawo żądania od pozostałych administratorów lub podmiotów przetwarzających, którzy uczestniczyli w tym samym przetwarzaniu, zwrotu części odszkodowania odpowiadającej części szkody, za którą ponoszą odpowiedzialność, zgodnie z warunkami określonymi w ust. 2.
6. Postępowanie sądowe dotyczące odszkodowania jest wszczynane przed sądem właściwym na mocy prawa państwa członkowskiego, o którym mowa w art. 79 ust. 2.

Art. 61 ustawy o ochronie danych osobowych

Organizacja społeczna, o której mowa w art. 31 § 1 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego, może również występować w postępowaniu za zgodą osoby, której dane dotyczą, w jej imieniu i na jej rzecz.

14. Kary pieniężne za naruszenia przepisów RODO – czy rzeczywiście należy się ich obawiać?

Artykuł 83 ust. 1 RODO - Ogólne warunki nakładania administracyjnych kar pieniężnych

Każdy organ nadzorczy zapewnia, by stosowane na mocy niniejszego artykułu za naruszenia niniejszego rozporządzenia administracyjne kary pieniężne, o których mowa w ust. 4, 5 i 6, były w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające.

Art. 102 ustawy o ochronie danych osobowych

1. Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 100 000 złotych, na:

1)jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1-12 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych;

2)instytut badawczy;

3)Narodowy Bank Polski.

2. Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 10 000 złotych na jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

3. Administracyjne kary pieniężne, o których mowa w ust. 1 i 2, Prezes Urzędu nakłada na podstawie i na warunkach określonych w art. 83 rozporządzenia 2016/679.

NOTATNIK